it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

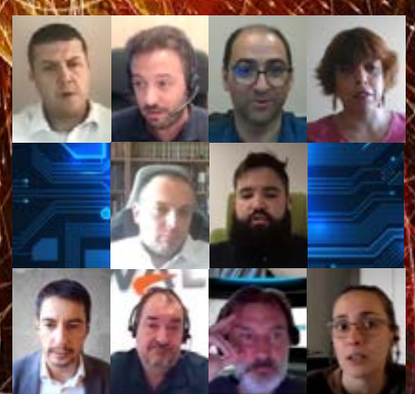
Junio 2021 - nº 42

La urgencia de la ciberinteligencia

‘Las empresas tienen que tener en mente la protección del ciclo de vida del dato’ (Manuel Barrios, Solvia)

Desayunos ITDS. XDR, la detección y la respuesta mandan

‘Es fundamental que los fabricantes tiendan a una filosofía de orquestación’ (Javier Modúbar, Ingecom)



Encuentros ITDS. Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?

“Nuestra apuesta es que la seguridad sea algo transversal, desde el principio hasta el final” (María José Talavera, VMware)

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

it Digital Security

Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara juanramon.melara@itdmgroup.es

Director de Contenidos
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Directora IT Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

La urgencia de la ciberinteligencia

Cada vez más ciberataques y más sofisticados. La evolución nos ha llevado de hablar de seguridad IT a ciberseguridad, y nos empuja hacia la ciberinteligencia. Es lo que tiene asumir que, antes o después, seremos atacados, que la mejor defensa es un buen ataque, y que la mejor opción es adelantarnos, conocer al enemigo y planificar una seguridad adaptativa capaz de hacer frente a cada tipo de ataque. Comprender cómo las amenazas se dirigen a la información, los sistemas, las personas y las organizaciones ayuda a empresas e individuos a comprender cómo realizar operaciones de búsqueda de amenazas y seguridad, responder a incidentes, diseñar mejores sistemas, comprender el riesgo y el impacto, realizar cambios estratégicos y protegerse del futuro.

Además de hablar de ciberinteligencia este número de IT Digital Security incorpora las entrevistas a Manuel Barrios, CISO de Solvia, para quien el cloud no es sinónimo de seguridad; Javier Modúbar, director general de Ingecom, quien demanda más orquestación; María José Talavera, responsable de VMware Iberia, una compañía cuya estrategia se ha reforzado con la pandemia, y Jorge Hurtado, quien a punto de cumplir un año en Cipher identifica cuatro ejes de inversión post pandemia.

La Seguridad Proactiva ha centrado el debate de unos nuevos #EncuentrosITDS en los que han participado los responsables de ciberseguridad de habitissimo, Aragonesa de Servicios Telemáticos, Sopra Steria, Userlytics y Maximice Events Group, y que han estado patrocinados por ESET, One Identity, Secure&IT, SonicWall y Trend Micro.

No hace mucho que el EDR, el Endpoint Detection and Response, se ha impuesto en el mercado, pero ya aparece la siguiente evolución que es el XDR, Extended Detection and Response, que centra unos #DesayunosITDS en los que han participado portavoces de Trend Micro Iberia, Varonis, Secure&IT, Palo Alto Networks Sophos y Kaspersky Lab.

Por último, la actualidad viene marcada por la evolución de Barracuda, la llegada a España de Kela y el impulso de Skybox Security, que quiere ayudar a los CISOs a dormir mejor.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

En Portada

La urgencia de la ciberinteligencia

itds

Sumario

Actualidad

Barracuda Networks: Teletransportar dispositivos a la red ha dejado de ser una buena idea

Kela: Ofrecemos visibilidad sobre los rincones más oscuros y peligrosos del ciberespacio

Skybox Security: Ayudamos a los CISOs a dormir por la noche

Encuentros ITDS

Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?

Desayunos ITDS

XDR, la detección y la respuesta mandan

Monográfico IT

Nuevos retos de seguridad en entornos financieros.
Su impacto en el modelo de negocio

Entrevistas

'Las empresas tienen que tener en mente la protección del ciclo de vida del dato'

Manuel Barrios, Solvia

'Es fundamental que los fabricantes tiendan a una filosofía de orquestación que permita que todas las tecnologías se hablen entre sí'

Javier Modúbar, Ingecom

No solo IT

Ciberseguridad: una oportunidad de transformación y diversidad

El SOC del futuro

Por qué no existe desempleo en ciberseguridad

Índice de anunciantes

'Nuestra apuesta es que la seguridad sea algo transversal, desde el principio hasta el final'

María José Talavera, VMware

'Uno de los principales riesgos en cualquier infraestructura es la complejidad'

Jorge Hurtado, Cipher

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA
CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN	PREVENCIÓN
ESET Threat Intelligence ESET Virus Radar WeLive Security	Endpoint Protection Platform ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
ESET Enterprise Inspector ESET Dynamic Threat Defense ESET Security Management Center ESET Cloud Administrator	Endpoint Protection Platform ESET Dynamic Threat Defense ESET Enterprise Inspector ESET Mail Security ESET Gateway Security ESET SharePoint Security ESET Secure Authentication ESET Endpoint Encryption ESET Security Management Center ESET Cloud Administrator
RESPUESTA	**DETECCIÓN**

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

Skybox Security: **Ayudamos a los CISOs a dormir por la noche**

El próximo hará 22 años, acumula 284 millones de dólares en varias rondas de financiación y su objetivo es ayudar a las empresas "a ir desde la incertidumbre a la certeza". Su nombre es Skybox Security y aunque hace un tiempo que está presente en nuestro país a través de Ireo, hace unos meses que cuenta con un responsable local: David García Cano.

Visibilidad es una de las mayores aportaciones a las empresas que realiza Skybox Security, una compañía que asegura proporcionar inteligencia y contexto para tomar "decisiones informadas" y ayudar a las empresas a "concentrarse en lo que importa". Dice David García Cano que en un modelo cada vez más Hybrid IT, con el despliegue de cada vez más soluciones de seguridad, cada vez es más difícil

PLANIFIQUE SU CIBERDEFENSA DE MANERA INTELIGENTE

CLICAR PARA VER EL VÍDEO

El modelado que realiza la compañía permite entender totalmente la situación real, no teórica, del nivel de riesgo que tiene un cliente en base al estado en el que se encuentran todos y cada uno de los elementos que conforman su red

prestar atención a las amenazas que son realmente importantes. “Los departamentos de Seguridad y TI necesitan visibilidad y análisis completos para mapear, validar y remediar rápidamente las vulnerabilidades en estas infraestructuras híbridas”, asegura el directivo.

Según datos del último informe “Vulnerability and Threat Trend Report 2021” de Skybox Security, la aparición de nuevas vulnerabilidades está alcanzando nuevos récords, complicando aún más la remediación. Además, aunque solo se explota una parte de las vulnerabilidades existentes, con 18.341 nuevas durante 2020 es cada vez más difícil para los equipos de seguridad orientar la acción hacia donde más se necesita. Se añade que los ciberdelincuentes empiezan a explotar vulnerabilidades de gravedad media o baja pero que aún así permiten realizar ataques laterales y acceder a activos críticos “porque saben que es probable que se encuentren sin parches”.

Más de 500 de las empresas más grandes del mundo confían en Skybox para obtener la seguridad y los conocimientos necesarios para hacer frente a las ciberamenazas. Los responsables de seguridad cada vez tienen más puntos que defender, dado que la superficie de ataque es mucho mayor, “y no tienen la capacidad de concentrarse en lo que realmente importa; no tienen la capacidad ni la visibilidad de poner foco en lo importante”, asegura David García Cano. “

"Ayudamos a las empresas a concentrarse en lo que importa"

David García Cano, Regional Director Spain & Portugal, Skybox Security

"Ayudamos a los CISOs a dormir por la noche", dice también el directivo de Skybox, explicando que su compañía ofrece soluciones de ciberseguridad que permiten definir un modelo de red dinámico y multidimensional donde se muestran todos los puntos de la red del cliente haciendo un modelado exacto de todos los elementos que la componen (FW, Balanceadores, IPS, Switches, Routers, Servidores, Endpoints). Añade que el modelado que realiza la compañía permite entender totalmente la situación real, no teórica, del nivel de riesgo que tiene un cliente en base al estado en el que se encuentran todos y cada uno de los elementos que conforman su red, y por tanto se puede tomar decisiones basadas en la realidad; "esto no es magia ni un arte, es tan solo ciencia de datos".

El valor de Skybox

"Ayudamos a nuestros clientes a concentrarse en lo que realmente importa", asegura David García Cano. La imagen completa y real de sus entornos híbridos es lo que permite a los clientes priorizar acciones y decisiones en función del riesgo real. "Trabajar con clasificaciones como CVSS ya no es suficiente. Es posible que algunas vulnerabilidades de muy alta gravedad no afecten a su seguridad, mientras que los delincuentes explotan las vulnerabilidades de baja gravedad porque saben que no son una prioridad para su remediación. Hasta ahora solo se ponían acciones para solventar lo crítico, no se paraban a pensar si eso era realmente

VULNERABILITY AND THREAT TRENDS REPORT 2021. EXECUTIVE SUMMARY

La séptima edición del "Informe Skybox Security Vulnerability and Threat Trends", destaca la necesidad de que maduren las prácticas de seguridad. Revela que 2020 fue otro año récord de nuevas vulnerabilidades y nuevas muestras de malware y que, al comprender el panorama de vulnerabilidades y amenazas, podemos anticipar mejor los cambios que los CISO y sus equipos deberán realizar en los próximos años.

"Somos uno de los nuevos cisnes negros del mercado de la ciberseguridad"

David García Cano, Regional Director Spain & Portugal, Skybox Security

lo importante o había que priorizar otras acciones previamente", explica el directivo, añadiendo: "En Skybox Security nos gusta acompañar a los clientes en su viaje desde la incertidumbre a la certeza para poder tomar las decisiones correctas en materia de ciberseguridad".

Asegurando que la gestión de la postura de seguridad se ha convertido en una necesidad crítica para la resiliencia y recuperación económica, explica David García Caño que la compañía se encuentra "en pleno crecimiento", con fuertes inversiones tanto en i+d como en capital humano, "lo que está

'Esto no lo hace nadie más que Skybox'

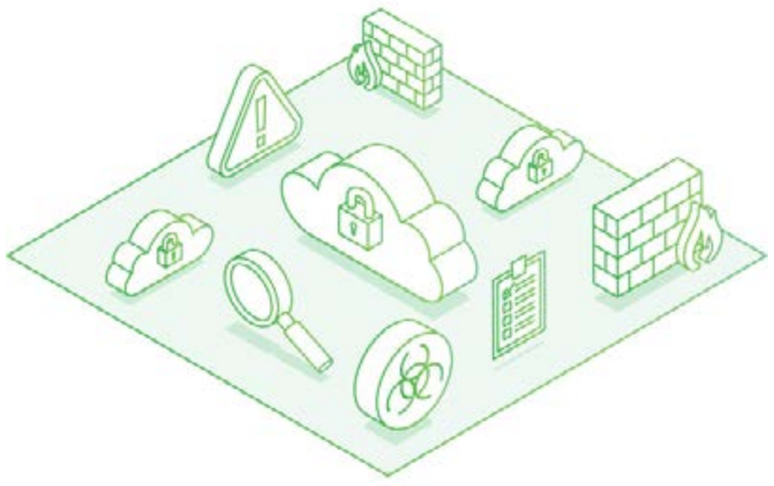
Chuck Cohen, Ireo

Sobre Skybox Security hemos hablado con Chuch Cohen, director general de Ireo, mayorista de este fabricante desde 2014. Asegura este directivo que, aunque hay muchas soluciones en el mercado que son capaces de escanear la infraestructura de una red para buscar agujeros de seguridad y la gestión de vulnerabilidades, "Skybox va mucho más allá porque lo que hace es crear una copia de la red del cliente para luego estudiar las diferentes formas en las que un elemento se puede conectar con otro", de forma que permite analizar con mucha más profundidad.

Al mismo tiempo, igual que hay muchos productos en el mercado que permiten centralizar la gestión de los firewalls, el modelo virtualizado de Skybox Security "permite experimentar con diferentes estrategias para modificar las reglas del firewall, ver qué funciona o qué no e implementar los cambios de forma automática para evitar errores de configuración". De forma que, en ambos casos "la clave de la tecnología es que reproduce la infraestructura del cliente dentro de un modelo teórico interactivo que permite al cliente probar diferentes escenarios, y esto no lo hace nadie más que Skybox".

Los ciberdelincuentes empiezan a explotar vulnerabilidades de gravedad media o baja porque saben que es probable que se encuentren sin parches

haciendo muy atractiva nuestra propuesta a inversores, empresas, partners, etc. Podemos decir que somos uno de los nuevos cisnes negros del mercado de la ciberseguridad". Añade que de cara al futuro "continuaremos evolucionando nuestra plataforma" y que en el corto y medio plazo "tenemos planes que nos están permitiendo crecer a doble dígito de manera sostenida convirtiéndonos en líder indiscutible en nuestro segmento".



Respecto al canal, explica David García Cano que se cuenta con un modelo de dos niveles y que todos ellos "son una extensión de Skybox Security" y asegura que "la cantidad de oportunidades que tiene el canal de ofrecer servicios de alto valor añadido en ciberseguridad con Skybox Security es enorme". it

Enlaces de interés...

- Blog Skybox Security
- A10 Networks, del ADC on-premise al cloud y la seguridad
- Sandbox Matter

Compartir en RRSS

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com

Kela: Ofrecemos visibilidad sobre los rincones más oscuros y peligrosos del ciberespacio

Kela es una compañía israelí que llega a España de la mano de Ingecom con capacidad para monitorizar varias decenas de grupos delictivos y gran parte de lo que ocurre en esa darkweb en la que los ciberdelincuentes negocian con herramientas, accesos y ese ransomware que acaba de dejar tu empresa expuesta a un chantaje.

Prefieren hablar del ecosistema del cibercrimen, y no de darknet o deepweb, ese lugar en el que los ciberdelincuentes se mueven con impunidad para vender sus creaciones, intercambiar datos robados y programar actividades ilícitas. Saber lo que allí ocurre es importante porque se pueden detectar indicios de un posible ataque, de una futura víctima. Kela, una compañía israelí que hace tres años consiguió 50 millones de dólares en una ronda de financiación, dedica sus esfuerzos a monitorizar lo que está pasando en ese ecosistema de

Las soluciones de Kela requieren un alto nivel de especialización y por eso las empresas de ciberseguridad son el medio natural para llegar al mercado final

cibercrimen, “en los rincones más inaccesibles y peligrosos del ciberespacio para detectar las amenazas que afectan a las empresas y organizaciones que se originan en dichos rincones”, nos cuenta Borja Rosales, vicepresidente europeo de Kela.

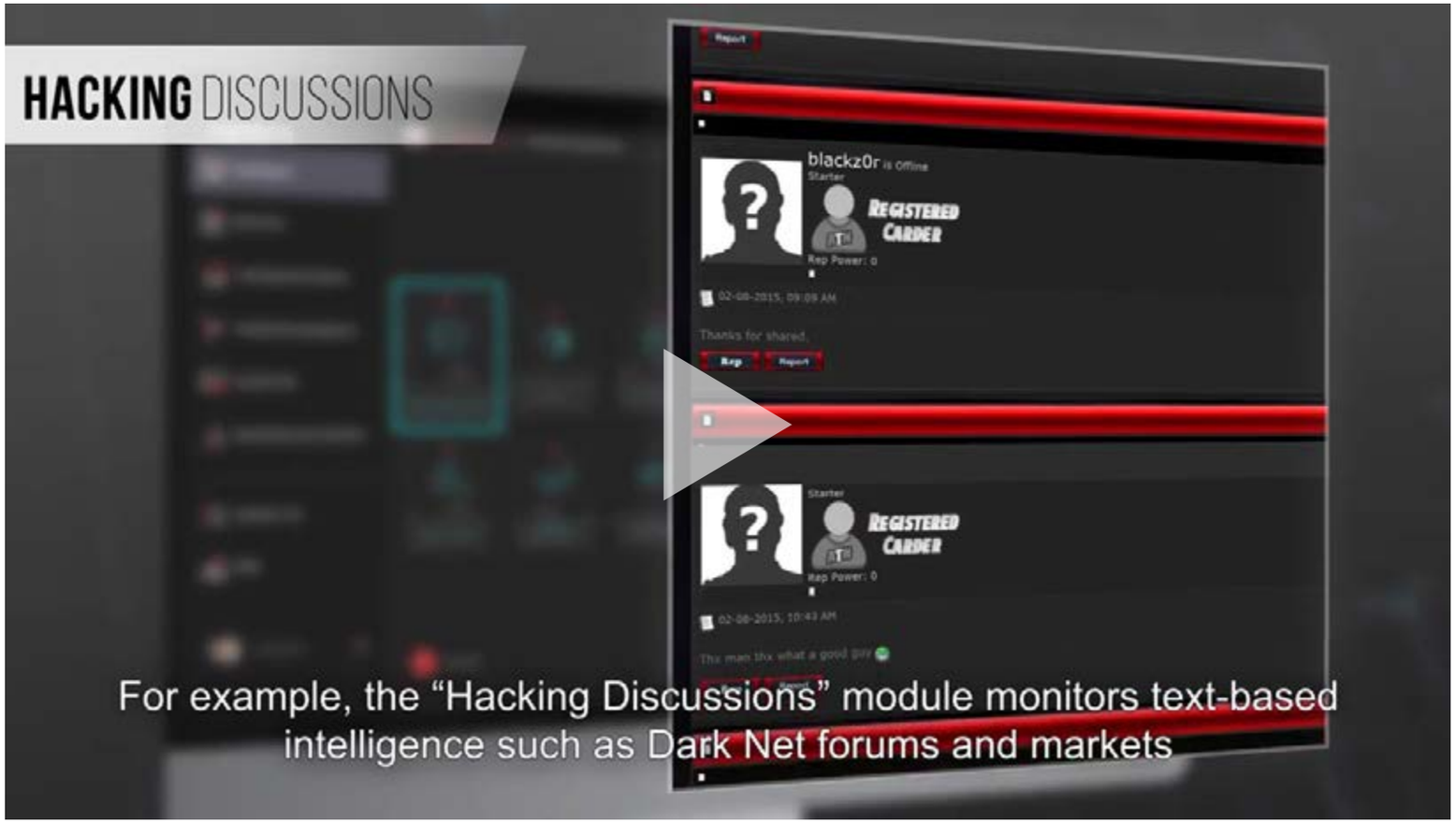
Este tipo de tareas encaja en un mercado que está despegando: el del ciberinteligencia, o inteligencia de amenazas, que según datos de Markets&Markets se ve impulsado por el incremento de las brechas de seguridad y que pasará de tener un valor de 10.900 millones de dólares en 2020 a 16.100 millones en 2025, con un crecimiento medio anual del 8%.

“Hablando en sentido militar, cuando hablamos de ciberinteligencia hablamos de saber qué está pasando detrás de las líneas del enemigo, qué está ocurriendo”, dice Borja Rosales. El enemigo, añade, no es un país, sino individuos y organizaciones que actúan en determinados lugares, y de lo que se trata es de “identificar qué saben sobre nuestros clientes que puedan utilizar para atacarles o desarrollar un ataque con más probabilidades de éxito”. Puntualiza el directivo de Kela que no monitorizan redes sociales o entornos open source, sino “sitios en donde realmente es muy difícil acceder”. Para ello Kela cuenta con un equipo de investigadores de inteligencia que están identificando y validando “cuáles son esos entornos, esos lugares en el ciberespacio en el que los cibercriminales se reúnen”.

Gracias a una tecnología desarrollada por Kela, la compañía es capaz de extraer información de esos entornos, de esas fuenrtes, y hacerlo de manera constante. Toda la información que se recupera de esos rincones oscuros se vuelca en un data lake al que pueden acceder los clientes de la compañía para recabar información de inteligencia que les afecta a ellos. Asegura Borja Rosales que lo que ha conseguido Kela es posiblemente una de las réplicas más completas de una parte del mundo del

cibercrimen “porque llevamos muchos años haciendo esto, y lo que hacemos es dar acceso a nuestros clientes y partners para que puedan adentrarse en esa réplica y consultar qué amenazas hay, o ha habido en el pasado, que les puedan permitir defenderse”.

Hacer esa copia no es tarea fácil ya que, en pro de la persistencia, la compañía no modifica ni toca los datos, y los extrae con mucho cuidado, pasando inadvertidos. “Los clientes nunca acceden al ecosistema directamente, sino a la réplica que tiene la compañía, lo que aporta varias ventajas, como es la anonimidad o protección de sus interesas y la capacidad de acceder al histórico de actividades de un entorno en el que, por lo habitual, se procura dejar pocas huellas”.



KELA TARGETED CYBER INTELLIGENCE — **CLICAR PARA VER EL VÍDEO**

El cliente

Kela tiene tres tipos de clientes. Por un lado las grandes empresas y administraciones públicas que están en el punto de mira de los ciberdelincuentes. Un segundo tipo de cliente son las empresas y proveedores de servicios de ciberseguridad, “con las que trabajamos para ayudarles a mejorar la defensa y anticiparse a las amenazas que afectan a sus clientes”. Reconoce que este perfil se puede dar alguna convergencia entre los grandes clientes que están haciendo uso de servicios gestionados.

Un tercer perfil de clientes con los que Kela trabaja y colabora son las fuerzas del orden “en un aspecto distinto al que lo hacemos con las empresas del sector porque el objetivo no es defender a una organización, sino intentar detener al cibercriminal”.

En el caso de las soluciones de monitorización continua, el modelo de negocio va en función del número de palabras clave de búsqueda que se configuran en las herramientas de la compañía. Una vez que se hace una búsqueda se tiene acceso a todos los resultados, aclara Borja Rosales.

Kela ha conseguido posiblemente una de las réplicas más completas de una parte del mundo del cibercrimen

El modelo de negocio de la solución de búsqueda de ciberamenazas, a la que Borja se refiere como el “Google de la Darknet”, es una suscripción en base al número de búsquedas diarias que se van a realizar.

“Somos una empresa de inteligencia”, dice el directivo cuando le preguntamos por el valor diferencial de la compañía. Añade que lo habitual para Kela es competir con empresas que desarrollan inteligencia, “pero nosotros somos una empresa de inteligencia que desarrolla la tecnología que nos permite gestionar esa inteligencia y recabar información que ayuda a nuestros clientes a saber por dónde les van a atacar, e incluso parar el ataque antes de que comience”.

Explica Borja Rosales que las soluciones de Kela requieren un alto nivel de especialización y que por eso “las empresas de ciberseguridad son nuestro medio natural para llegar al mercado final”. La estrategia en España es básicamente a través de canal, “y para ello hemos firmado el acuerdo de distribución con Ingecom que nos aporta un nivel de conocimiento, tanto de los partners especializados como de los proveedores de servicios gestionados (MSSP) muy amplio y una reputación muy sólida como mayorista de valor que los resellers de España valoran.

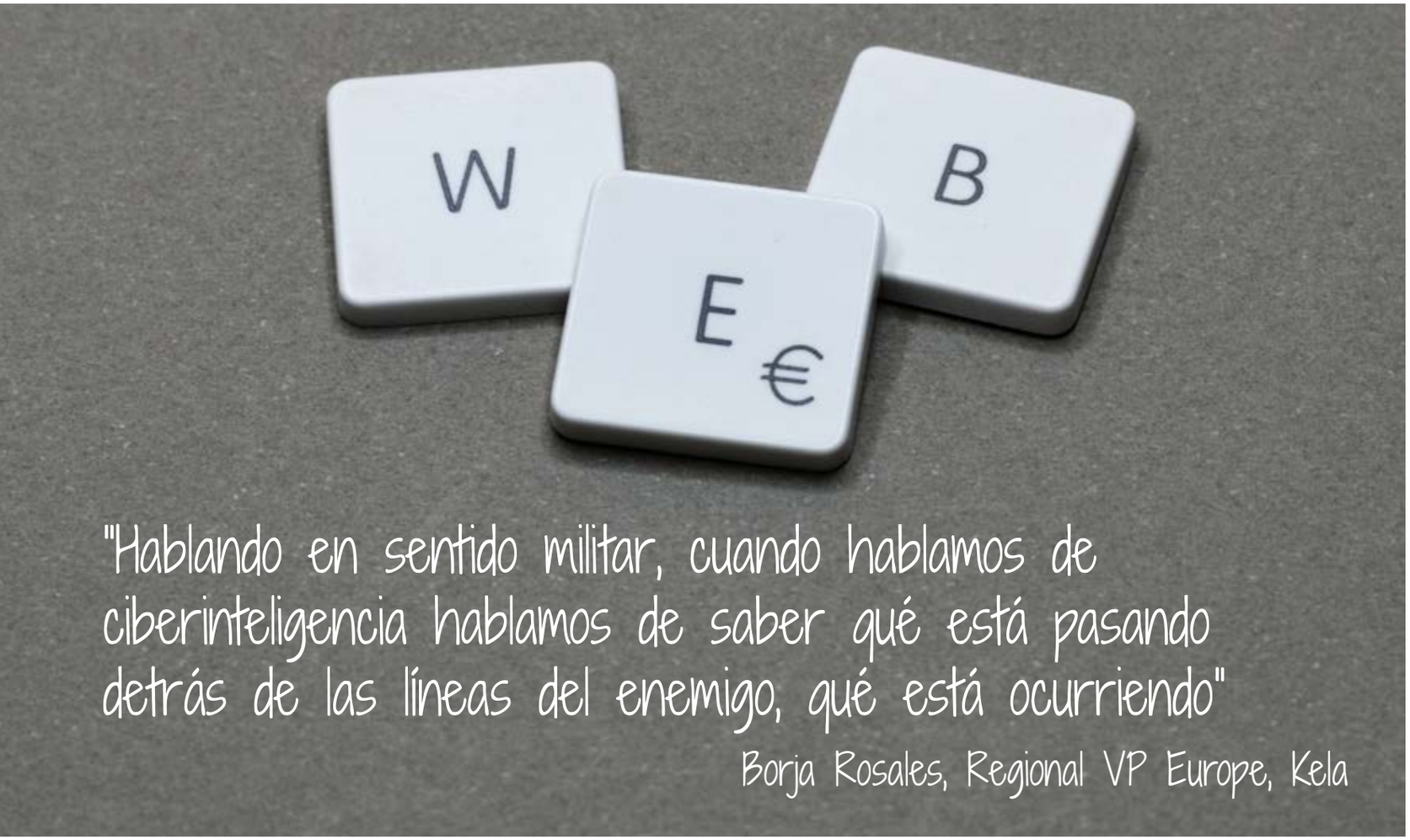
Darkweb

¿La darkweb sigue siendo un paraíso para los cibercriminales? “Yo no lo llamaría paraíso”, dice Borja Rosales, aunque sí que es un sitio “donde se sienten más cómodos porque se creó para proteger el anonimato de determinadas personas”.

Le preguntamos también al directivo de Kela si, sabiendo los ciberdelincuentes que existen soluciones como la de su compañía, existe una web aún más profunda a la que es imposible acceder. Dice que los ciberdelincuentes optan por moverse constantemente, pasar de un entorno a otro; “no sólo están en Tor, sino en canales de mensajería, o en cualquier sitio donde piensen que es más difícil que se les persiga… por eso nosotros no hablamos tanto de darknet como de ecosistema del cibercrimen”.

Además de ver cómo adoptan otro tipo de entornos, la compañía también ha observado en la darknet “un proceso de industrialización del cibercrimen, una profesionalización, una producción en cadena, y eso es algo que se está produciendo y creemos que va a seguir produciéndose”.

Esta especialización crea diferentes figuras, como el Initial Access Brokers que son cibercriminales que se dedican a conseguir el acceso a determinados entornos corporativos de empresa;



"Hablando en sentido militar, cuando hablamos de ciberinteligencia hablamos de saber qué está pasando detrás de las líneas del enemigo, qué está ocurriendo"

Borja Rosales, Regional VP Europe, Kela

“no desarrollan ningún ataque, sino que venden el acceso a una red a otros cibercriminales que son quienes desarrollan el ataque”.

Lo habitual es que la búsqueda de las amenazas en esa copia de la darkweb empiece con la búsqueda del nombre del cliente, explica el directivo de Kela. También se realizan búsquedas por los dominios e IPs de las empresas, o según las noticias o impactos como pudo ser el de Phone House o SolarWindows, “e incluso por los grupos o actores que sabes que te están monitorizando o que podrían tener interés en atacarte”.

Teniendo en cuenta que hay foros que están en ruso, ¿cómo resuelven vuestros clientes esta barrera? Kela cuenta con una herramienta que ayuda a traducir y permite a los clientes acceder a la información de una manera rápida, “que evidentemente no es lo mismo que un analista que hable ruso, porque hay que tener en cuenta la jerga, pero que es útil”.

Enlaces de interés...

- Kela
- El Gobierno anuncia una inversión de 450 millones para impulsar el sector de la ciberseguridad - 12 ABR 2021
- Las empresas europeas son poco propensas a compartir datos sobre amenazas

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTIÓN DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

Barracuda Networks: Teletransportar dispositivos a la red ha dejado de ser una buena idea

Desde su nacimiento en 2003, Barracuda Networks ha pasado de ofrecer protección del correo electrónico a una propuesta de backup capaz de proteger los datos, soluciones de seguridad de las aplicaciones y el cloud, y propuestas en torno a conceptos tan actuales como SD-WAN, SASE o Zero Trust Network Access.

Barracuda inicia su actividad hace 18 años con una primera línea de soluciones alrededor del correo electrónico. Nos lo cuenta Miguel López, director general de Barracuda Networks en Iberia, quien añade que la compañía fue abriendo nuevas líneas de negocio y que a día de hoy se trabaja tanto la protección de correo con appliances físicos o virtuales para proteger lo que es la entrada y salida de correo, como con cortafuegos de red, de aplicaciones (WAF) así como la seguridad de Office 365, "donde se cubre la protección tanto a nivel perimetral como interna, incluyendo tareas de backup, análisis mediante inteligencia artificial de posibles ataques internos, comportamiento de los usuarios, security awarenes, formación de usuarios… todo un paquete de soluciones para securizar Office 365".

Las soluciones de la compañía se repartem en propuestas en torno al Email Protection, App and Cloud Security, Network Security, Data protection – backup y Gestión centralizada, todo ello distribuido a través de canal bajo un modelo de dos niveles, mayorista e integrador, al que se ha añadido en los últimos meses la posibilidad de trabajar un modelo MSSP, o de proveedor de servicios de seguridad gestionado".

A primeros de 2018 Thoma Bravo anunciaba la compra de Barracuda Networks por 1.600 millones

de dólares. Asegura Miguel López que el acuerdo no cambió la estrategia de la compañía “en cuanto a trasladar la seguridad tradicional y hacerla compatible al mundo cloud”, sino quizá acelerarla “porque fue uno de los factores que interesaron en la compra”. “Lo que nosotros veníamos haciendo desde hace 20 años ahora se le llama SD-WAN y SASE”, dice también el directivo añadiendo que el portfolio se ha incrementado con la compra, en noviembre de 2020, de Fyde, proveedor de soluciones ZTNA (Zero Trust Network Access) que añade nuevas funcionalidades a la plataforma Barracuda CloudGen SASE

Sobre ZTNA dice el directivo de Barracuda Networks que es un mercado que cobra cada vez más relevancia en tanto en cuanto la pandemia ha obligado a la mayoría de las empresas a mover su fuerza de trabajo fuera de la oficina y conectarlos a todos ellos mediante VPN no es la solución porque “eso es teletransportarlos a la red con su dispositivo”.

La VPN está muy bien para el usuario porque tiene acceso a todo como si estuviera desde la oficina, asegura Miguel López, pero ese dispositivo está en casa y ni siquiera sabemos quién lo está utilizando, “de forma que teletransportar los dispositivos a la red ha dejado de ser una buena idea y lo que estamos viendo es que para muchos clientes disponer una herramienta que les permita asegurar que la conectividad se realiza de manera segura es una ventaja muy importante”.

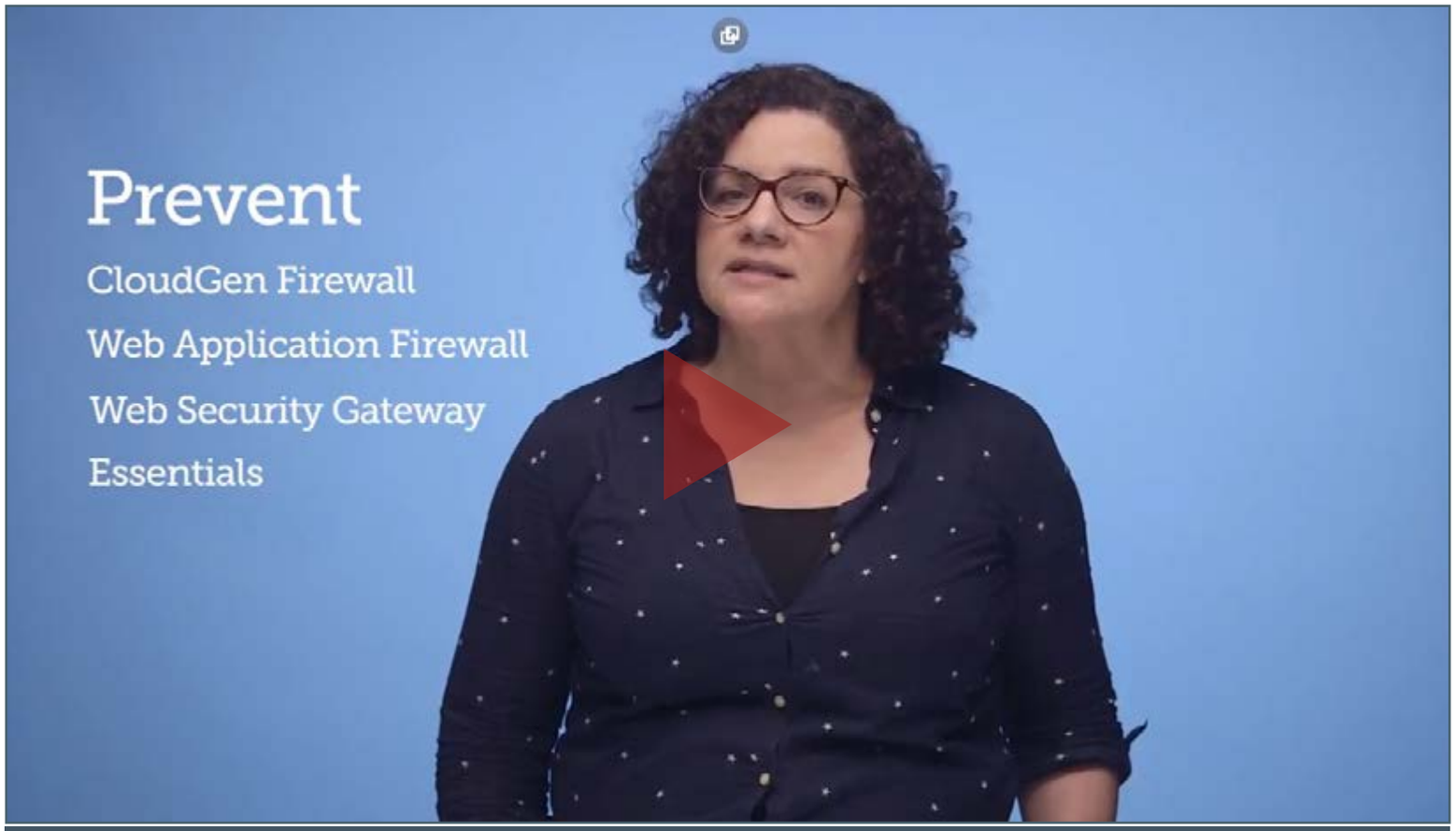
En el caso de SD-WAN “nosotros entendimos desde el principio que no bastaba con dar conectividad únicamente, sino que había que asegurar que esa conectividad fuera óptima desde el punto de vista de la gestión de los tráficos que había dentro. Ocho años después a esto se le ha llamado SD-WAN”.

El haberse adelantado ha permitido a Barracuda contar con protocolos de conectividad propietarios “que nos permiten hacer cosas más sofisticadas a nivel de la conectivdad que otros fabricantes que solamente utilizan de IPsec no pueden hacer porque están constreñidos por las limitaciones de este protocolo”.

Las mayores opciones de conectividad de los firewalls de Barracuda también les han permitido “adaptarse muy bien al mundo cloud porque no hay que olvidar que uno de los grandes retos del mundo de la nube es precisamente permitir la conectividad de todas esas cargas de trabajo que subimos a la nube, algo que no es sencillo utilizando la aproximación tradicional de colocar una VPN para conectar lo que hiciera falta”, explica Miguel López.

La propuesta de Barracuda es la de realizar una gestión inteligente del tráfico asegurando por

El incremento de los ataques de ransomware está impulsando el negocio de backup de Barracuda Networks



BARRACUDA | RANSOMWARE SOLUTIONS **CLICAR PARA VER EL VÍDEO**

ejemplo que el tráfico que pueda ser crítico, porque requiere un delay mínimo o que sea súper ágil en cuanto a la conexión, “lo podemos mandar por aquel link que en ese momento nos está dando la mejor respuesta, y que además lo podamos mandar acelerado, deduplicado, comprimido, priorizado con respecto a otros y todo ello gestionado dentro de un solo link, ya sea entre sitios on-premise, pero también conectándolo con la nube, y esa es una de las cosas que diferencian a Barracuda”.

Otro de los valores añadidos de la compañía, en opinión de Miguel López, es que todas las herramientas se han diseñado “tratando de maximizar la sencillez de las mismas”, algo importante para poder configurarlas correctamente y sacar el máximo partido de ellas. También destaca el directivo el hecho de que todo quede integrado en una consola que podría ser gestionada remotamente, y esto es muy interesante “porque permite que cada cliente decida a la carta qué soluciones necesita, que

"Nos encaja el cambio de paradigma que ha supuesto la pandemia"

pueda ir añadiendo más soluciones y que además arrope esas soluciones con un valor añadido por parte del canal a través de servicios profesionales del tipo que necesite de la manera que desee”.

Negocios

Asegurando que uno de los grandes caballos de batalla que existe actualmente en el mundo IT es la migración al cloud y que uno de los elementos que más se están migrando, o se han migrado ya, es el correo electrónico, dice Miguel López que el de Email Protection es uno de los negocios de Barracuda que más crece. Explica que cuando una empresa lleva el correo a la nube y además empieza a construir todo un ecosistema de soluciones complementarias alrededor, entre otras las generadas por el teletrabajo, “empiezas a hacer frente a desafíos de seguridad muy importantes”.

Asegura el directivo de Barracuda que la propuesta de la compañía es proteger el email desde una perspectiva global, lo que significa protegerlo desde diferentes vectores con una única consola de gestión a la que se pueden ir añadiendo nuevas funcionalidades y que además puede ser multitenant para que los partners puedan ofrecer servicios gestionados.

"Todo lo que sea la protección de Office 365 juega un papel crucial dentro de nuestro portfolio, junto con la protección de las aplicaciones web, donde todavía queda muchísimo por hacer"

Dice también Miguel López que Barracuda Networks es "el único fabricante a día de hoy que ofrece cobertura global del correo electrónico protegiendo tanto lo que sería la seguridad perimetral del correo como también proteger el correo desde dentro vigilando ataques de ingeniería social; protegerlo frente a la pérdida de información, frente a la pérdida de datos o frente ataques de ransomware con soluciones de backup y archivado; y protegerlo desde la perspectiva del usuario con formación para ayudarle a auto protegerse a día de hoy". Añade que no hay ningún otro fabricante que cubra las tres facetas: Protección del correo, protección de los datos y formación del usuario en una única solución.

Las potentes funcionalidades de Office 365 hace que los empleados pasen utilizándola la mayor parte de su tiempo y que sean muchos los datos que pasen por alguna de sus aplicaciones, lo que le convierten en un elemento muy atractivo para los ciberdelincuentes y un gran vector de ataque. Dice Miguel López que "todo lo que sea la protección de Office 365 juega un papel crucial dentro de nuestro portfolio, junto con la protección de las aplicaciones web, donde todavía queda muchísimo por hacer".

Respecto a la propuesta WAF de Barracuda, destaca la gran variedad de modos de despliegue que se ofrecen y la gestión sencilla de accesos, pudiendo establecer qué usuarios tienen acceso a qué aplicaciones, "y sólo podrán tener acceso una vez que hayamos comprobado que el dispositivo desde el que se están conectando es razonablemente seguro. Y eso es complementario al firewall existente".

El incremento de los ataques de ransomware está impulsando el negocio de backup de Barracuda Networks. En opinión de Miguel López cada vez hay más ataques de este tipo y las empresas no se han dotado de herramientas para protegerse del ataque, para detectarlo y para recuperarse una vez se ha producido. Asegura que la mayoría de las empresas fallan en una o varias de estas etapas y dice que la compañía cuenta con soluciones para cada una de las etapas, lo que "nos posiciona de una forma muy diferencial porque muchos de nuestros competidores pueden dar soluciones a nivel de proteger frente al ataque, incluso de analizar, pero pocos cuentan a la vez con herramientas para poder recuperarte frente a un ataque".

Barracuda en España

La filial de Iberia es una de las que más ha crecido en los últimos tres años, nos cuenta Miguel López, añadiendo que se ha visto un despegue importante de las soluciones cloud y SaaS, que no sólo es algo que demanda el mercado, sino que es un mundo "en el que los competidores de Barracuda van un par de pasos por detrás, lo que nos ha permitido crecer de manera muy saneada".

Los mayoristas en España son Ingram Micro y Ajoomal "a los que pedimos que aporten valor". Respecto a los integradores, explica Miguel López

"No hay ningún otro fabricante que cubra las tres facetas: Protección del correo, protección de los datos y formación del usuario en una única solución"

que se busca un equilibrio entre integradores grandes capaz de cubrir proyectos a nivel nacional o incluso internacional, e integradores más locales enfocados en compañías y territorios específicos.

Por otra parte, explica el directivo que el buen rendimiento de la compañía en los últimos años ha impulsado el crecimiento del canal, al que se ha dotado de herramientas "que les permiten mejorar la construcción de servicios de valor añadido sobre nuestras soluciones".

"Nos encaja el cambio de paradigma que ha supuesto la pandemia", dice Miguel López cuando le preguntamos qué cree que ha cambiado un año después de desatarse al crisis sanitaria y qué impacto puede tener en las tendencias de inversión en ciberseguridad. Explica el directivo que la pandemia ha acelerado el ciclo de cambio que se estaba produciendo de migración de servicios al cloud, así como la adopción masiva del teletrabajo, dos cambios "que encajan perfectamente con la aproximación que en general Barracuda tiene como compañía" y "dibuja un panorama bastante positivo para nosotros".

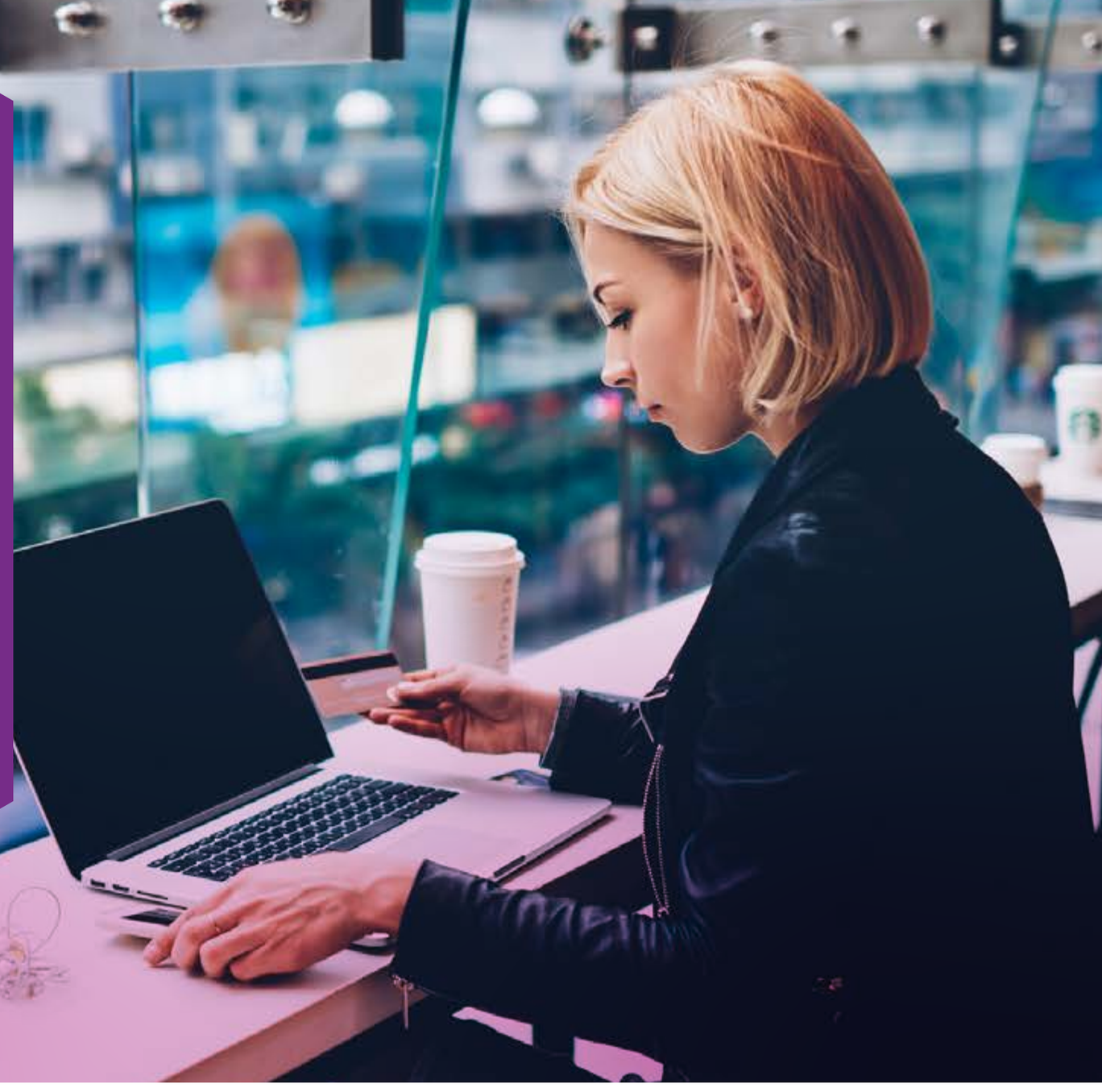
Enlaces de interés...

- En 2020 se detectó al menos un ataque en el 14% de los buzones de correo electrónico - 12 FEB 2021
- Barracuda compra Fyde para ampliar sus capacidades de Zero Trust
- Barracuda protege las aplicaciones web con Cloud Application Protection

Compartir en RRSS

ACCEDIENDO A UNA NUBE SEGURA

LA CONEXIÓN EN LA NUBE NO SIGNIFICA MENOS PROTECCIÓN



ENTRUST

‘Las empresas tienen que tener en mente la protección del ciclo de vida del dato’

(Manuel Barrios, Solvia)

Integridad y ética son dos grandes cualidades que debe tener un buen CISO, que además deber tener sentido común y dotes de liderazgo. Añade Manuel Barrios, responsable de ciberseguridad de Solvia, que tener un plan de continuidad de negocio es fundamental porque es la última salida ante un evento inesperado, que el cloud no es sinónimo de seguridad y que un EDR y una buena solución de actualizaciones y parches son elementos imprescindibles en el stack de seguridad de cualquier empresa.

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

Tener conocimientos de negocio y amplios conocimientos técnicos son dos de las cualidades que debe tener un buen CISO. Lo dice Manuel Barrios, CISO de Solvia, añadiendo además que se debe tener la capacidad de valorar los daños que pudiera haber en una pérdida de confidencialidad, saber hablar el idioma de cada uno, ser flexible, tener sentido común, dotes de liderazgo y capacidad de influencia. A todo esto, y debido "a la responsabilidad que tiene un cargo como éste" apunta dos últimas cualidades: integridad y ética; porque… ¿quién vigila al vigilante?

Sobre el grado de concienciación que tiene la empresa española respecto a la seguridad, dice Manuel Barrios que el panorama actual, en el que rara es la semana que no se informa de un incidente de seguridad, "ha obligado a que las empresas tomen conciencia de que lo que ocurre a otras empresas les puede ocurrir a ellas tarde o temprano". Añade el directivo que se suman regulaciones como GDPR y el miedo a las sanciones, lo que ha provocado que la seguridad se vea como algo necesario.

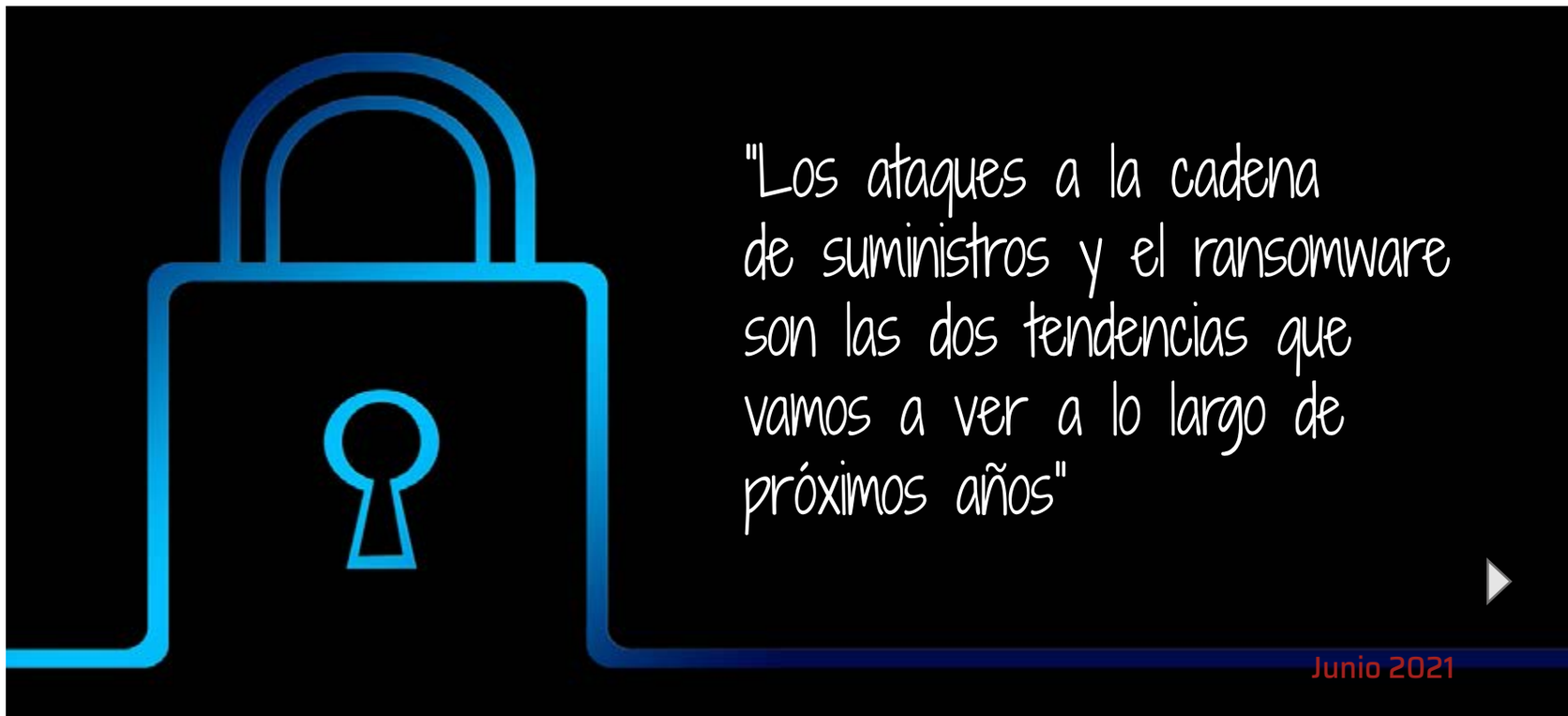
Tres cosas son las que, en opinión de Manuel Barrios, han aprendido los CISOs de la pandemia. La primera es que "hay que estar preparado para lo inesperado y hay que tener una mente abierta para una gestión del cambio" porque un incidente disruptivo puede presentarse el día menos pensado. Asegura el CISO de Solvia que la pandemia "ha puesto al descubierto las carencias de muchos planes de continuidad de negocio que se centraban exclusivamente en la IT pero no contemplaban el resto de escenarios, como es la falta de personal o el impacto reputacional" y que un plan de continuidad de negocio "es fundamental porque es nuestra última salida ante un evento inesperado".

Añade el directivo que se ha pasado de un modelo tradicional de presencialismo en oficinas a estar un 100% en teletrabajo, lo que obligó a plantearse "si los modelos y medidas de seguridad existentes eran suficientes y si se cubrían este tipo de escenarios". Para finalizar, asegura el directivo que este año "hemos aprendido mucho y hemos visto también que es posible hacer cosas que en la mente de mucha gente no estaba ni planteadas y se veían como una cosa imposible".

Y los CEOs, ¿qué han aprendido de la pandemia? Apunta Manuel Barrios a que mientras que los CISOs han aprendido a gestionar amenazas en entornos no planteados, adaptase al cambio y aprender nuevas técnicas para la protección de dato en cualquier ambiente, lo que los CEOs han visto son nuevos modelos de negocio, que es posible conseguir ahorros en infraestructuras y que se necesita inversión en ciberseguridad para proteger estos nuevos escenarios.

Cloud y servicios

"Estar en cloud no es sinónimo de estar seguro", dice Manuel Barrios cuando le preguntamos cómo se aborda una migración al cloud que se aceleró el año pasado. Explica que, independientemente de la pandemia, Solvia es una empresa cien por cien cloud, y



"Hemos aprendido mucho y hemos visto también que es posible hacer cosas que en la mente de mucha gente no estaba ni planteadas y se veían como una cosa imposible"

que si bien los proveedores cloud ofrecen unos SLAs que garantizan la disponibilidad en un alto grado, "todo lo relativo a seguridad y continuidad dependen de cada uno, y esto comprende desde la gestión de identidad, el backup, los firewall, el antimalware…". Añade que cualquier proyecto tiene que dotarse de requerimientos de seguridad, "al igual que se hace en entornos on-premise pero con la mentalidad de que las máquinas están en el CPD de un tercero".

Dice también el CISO de Solvia que cada vez son más las empresas que se van al cloud por temas de mantenimiento operativo, pero que el modelo de responsabilidad compartido "llega hasta cierta parte. El proveedor te ofrece la disponibilidad, pero todo lo demás dependerá de cómo lo tengas tú configurado".

Según datos de hace un año, el mercado de servicios de seguridad gestionados pasará de los 31.600 millones de dólares en 2020 a los 46.400 millones en 2025, con un crecimiento medio anual del 8% durante el periodo. El incremento de las brechas y los ciberataques son, en opinión de MarketsandMarkets, los principales impulsores de este mercado, así como la necesidad de adoptar las medidas necesarias para asegurar la postura de seguridad.

Dice Manuel Barrios que los servicios de seguridad gestionados ayudan mucho a la gestión operativa, "especialmente a la hora de proporcionar recursos especializados en ciertas tecnologías, lo que presenta un refuerzo casi fundamental para la gestión IT".

Tecnologías de seguridad

Cuando le preguntamos al CISO de Solvia por las tecnologías de seguridad que considera imprescindibles empieza respondiendo que "las empresas tienen que tener en mente la protección del ciclo de vida del dato, que es lo que hace que una empresa funcione. Si un dato pierde la integridad, confidencialidad y disponibilidad va a suponer un impacto en la empresa". Teniendo esto en cuenta Manuel Barrios considera fundamental "contar con una buena solución antimalware que no esté únicamente

Enlaces de interés...

- Ingecom
- 'El cloud no se hace responsable de la seguridad' (Toni García, LETI Pharma)
- 'Si puedo envenenar un data lake o hacer que un algoritmo funcione mal, tendré más influencia para la extorsión' (Rik Ferguson, Trend Micro)
- 'Ha habido estafas millonarias con un phishing básico' (Forensics&Security)

"Hay que estar preparado para lo inesperado y hay que tener una mente abierta para una gestión del cambio"

basada en firmas [un EDR], y una buena solución de actualizaciones y parches. Dos tecnologías con las que se van a salvar un amplio porcentaje de amenazas", a lo que el directivo añadiría el contar con tecnologías de backup que permitan recuperarse cuanto antes de un incidente. A partir de aquí, se irían añadiendo capas capaces de detectar y detener amenazas hasta llegar al puesto de trabajo, donde "más que cualquier tecnología pediría concienciación. De nada te sirve gastarte un millón de euros en una tecnología de seguridad si no tienes un usuario concienciado".

Sobre las tecnologías que Manuel Barrios considera que podrían ser fundamentales en un futuro, menciona con humor que aquella que fuera capaz de concienciar automáticamente al usuario, para después añadir que "cualquiera que permita detectar y bloquear amenazas en tiempo real".

Resume Manuel Barrios que "los ataques a la cadena de suministros y el ransomware son las dos tendencias que vamos a ver a lo largo de próximos años, y que seguramente serán nuestro mayor dolor de cabeza y nos llevarán adoptar soluciones de análisis de comportamiento y entornos SASE".

Compartir en RRSS

Proteja su experiencia en la nube de Azure.

Soluciones para proteger las aplicaciones y la información en Microsoft Azure y garantizar el cumplimiento de las reglas de seguridad »

Más información:
iberia_team@barracuda.com
barracuda.com

Barracuda Microsoft

STRENGTH IN SECURITY™

‘Es fundamental que los fabricantes tiendan a una filosofía de orquestación que permita que todas las tecnologías se hablen entre sí’

(Javier Modúbar, Ingecom)

Gestiona casi una treintena de fabricantes de seguridad que le permiten ofrecer una amplia variedad de propuestas, tanto las más habituales como otras que están empezando a adentrarse en el mercado y serán necesarias en un futuro próximo. Dice que el conocimiento es uno de los diferenciales de Ingecom; que las empresas demandan tecnologías que no requieran recursos propios y que, roto el perímetro, hay tecnologías que se han convertido en prioritarias, como la gestión de las identidades, múltiple factor de autenticación, análisis del comportamiento o planes de concienciación.

Texto: Rosalía Arroyo
Fotos: Ania Lewandowska

Junio 2021

Ciberseguridad y ciberinteligencia son las dos grandes áreas de negocio definidas por Ingecom a comienzos de este año. Nos lo cuenta Javier Modúbar, co-fundador y CEO de Ingecom un mayorista con presencia en nueve países y que trabaja con casi 30 fabricantes que le permiten ofrecer tecnologías tanto para el mercado de big data como de cloud, protección de datos, simulación, endpoint, concienciaión o IIoT/OT.

Diferencia Javier Modubar la ciberseguridad de la ciberinteligencia porque mientras que la primera se centra en poner medidas para prevenir los ataques o posibles amenazas, “la ciberinteligencia busca detener a los ciberdelincuentes antes de que realicen los ataques”.

“Buscar soluciones disruptivas y novedosas que encajen en las necesidades presentes y, sobre todo, futuras”, es uno de los grandes diferenciales de Ingecom. Añade Javier Modúbar que la compañía también destaca por el apoyo que se presta a los fabricantes a la hora de desarrollar su negocio en el mercado; “no queremos que nos vean como un mero tramitador de su oferta, sino como un partner que le ayuda a detectar nuevos negocios”. El tercer pilar en el que se sustenta el diferencial de Ingecom es “nuestra capacidad técnica para apoyar a los fabricantes y a nuestros partners a la hora de integrar tanto las soluciones de ciberseguridad como de ciberinteligencia”.

¿Qué demanda la empresa española?

“No todas las tecnologías valen para todas las empresas”, responde Javier Modúbar cuando le preguntamos qué es lo que están demandando las empresas y, sobre todo, si tienen claro lo que necesitan. De manera más genérica, lo que está

"Roto el perímetro, hay tecnologías que se han convertido en prioritarias, como la gestión de identidades, múltiple factor de autenticación, análisis del comportamiento o planes de concienciación"

"Para los mayoristas de seguridad puros 2020 no fue un año malo, pero tampoco fue un año excelente"

demandando el mercado es: tecnologías que no sean difíciles de implantar, que no requieran muchos recursos técnicos propios, "por lo que estamos viendo una tendencia a ir a un sistema de MDR (Managed Detection and Response) en el que los propios fabricantes ponen su experiencia y recursos humanos para dar ese valor y ese conocimiento al que muchas empresas no pueden llegar".

Además, y aunque es complicado "porque cada empresa es buena en una cosa y ninguna es buena en todo", los clientes quieren concentrar fabricantes, asegura el directivo de Ingecom. Por último, lo que más demanda la empresa española "es conocimiento, que es el diferencial de Ingecom".

Orquestando

Identifica Javier Modúbar, como "fundamental" que los fabricantes tiendan a una filosofía de orquestación que permita que todas las tecnologías se hablen entre sí. "Aquel que actúe como estanco difícilmente va a evolucionar. Necesitas hablar con otros fabricantes porque cada uno aporta una cosas y entre todos dan seguridad".

La búsqueda de simplificación de la operativa de seguridad también está acelerando la consolidación en el mercado de seguridad. Habla Modúbar de una "vorágine" de compras el año pasado; fabricantes que compraban a otros fabricantes e incluso "grupos tecnológicos que no están comprando una o dos empresas, sino decenas, y las están integrando en una misma plataforma con la intención de cubrir el 90% de la seguridad de una empresa". ¿Cómo lo están haciendo? "Con el orquestador. Primero ven quién se habla bien con ellos y luego tienden a comprarlo".

Por otro lado, siguen apareciendo empresas nuevas empresas, no sólo en el mercado de ciberseguridad, sino de ciberinteligencia. Respecto a esto último asegura Javier Modúbar que hasta hace cinco años no existían tantas pero que "empieza a haber un nicho potente porque la tendencia es intentar coger a los malos antes de que actúen". Identifica también el directivo otro grupo de empresas que aprovechan la información que hay en la Darknet para cazar a los malos antes de que la exploten.

Y por supuesto "todos los años hay tendencias nuevas. Donde se creía que se estaba cubierto ahora no se está".

"La ciberinteligencia busca detener a los ciberdelincuentes antes de que realicen los ataques"

El humano y el dato

Si yo tuviera que atacar, empezaría por la debilidad del humano, dice Modúbar, añadiendo que se ha visto un aumento de los ataques de ransomware, de phishing y un aumento de la ingeniería social porque "es más fácil atacar a alguien que está en su casa". Continúa diciendo el directivo que una vez que ha caído el humano "se intenta atacar el dispositivo al que está conectado el humano". El tercer pilar a proteger es la infraestructura, la red; "todo el mundo piensa en una red interna, pero puede ser la VPN o la conexión que haces a la nube para llegar a una aplicación". Las aplicaciones son el cuarto pilar a proteger para impedir que los ciberdelincuentes lleguen al verdadero tesoro, los datos, que son el quinto pilar a proteger.

"Estos cinco pilares es como se produce un ataque habitualmente y es donde nosotros montamos casi toda la arquitectura de Ingecom", explica Javier Modúbar sugiriendo que las inversiones en seguridad prioricen dos pilares: el humano y el dato. "Si a través de planes de concienciación evitamos los errores reduciremos un porcentaje de brechas de seguridad enorme. Y si protegemos el dato, que es lo que han venido a buscar, cerramos también muchas oportunidades", asegura Javier Modúbar añadiendo que "esto no quiere decir que no haya otro tipo de ataques".

Impacto de la pandemia en hábitos de compra/inversión

Preguntamos a Javier Módubar cómo ha impactado la pandemia sanitaria en las previsiones de inversión en ciberseguridad de las empresas. Habla de dos etapas, una inicial, en el que las inversiones de las empresas se centraron en la disponibilidad de la gente, y donde "la seguridad

"Si a través de planes de concienciación evitamos los errores reduciremos un porcentaje de brechas de seguridad enorme"

no fue una prioridad en un primer momento, pero se han ido concienciando de que hay que meter capas de seguridad y es ahora cuando se está haciendo".

Dice también Javier Modubar que el crecimiento en Ingecom no fue el de otros años porque los grandes proyectos de seguridad en infraestructuras se pararon en seco, entre otras cosas porque la gente ya no estaba disponible para implantar esos proyectos. "Vimos cómo los distribuidores que eran más 'dispach' tuvieron un año increíble porque tuvieron rotura de stock. Para los mayoristas de seguridad puros no fue un año malo, pero tampoco fue un año excelente".

Sin embargo, este año las cosas cambian. La segunda fase es la de asegurar a toda esa gente que se ha ido a trabajar a casa, y no va a volver, y que acceden a aplicaciones que ya están en la nube. Por tanto "es en esta segunda fase cuando se van a realizar inversiones en ciberseguridad".

Por otra parte, hay que tener en cuenta que, roto el perímetro, hay tecnologías que se han convertido en prioritarias, como la gestión de las identidades, múltiple factor de autenticación, análisis del comportamiento o planes de concienciación. Asegura también Javier Modubar que conceptos como Zero Trust o SASE son tendencia, junto con la protección del dato.

Enlaces de interés...

- Ingecom
- 'El cloud no se hace responsable de la seguridad' (Toni García, LETI Pharma)
- 'Si puedo envenenar un data lake o hacer que un algoritmo funcione mal, tendré más influencia para la extorsión' (Rik Ferguson, Trend Micro)
- 'Ha habido estafas millonarias con un phishing básico' (Forensics&Security)

Compartir en RRSS

X-Ray Vision for Malware

VMRAY

vmray.com

‘Uno de los principales riesgos en cualquier infraestructura es la complejidad’

(Jorge Hurtado, Cipher)

A punto de cumplir un año en Cipher, la unidad de ciberseguridad de Prosegur, hablamos con Jorge Hurtado, quien identifica cuatro ejes de inversión post pandemia: habilitar el trabajo de forma segura, protección del endpoint, formación y concienciación y automatización.

Cuando el valor pasó a estar en los datos y en la tecnología más que en los edificios y las cosas, Prosegur quiso avanzar y en 2014 comenzó a invertir en la creación de una unidad de ciberseguridad capaz de proteger los activos digitales. Tras las compras de Innovis y Dognaedis fue crucial la de Cipher, uno de los proveedores de referencia del mercado brasileño y con presencia en Estados Unidos, Colombia y Paraguay, tras la que se decide consolidar todas las actividades de ciberseguridad bajo la marca Cipher y posicionarla como una unidad de negocio independiente.

Desde hace casi un año Jorge Hurtado es el Vicepresidente de Cipher para la región de EMEA tras pasar más de dos años en S21sec. Nos cuenta que los 40 años que lleva Prosegur haciendo el mundo más seguro “confieren a Cipher algunas características importantes como es tradición, compromiso, servicio al cliente y calidad de los servicios, así como la cobertura internacional”.

Destaca también Jorge Hurtado que Cipher se posiciona como “un proveedor de ciberseguridad nativo digital” porque no es lo mismo la seguridad para un entorno on-premise, o de hace diez o quince años, que para los nuevos entornos tecnológicos que tienen en cuenta el cloud, el IoT o cómo aplicar

la cibeseguridad desde el diseño en todos los procesos de transformación digital.

Como elemento diferenciador de Cipher destaca Jorge Hurtado que es “una de las pocas compañías que pueden aunar el mundo de la seguridad lógica, o ciberseguridad, con el de la seguridad física, que cada vez tienen más relación”. En este terreno se han de tener en cuenta ataques que se aprovechan de un elemento físico, como un acuario, para acceder mundo IT, o los ataques al mundo OT que acaban impactando en el agua que se consume.

También destaca Hurtado como valor diferencial que en un mundo en el que hay cada vez más proveedores, Cipher se dedica sólo a la ciberseguridad y que “no somos un fabricante por lo que nos podemos permitir recomendar a nuestros clientes la mejor opción para la necesidad que tenga”.

De forma que, como resumen, ser un proveedor nativo en seguridad digital; un player a nivel internacional con músculo financiero; la tradición que le aporta Prosegur, que le permite afrontar las amenazas híbridas que traspasan las barreras físicas y las barreras digitales; y la ausencia de conflictos de interés, “son los valores diferenciales que nos definen”.

Innovación

La innovación es otros de los grandes diferenciadores de Cipher, que ha creado un sistema de orquestación y automatización nativo en cloud para atender incidentes de seguridad. Explica Hurtado que atender un incidente de manera automatizada no significa que se dé con una calidad peor que cuando lo atiende un humano, “sino que se va a dar de una manera más rápida, que no se cometen errores y que el tiempo medio de respuesta es mucho más corto”. Añade que como empresa proveedora de servicios, ser capaces de responder mucho más rápido ante los incidentes de seguridad a través de esa automatización “es algo básico”.

Menciona también Jorge Hurtado la ciberinteligencia, “entendida como todo el conocimiento del contexto” como un elemento diferenciador que se integra en los servicios gestionados de la compañía y que no sólo permite ofrecerlos de una manera mucho más eficiente sino “anticiparnos al propio incidente”.

El servicio que más crece

Sin dar cifras concretas, comenta Jorge Hurtado que Cipher ha tenido un crecimiento “muy sustancial en el año 2020” y que fueron los servicios gestionados desde el SOC son los que más crecieron, “en particular lo que tiene que ver con la gestión de incidentes”. Además, la compañía cuenta con un servicio de vigilancia digital y de ciberinteligencia que también creció durante la pandemia.

“Cada vez más los clientes saben lo que quieren”, responde el directivo de Cipher cuando le preguntamos si las empresas demandan servicios más generales de ciberseguridad o tecnologías específicas. En opinión de Jorge Hurtado, todavía existen casos en los que “tenemos que guiar al cliente

"Atender un incidente de manera automatizada no significa que se dé con una calidad peor que cuando lo atiende un humano, sino que se va a dar de una manera más rápida y sin errores"

desde el principio", pero que el corporativo, que es más maduro, "sabe lo que quiere, con los proveedores con los que quiere trabajar y las características dentro de cada uno de los servicios que está buscando". Asegura también que este cambio es bueno porque hace que los proveedores "nos enfoquemos en innovar y aplicar servicios que van a aportar valor a esos clientes".

En el mundo de la pyme aún queda mucho camino por recorrer, dice Jorge Hurtado, que habla del 'Wild Wild West', de un entorno en el que no hay soluciones adaptadas a las pymes y en el que el nivel de concienciación y conocimiento no está al nivel de lo que saben las corporaciones; "yo creo que tenemos que hacer todos un esfuerzo por cubrir este entorno porque además, según los estudios, es el ámbito más atacado", dice el directivo de Cipher, que a mediados de marzo anunciaba su incorporación a Cybermadrid, el clúster de ciberseguridad de la capital española que tiene como objetivo sensibilizar y formar a empresas y ciudadanos en la importancia crítica de la ciberseguridad, y que ha desarrollado una oferta de servicios para empresas de menor tamaño.

Inversiones post-pandemia

Un año después de la pandemia, ¿se invierte de otra manera en ciberseguridad? "Yo creo que sí", asegura Jorge Hurtado, que identifica cuatro ejes fundamentales de inversión post-pandemia. El primero es todo lo que tiene que ver con habilitar el teletrabajo de manera segura. La segunda es la protección de endpoint, donde se está produciendo la transición del antivirus tradicional a un modelo de endpoint monitorizado, EDR, "porque ya no nos podemos fiar de los controles de seguridad perimetrales". El tercer eje es la propia transformación digital, que se aceleró debido a la pandemia, impulsora también de la adopción del cloud como "una solución absolutamente natural al problema de que todo el mundo esté distribuido por todos

"Tenemos que tener una visión bastante pragmática de lo que son las soluciones de ciberseguridad"

los sitios y que cada empleado esté trabajando desde su casa".

Un tercer eje de inversión tiene que ver con la formación y concienciación, una tendencia "que obviamente es creciente porque en cada incidente grave las personas aparecen de una forma u otra". Añade que, además, este año los empleados han sufrido mucho y han pasado de estar en un entorno muy controlado, donde tenían compañeros con los que interactuar o a los que preguntar dudas, a un entorno donde el empleado está aislado y es incapaz de discernir por él mismo si se está enfrentando a una amenaza o no.

En esta línea de formación y concienciación Cipher lanzará un servicio al que se ha bautizado como Mistery Insider "que simula lo que podría hacer un usuario malicioso desde la perspectiva del atacante" y que permitirá a la compañía determinar "cuál es el acceso, la visibilidad y el nivel de exposición de los activos hacia cada uno de los individuos o grupos de individuos dentro de los servidores".

Respecto a la última tendencia de inversión dice Jorge Hurtado que "no nos podemos olvidar que las compañías, y sobre todo las grandes, siguen en crisis", y por lo tanto "tenemos que tener una visión bastante pragmática de lo que son las soluciones de ciberseguridad" e ir hacia una seguridad efectiva y eficiente que unifique las soluciones al máximo posible "para tratar de simplificarlas y que por un lado resulten más efectivas en coste, pero por otro también resulten menos arriesgadas, porque uno de los principales riesgos en cualquier infraestructura es la complejidad".

Tipo de cliente

"El foco está en el cliente empresarial corporativo", dice Jorge Hurtado, añadiendo que hay una oportunidad de mercado en un tipo de empresa más pequeña "que desde el punto de vista de ciberseguridad está siendo desatendida".

El objetivo es trasladar a este mercado una oferta más acotada, diseñada a la medida de las posibilidades de una pyme, y que les aporte esa seguridad efectiva y eficiente. Se pregunta Hurtado por qué una respuesta ante incidentes tiene que estar reservada a una gran empresa y asegura que hay muchas empresas que tienen incidentes y que no encuentran una solución o servicio de respuesta. "Nosotros estamos trabajando para poder ayudar no solo a los grandes bancos o las grandes cadenas de retail, sino también a las pequeñas empresas".

¿Se trata de llevar la Thin Security a la pyme? "Exacto", responde el vicepresidente de Cipher, quien añade que los desafíos "son obviamente distintos" y que en la pyme se tienen que dar

Enlaces de interés...

- Ryuk acaba con la cúpula directiva de Cipher, la unidad de ciberseguridad de Prosegur
- Prosegur Ciberseguridad presenta Cipher a sus clientes
- Prosegur adquiere Dognaedis en Portugal y refuerza su división de ciberseguridad

soluciones más acotadas y automatizadas; “a través de la automatización y a través de la inteligencia artificial somos capaces de dar soluciones en el entorno pyme”.

Tecnologías de futuro

Respecto a las tecnologías que están empezando a despegar y serán fundamentales en un futuro, menciona Jorge Hurtado el XDR como una de las innovaciones que más rápido va a llegar al mercado porque está ya lista y funcionando. Añade también que se tiene que avanzar mucho “en la securización de los entorno cloud nativos, sobre todo cuando hablamos de entornos multicloud” porque hay opciones que están en marcha pero “no han cristalizado en un offering estándar que pueda ser trasladado fácilmente a los clientes”.

No se olvida de la securización de los entornos de IoT, “que continúan siendo un desafío no tanto en lo que se refiere a los nuevos productos conectados sino a los que ya están desplegados y funcionando sin que en ningún momento se haya tenido en cuenta la ciberseguridad”.

La Deception, una tecnología en la que ha invertido la compañía, también es otra de las que darán mucho que hablar en el futuro, en opinión de Hurtado. Dice el vicepresidente de Cipher que el concepto es atractivo y que la compañía ha intentado establecer una serie de nodos de engaño, por ejemplo de sistemas electrónicos de seguridad que permiten recopilar IOCs que después se aplican en los servicios.

Los llamados servicios de red team automatizados son otra de las tendencias apuntadas por Jorge Hurtado, quien explica que el mercado aún no está del todo preparado para ellos. Y una última tendencia, que es más una necesidad, es la automatización debido a la falta de personal y el aumento exponencial de incidentes; “la inteligencia artificial y el machine learning aplicados con una utilización práctica y concreta que me lleve a reducir las incidencias del SOC, o poder levantar alertas cada vez que hay un patrón que se sale de lo normal que hemos tenido en cada uno de los clientes creo que es algo que, obviamente se ha hablado mucho de ello y no es nada nuevo, pero todavía está por aplicar en muchos sitios”.

Compartir en RRSS

Síguenos en:

CIFRADO HARDWARE
EN EL ÁMBITO FINANCIERO

cryptosec LAN

realsec
La clave para proteger su negocio

www.realsec.com

HSM con el mayor rendimiento transaccional del mercado

- Incluidos todos los algoritmos de cifrado simétricos y asimétricos **(sin costes adicionales ocultos).**
- Autenticación de doble factor para cumplimiento PSD2 e integración con soluciones de Blockchain.
- Certificación FIPS 140-2 level 3 del NIST y la Certificación PCI PTS HSM v2.0. del PCI Security Standards Council.

it Digital Security
Entrevista

‘Nuestra apuesta es que la seguridad sea algo transversal, desde el principio hasta el final’

(María José Talavera, VMware)

El próximo hará diez años en VMware, una empresa con una gran evolución y cuatro pilares capaces de cubrir las necesidades de una empresa, incluidas las de seguridad. Dice María José Talavera que la compañía ha conseguido crear una plataforma sólida para dotar de infraestructura a cualquier modelo de servicios cloud, que la pandemia ha reforzado la estrategia de VMware, que hay que hacer frente a la escasez de talento y que, aunque tardaremos en verlo, los productos de seguridad como tales desaparecerán.

Rosalía Arroyo

Fundada en el mundo de la virtualización, tanto de estaciones de trabajo como de servidores para entornos Windows y Linux, VMware evolucionó al ritmo del mercado virtualizando no sólo las cargas de trabajo sino el almacenamiento, con VSAN, y las redes, con NSX, y creando conceptos como el Software Defined DataCenter (SDDC). Los últimos años la estrategia de la compañía se ha centrado en cuatro pilares: el SDDCD moderno, la integración entre nubes públicas y privadas, la seguridad intrínseca y ofrecer acceso a los usuarios desde cualquier dispositivo, en cualquier momento y desde cualquier lugar.

Con más de 26 años de experiencia en el sector TI, María José Talavera es, desde marzo de 2012, la directora de VMware tras su paso por Compuware o IBM. Hablamos con ella de seguridad, del valor de su compañía, el impacto de pandemia, la escisión de Dell o cómo ve el futuro mercado de la seguridad.

VMware ha sufrido una enorme evolución desde su nacimiento en 1998 en el mercado de virtualización hasta ser una empresa que se mueve bien en el mercado de seguridad. ¿A qué se dedica VMware?

No somos una empresa de seguridad al uso, pero tenemos un concepto de seguridad intrínseca que nos permite velar por la seguridad de la carga de trabajo, esté donde esté. A lo largo de estos 23 años y empezando por la virtualización, la compañía ha conseguido crear una plataforma sólida para dotar de infraestructura a cualquier modelo de servicios cloud. Y como queremos ser una plataforma sólida que provea todo, incluida la seguridad, tenemos que hacer inversiones en seguridad, sobre todo cuando las compañías empiezan a decidir sobre su estrategia multi cloud. Estas inversiones son de todo tipo y en todos los productos. Aunque quizá la más específica fue la de Carbon Black para añadir seguridad en el endpoint, también hay que recordar la de Nicira, que desde hace mucho tiempo es NSX, y la compra de VeloCloud, que implica establecer seguridad a lo largo de la red.

"Soy una firme convencida de que el mercado está tan sumamente fragmentado que cada vez resonará más la idea de la seguridad intrínseca, de algo que sea transversal"

Por otra parte, con Workspace One nosotros intentamos proveer una plataforma digital de puesto de trabajo que interioriza el concepto de que el trabajo es lo que uno hace y no desde donde uno lo hace. Cuando ese dónde no es necesariamente en la oficina, la posibilidad de poder trabajar desde cualquier punto implica también añadir capacidades de seguridad a la plataforma digital de trabajo.

Por otra parte, entendemos que el concepto Datacenter va más más allá de lo que es el propio centro de proceso de datos y que se puede extender a cualquier nube con todas las capacidades, con los mismos niveles de seguridad y políticas de seguridad, con las mismas operaciones, etcétera. Secure State se ha lanzado para garantizar también la seguridad en la nube pública.

¿Qué impacto ha tenido la pandemia en las demandas de los clientes en la estrategia de VMware?

La pandemia ha venido a hacer dos cosas fundamentales. La primera es darle la visibilidad y la enjundia que IT se merece en la transformación del negocio que todas las compañías y las administraciones públicas estaban abordando desde hace ya

"El spin-off de Dell Technologies nos aporta es mucha más libertad, flexibilidad y agilidad, tanto de definición como de ejecución de la estrategia"

algunos años. Es decir, darle una relevancia que le correspondía por derecho y que ha obtenido desgraciadamente por una situación absolutamente anómala y que nadie era capaz de prever.

Y el segundo efecto es que ha venido a reforzar la estrategia de VMware. La estrategia de la compañía en cuanto a visión tecnológica y desarrollo de soluciones no ha cambiado. La pandemia ha venido a reforzar que el portfolio de VMware es un 'must to have', que es algo que todas las compañías deben contemplar, con o sin nosotros.

¿Qué está fomentando VMware?

Nosotros abogamos por una fuerza de trabajo distribuida y por una libertad de elección de dónde quieres tener tus cargas de proceso de datos, bien sea on premise o en la nube pública. Y cuando hablamos de nube pública, hablamos de libertad de elección, de tener realmente una estrategia multi cloud, de poder mover tus cargas y tus datos alrededor de todas las nubes y de tu propio datacenter sin que eso cambie tu operación, tus políticas de seguridad, etcétera.

Nuestra apuesta es que la seguridad no es solamente un producto o una solución, sino que tiene que ser algo transversal desde el principio hasta el final. Y lo que ha dejado claro la pandemia es que, al volverse todo más digital, las superficies de ataque se multiplican. La misma digitalización hace que puedas moverte de un sitio a otro a golpe de ratón y que la competitividad entre las empresas sea mucho mayor, y si no tienes una plataforma digital sólida, puedes perder clientes sin ningún problema.

El año pasado fue el de las grandes implantaciones de soluciones de todo tipo, ¿2021 es el año de la consolidación? ¿se frena la inversión?

Es verdad que hay que revisar y consolidar, sobre todo si se ha tenido una estrategia un poco a bandazos, que es lo que yo creo que ocurrió al principio de la pandemia, pero no hay que parar. Yo creo que vivimos tiempos en los que al mismo tiempo que revisas tienes que seguir construyendo a futuro. Ahora es cuando tenemos que estar definiendo las

nuevas plataformas digitales, tanto para las aplicaciones existentes como para las nuevas aplicaciones, porque, si no somos capaces de empezar a trabajar ahora en lo que va a venir después, nos volverá a pasar algo parecido a la pandemia. Hemos tenido tiempo para revisar y sobre todo para aprender la lección de que hay que planificar a futuro con tiempo.

Entre otras cosas hay que hacer frente a la escasez de talento. Hay que atraer talento, pero no solamente el talento joven. También un talento más mayor que puede trabajar desde otro punto que no sea la oficina, que tiene más posibilidades de llevar una conciliación a cabo como Dios manda, con sus tareas o responsabilidades personales o familiares, que además sabe que estaría bien no contribuir a la contaminación en las ciudades por el transporte. Hay que empezar a pensar en el acceso a un puesto de trabajo para gente que tenga ciertas discapacidades de movilidad física, empezar a pensar en que puedes atraer talento que puede estar incluso en otro país.

Algo tan importante como es la inclusión de género también es importante. Yo creo que las mujeres hemos sido las grandes beneficiadas de la posibilidad de tener un puesto de trabajo flexible en cuanto a dónde desarrollas el trabajo; nosotras lo hemos aprovechado más, o lo hemos necesitado más, o lo demandamos más. Y todo esto hay que hacerlo, no porque vaya a venir otra crisis sanitaria, sino porque el mundo va evolucionando.

Creo que estamos en la era en la que debemos intentar modernizar nuestros centros de proceso de datos, modernizar nuestras aplicaciones existentes y empezar a desarrollar aplicaciones cloud nativas, porque las aplicaciones son las que dominan el mundo. Las empresas que son competitivas son las que tienen aplicaciones accesibles y amigables para los consumidores, porque en función de la experiencia de la aplicación los usuarios deciden incluso cambiar de compañía.

¿Y la experiencia del empleado?

También es importante. Si el empleado de una tienda física es amable y está contento, es más probable que compres que si no te atienden bien. Tener empleados contentos redunda muy positivamente en el éxito de cualquier compañía, y nos hemos dado cuenta de que la experiencia del empleado no se reduce a ir físicamente a una oficina, sino que se amplía a todas las posibilidades de interacción que tiene esa persona con la compañía o con los clientes a los que gestiona, o con los partners con los que colabora. Puede ser en cualquier momento y en cualquier lugar, que es la misma propuesta que plantea VMware cuando dice “Any App. Any cloud. Any Device”, un mensaje

"Tener empleados contentos redunda muy positivamente en el éxito de cualquier compañía"

que no ha cambiado desde hace varios años y es más válido que nunca.

¿Cuál crees que es el valor diferencial de VMware?

Que siempre estamos pensando en el cliente. Por ejemplo, el concepto de Seguridad Intrínseca viene a ser una cosa tan sencilla como simplificar el espectro de eventos que hay alrededor de la seguridad. Las empresas gestionan decenas de soluciones de decenas de fabricantes de seguridad diferentes, lo que añade una complejidad tremenda. No dudo de que todos y cada uno de ellos de forma individual sean buenos, pero el problema es la interoperabilidad y la trazabilidad cuando tienes un problema serio. Siempre hemos pensado en que la seguridad es algo tan importante que debería ser algo intrínseco a todo.

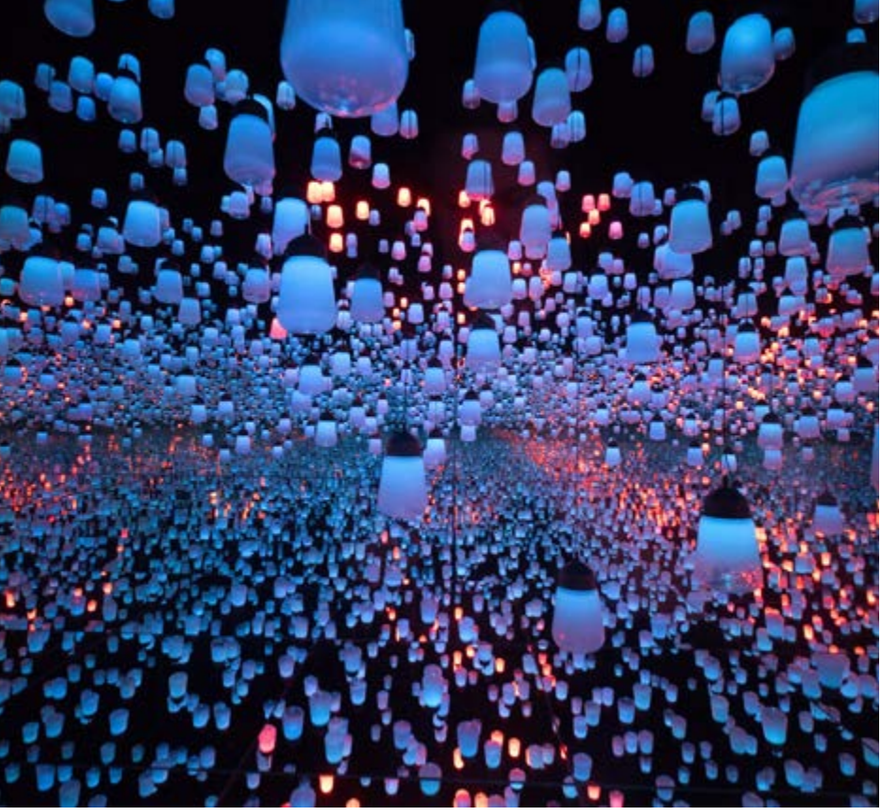
Otro de los focos es la libertad de elección. Hemos trabajado desde hace muchos años para que los clientes pudieran tener una estrategia de cloud lo más abierta posible que pudiera ser en on premise o abierta a la cloud pública. Y dentro de la cloud pública les hemos dado las opciones de los grandes hyper scalers para que pueda decidir cómo quieren gestionar su estrategia multicloud.

"Seguiremos trabajando en dar opciones de flexibilidad a nuestros clientes"

¿Cuál es el futuro de VMware?

La estrategia se mantiene y se seguirá reforzando porque las áreas en las que vamos a seguir invirtiendo seguirán siendo el puesto de trabajo, porque es una demanda a nivel mundial y entendemos que es algo clave y necesaria para la mayoría de las organizaciones y de las instituciones públicas.

También vamos a seguir invirtiendo en el concepto de seguridad intrínseca y en la libertad de elección en general, que es el fundamento de Cloud Universal, un producto multi-nube mediante suscripción que brinda prestaciones flexibles de gestión e infraestructura de nube de VMware a entornos de nube pública, privada o local. Es decir, seguiremos trabajando en dar opciones de flexibilidad a nuestros clientes, no solamente en con quién quieren trabajar, sino también cuál es el modelo de compra por el que quieren optar.



"Las aplicaciones son las que dominan el mundo"

¿Cuál es el impacto del nombramiento del nuevo CEO y de la separación definitiva de Dell Technologies?

Raghu Raghuram viene a reforzar que no habrá grandes cambios después del spin-off, sino que continuaremos con nuestra estrategia. El nuevo directivo está en VMware desde 2003, es decir que lleva muchísimo tiempo con nosotros y ha hecho contribuciones muy importantes, como ha sido el concepto de Software Defined Datacenter para virtualizar no solo la capacidad de cómputo, sino las redes, el almacenamiento, las operaciones. Él fue el gran cerebro de todo esto y ha trabajado mucho en preparar a la compañía para esa transformación hacia el modelo SaaS, con lo cual tiene un perfil magnífico para liderar la empresa. Que sea alguien de dentro y tenga un histórico con nosotros nos ayuda a mantener una continuidad de estilo, de compromiso, de valores.

En cuanto al spin off, se anunció hace un año y se ha ido preparando el terreno. Lo que nos aporta es mucha más libertad, flexibilidad y agilidad, tanto de definición como de ejecución de la estrategia. Somos una compañía de software, y para una compañía de software es muy importante definir la estrategia a largo plazo.

¿Cómo ve María José Talavera el mercado de ciberseguridad? ¿hacia dónde vamos?

Es un mercado que va a ser cada vez más grande. Primero, porque cuanto más se digitaliza el mundo, más crece la superficie de ataque y por lo tanto la seguridad será cada vez más importante. En la medida que es un mercado creciente debería consolidarse porque si no añadimos complejidad. Al mismo tiempo es un mercado que tiene que ser muy innovador, y volvemos a que el problema de la innovación es la complejidad, y poder abordar la innovación sin complejidad requiere de mucha simplificación.

Por otra parte, soy una firme convencida de que el mercado está tan sumamente fragmentado que cada vez resonará más la idea de la seguridad intrínseca, de algo que sea transversal. Incluso yo me atrevería a decir, y esto es muy visionario y no sé si lo veremos, que los productos de seguridad como tales desaparecerán.

Enlaces de interés...

- VMworld 2020: Planteando la base digital para el negocio en un mundo cambiante
- VMware busca reforzar la seguridad de las aplicaciones con la compra de Mesh7
- 'El teletrabajo se convierte en requisito esencial de los empleados' (VMware)
- 'Lo que cambia radicalmente el panorama es el análisis por comportamiento y no basado en firmas' (Carbon Black)

Compartir en RRSS

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

Los **equipos de investigación de amenazas de SonicWall Capture Labs** proporcionan a las empresas, pymes, agencias gubernamentales y otras organizaciones inteligencia de ciberamenazas existentes para proteger a su personal distribuido contra una superficie de ataque en continua expansión.

Al proporcionar una visión completa de estos datos, el ***Informe de Ciberamenazas 2021 de SonicWall*** muestra cómo piensan y operan los cibercriminales, ayudando a las organizaciones a prepararse mejor para las amenazas del futuro.

OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

▼ 43%

EL MALWARE CAE AL NIVEL MÁS BAJO DESDE 2014

+ 1 días

IDENTIFICACIÓN MÁS RÁPIDA DE MALWARE "NUNCA ANTES VISTO"

▲ 62%

EL RANSOMWARE ALCANZA UNA CIFRA RÉCORD

▲ 74%

INSPECCIÓN DE MEMORIA PROFUNDA MEJOR QUE NUNCA

▲ Máx. 3 años

EL CRYPTOJACKING HA VUELTO

▲ 66% IOT

EL MALWARE DE IOT AUMENTA UN 66%

▲ 20%

INTENTOS DE INTRUSIÓN EN CONSTANTE CRECIMIENTO

it Digital Security

Desayuno ITDS

XDR, la detección y la respuesta mandan

El panorama de amenazas continúa evolucionando. Cada vez son más y más sofisticadas y las tecnologías de seguridad tienen que ir avanzando para hacerles frente. No hace mucho que el EDR, el Endpoint Detection and Response, se ha impuesto en el mercado, pero ya aparece la siguiente evolución que es el XDR, Extended Detection and Response, que centra este debate en el que participan Alexandre Tovar, Channel Account Manager de Trend Micro Iberia; Julián Domínguez, Ingeniero Preventa para España y Portugal de Varonis; Francisco Valencia, CEO de Secure&IT; Jesús Díaz Barrero, Systems Engineer Spain & Portugal de Palo Alto Networks; Alberto Ruiz Rodas, Presales Engineer for Spain and Portugal de Sophos y Luis Javier Suárez, Presales Manager de Kaspersky Lab.

Junio 2021

Qué es el XDR y qué viene a solucionar, a qué tipo de clientes está dirigido, qué retos plantea su adopción, por qué no hay que confundirlo con un SIEM son algunas de las preguntas que planteamos en este debate.

Kaspersky

"El XDR se plantea como un conjunto de herramientas que nos permiten dotar de más visibilidad y capacidades a las compañías", dice Luis Javier Suárez, Presales Manager de Kaspersky Lab para la región de Iberia. Asegura el directivo que los vectores de ataque han aumentado y que, para poder tener una visibilidad extendida, "tenemos que apoyarnos en este tipo de soluciones que vienen a complementar el mundo de EDR".

Durante una de sus intervenciones el portavoz de Kaspersky asegura que la adopción de este tipo de tecnologías permite tener una capacidad de detección y de respuesta que va mucho más allá de la seguridad tradicional "y se tiene que apoyar en cierto expertise o cierta dedicación por parte del cliente" porque "no sirve de mucho el hecho de que yo tenga una tecnología capaz de detectar algo si no tengo capacidad para tomar una acción".

Explica Luis Javier Suárez que, desde el punto de vista de fabricante, uno de los desafíos es hacer la tarea de integración mucho más fácil para que el cliente no tenga que preocuparse por tener que cambiar ciertos componentes dentro de su estrategia de seguridad.

"El principal desafío a la hora de adoptar una solución de XDR es entender hasta dónde puede llegar cada compañía a la hora de cubrir esa visibilidad", dice el directivo de Kaspersky. También hay que tener en cuenta las necesidades de cada empresa, porque no es lo mismo las que tiene un cliente que trabaja en el sector financiero a las que tiene una pequeña o media empresa

"No en el corto plazo", responde Luis Javier Suárez cuando le preguntamos si el empuje de XDR pone en peligro la existencia del EDR, que se sigue adoptando por parte de las empresas. Asegura también que la función del XDR no es la de suplantar al SIEM, "que sigue teniendo una importante funcionalidad".

Sophos

Para Alberto Ruiz Rodas, Presales Engineer for Spain and Portugal de Sophos, los XDR son la evolución natural del EDR. "Nosotros ya

DESAYUNOSITDS. XDR, LA DETECCIÓN Y LA RESPUESTA MANDAN

CLICAR PARA VER EL VÍDEO

proporcionábamos sistemas EDR, pero con XDR no solo vamos a tener la visibilidad de lo que sucede en los servidores y en los puestos de trabajo, sino que lo extendemos a todo el portfolio de productos".

"Desde Sophos tratamos de que este tipo de soluciones sea asequible a cualquier tipo de cliente y no sólo para empresas con personal especializado", dice Alberto Ruiz. Además, la versatilidad de la herramienta no sólo le hace útil para el departamento de seguridad, sino para el de operaciones.

En el caso de Sophos a la hora de implementar una solución de XDR se puede partir desde cualquier producto. Explica Alberto Ruiz que todos los productos de la compañía se manejen desde la consola Sophos Central, "que es desde donde se van a obtener las capacidades de XDR". Aun así, se trata de una herramienta que requiere de un

equipo dedicado, de expertise, y por eso también se ofrece bajo un modelo de servicio gestionado.

Para Alberto Ruiz, el reto de adoptar una solución de XDR es "usarla", y eso requiere gente que esté disponible para investigar, para estudiar las alertas y revisar los indicadores.

"No creo que el EDR muera. Para nosotros es la evolución", dice Alberto Ruiz cuando le preguntamos si el empuje del XDR pone en peligro la misma existencia de EDR. Habla el directivo de Sophos de una migración paulatina del EDR al XDR al tiempo que advierte que hay empresas que no tienen ni eso.

> "No creo que el EDR muera. Para nosotros es la evolución"
>
> Alberto Ruiz Rosa, Presales Engineer for Spain and Portugal, Sophos

A grandes retos, grandes soluciones

Para finalizar el debate pedimos a los expertos en seguridad que explique cuál es la propuesta de cada una de sus empresas en torno al XDR.

Kaspersky

La propuesta en torno a XDR de Kaspersky pasa por la recogida de diferentes evidencias, independientemente de su origen, así como la capacidad de análisis de las mismas y una correlación para que, con sistemas de inteligencia, poder contextualizar y enriquecer el incidente. Se ofrecen también herramientas extendidas, como las de Threat Hunting y monitorización así como la parte de respuesta, y todo ello con una sencilla integración con cualquier fabricante.

Sophos

El planteamiento de Sophos es un ecosistema adaptativo de seguridad basado en la consola Sophos Central desde la que se gestiona todo el portfolio de la compañía, una propuesta amplia que aporta numerosos indicadores e información que acaban en un data lake que permite a los equipos de threat intelligence y los SOCs proporcionar una respuesta coordinada a los incidentes de seguridad. Y todo ello nutrido con una serie de APIs para permitir la orquestación y la integración con terceros.

Palo Alto

El XDR de Palo Alto se integra con los elementos de red para ver si el movimiento de una gran cantidad de datos es anómalo o no, para lo cual hay un motor de analítica que de manera automática está correlando la información teniendo en cuenta el análisis de comportamiento. A través de una consola se investigará esa alerta para determinar si ese movimiento de datos es una exfiltración de datos sensibles o que un empleado está subiendo las fotos del verano a la nube.

Secure&IT

No siendo fabricantes, lo que hace Secure&IT es la implementación y aportar la inteligencia al cliente final en la gestión de su seguridad. Apuestan por fabricantes que les ayudan en cada uno de los pasos y se huye del modelo del fabricante que lo hace todo porque cree que nadie es bueno en todo, pero todo el mundo es bueno en algo. Las tareas de integración, la gestión de alarmas y las personas que están 24 horas en los SOCs analizando eventos y respondiendo ante ellos es el valor que aporta al mercado.

Varonis

La compañía complementa la protección del XDR desde el punto de vista de que se auditan todos los permisos que tienen los clientes para acceder a la información, protegen la información y son capaces de identificar qué información es importante y cuál, aprenden de lo que están haciendo los usuarios respecto a esa información. Varonis cuenta además con un equipo de respuesta ante amenazas en tiempo real y da visibilidad completa en un entorno híbrido, pudiendo detectar las alertas reales y realizar la investigación posterior.

Trend Micro

La compañía incluyó XDR en su plataforma Cloud One en 2020 por lo que los clientes ya tienen XDR como parte de la protección de sus servidores, correo electrónico y entornos colaborativos. Todo ello se gestiona desde la consola Vision One bien por parte del cliente y del canal de la compañía, que es un referente en cuatro áreas clave del XDR: detección, email, endpoint y cloud

"El XDR se plantea como un conjunto de herramientas que permiten dotar de más visibilidad y capacidades a las compañías"

Luis Javier Suárez, Presales Manager, Kaspersky Lab Iberia

Explica Alberto Ruiz que los XDR son diferenciales en cuanto al nivel de integración de sus productos en el despliegue, así también como el foco en la lo que sería la detección de amenazas y respuesta a incidentes.

Palo Alto

Cuando habla de XDR, Extended Detection and Reponse, a Jesús Díaz Barrero, Systems Engineer Spain & Portugal de Palo Alto Networks le gusta pensar en la X como en las incógnitas de las ecuaciones, de forma que se puede sustituir por la 'E' de Endpoint, por la 'N' de Network, o por la 'C' de cloud; "la idea es ser capaces de ofrecer sistemas de detección, de respuesta y de prevención que sean capaces de correlar la información desde cualquier punto", y hacerlo en un entorno heterogéno, que es el que normalmente nos vamos a encontrar con los clientes.

Asegurando que el objetivo de un XDR es un cliente empresarial, dice Jesús Díaz que no sólo hay que tener en cuenta el coste de la adquisición, sino de la operación, porque "no todos tienen el expertise necesario para poder desplegar o instalar una solución de este estilo", y añade que por eso hay distintas formas de trabajar con los XDR, "normalmente través de un partner que va a contar con la gente especializada para poder operar la solución".

A la hora de hacer frente al reto de adoptar una solución de XDR el primer paso es "ser consciente de los problemas que puede resolver XDR", además de intentar aprovechar al máximo las herramientas existentes para que sea lo más sencillo posible y los despliegues no se conviertan en un puesto de ingeniería costosísimo.

Saber encontrar la aguja en el pajar es, para el ejecutivo de Palo Alto, uno de los retos que plantea la adopción de un XDR. Para ello, explica, hay que trabajar en tres grandes áreas, por un lado los servicios, bien con capacidad propia o externalizándolos; otra área es que la propia herramienta cuente con mecanismos de identificación, simplificación

y agregación de eventos para intentar reducir ese ruido y facilitar el encontrar esa aguja en el pajar. Y el tercer punto es la automatización.

"El EDR tiende a desaparecer", dice el directivo de Palo Alto apuntando a que en todo caso el mercado se mueve en distintas velocidades y hay empresas a las que les costarán más tiempo llegar al XDR; "pero como concepto el EDR está muerto y no tiene sentido".

En determinadas ocasiones Jesús Díaz sí que ve el XDR como una alternativa al SIEM. Explica que Palo Alto ya está trabajando en algunos proyectos en los que se están moviendo parte de reglas que se estaban intentando implementar en los SIEM y que son complejas al mundo del XDR porque las da de manera automatizada.

Secure&IT

Dando un punto de vista u poco diferente "porque somos el SOC y no el fabricante", dice Francisco Valencia, CEO de Secure&IT, que el XDR "viene a solucionar la investigación que sucede después de que ha habido un incidente, y cuanta más información sea capaz de absorber y mejor haga la correlación, más fácil nos hace el trabajo de investigar un incidente cuando ha sucedido". En todo caso aclara que tanto EDR como XDR son tecnologías "que nos ayudan a identificar un ataque cuando ya se ha producido".

Diciendo que "como sector tenemos la obligación de democratizar la ciberseguridad porque todo el mundo tiene derecho a estar protegido", y que las empresas pequeñas son mucho más sensibles a las amenazas, asegura Francisco Valencia qua hay que transmitirles la sencillez de la solución. "Lo que necesitan las compañías

"El XDR es un paso totalmente natural para poder combatir los ataques multicapa"

Alexandre Tovar, Channel Account Manager, Trend Micro Iberia

"No todas las empresas tienen el expertise necesario para poder desplegar o instalar una solución XDR"

Jesús Díaz Barrero, Systems Engineer Spain & Portugal, Palo Alto Networks

son partners bien formados porque el problema de EDR y de XDR es que alguien tiene que estar mirando la pantalla y ellos no tienen recursos para hacerlo", añade el CEO de Secure&IT. Y esto es precisamente uno d los retos que plantea la adopción de una solución XDR: la necesidad de estar encima de ella porque no es algo que funcione solo ni de manera automática". Advierte también el directivo que en ocasiones las empresas lo instalan y no hacen nada más "y tienen la falsa sensación de estar protegido porque tienen algo más que un antivirus".

Sobre si el XDR pone fin al EDR, dice Francisco Valencia que la pregunta es análoga a si EDR puso fin al Endpoint Protection tradicional y que el XDR no elimina ni sustituye al EDR, sino que lo complementa.

Coincide Francisco Valencia con Jesús Díaz en que sí es cierto que ciertos clientes que no tiene un SIEM se pueden conformar con las funcionalidades que ofrece un XDR, "pero cuando ya tienes el SIEM implantado, la capacidad del SIEM en cuanto a analítica, recepción y correlación de eventos es muy potente".

Varonis

Asegurando que no "somos ni un EDR, ni un XDR tradicional", dice Julián Domínguez, Ingeniero Preventa para España y Portugal de Varonis, que la compañía ha trabajado en la misma estrategia de poder relacionar un montón de variables dentro del comportamiento de lo que está pasando en la red para llegar a detectar que, aunque el comportamiento sea normal o sea autorizado, está ocurriendo algo raro.

Tiene claro Julián Domínguez que en la época de transformación digital en la que estamos "cualquier

empresa de cualquier tamaño necesita un XDR", bien a través de recursos propios o contratando servicios "porque al final su negocio está en la digitalización y los ciberdelincuentes intentan hacerse con diversa información para luego pedir un rescate por ella".

En la propuesta de Varonis para que cualquier cliente pueda evaluar una solución de este tipo la compañía ofrece una prueba que permite obtener un informe de riesgos que le permite definir sus necesidades concretas de protección de la información; "es una manera muy sencilla y gratuita de poder analizar qué es lo que necesita para después ir más allá en las capacidades".

Destaca Julián Domínguez que uno de los retos a la hora de implementar una solución de XDR es el aprendizaje de lo que es sospechoso, aunque sea lícito, así como "el ajuste y parametrización de esas alertas y acciones corruptas en función de cada red y cada sistema".

"La evolución de las amenazas nos ha impulsado a establecer una nueva frontera de protección con el XDR", asegura Julián Domínguez, que no cree que el XDR termine sustituyendo al EDR, y que en realidad lo que hay que hacer es centrarse en estar protegidos, tener funcionalidades extendidas y que los nombres y siglas de las soluciones se irán cambiando.

La experiencia que tiene Julián Domínguez con los clientes que tienen un SIEM y a los que se les ha ofrecido la suite de la compañía es que hay tal cantidad de eventos que se reciben en el SIEM que es difícil saber diferenciar la amenaza. En todo caso asegura que la integración XDR/SIEM/SOAR "es fundamental para dar una protección más amplia".

"La evolución de las amenazas nos ha impulsado a establecer una nueva frontera de protección con el XDR"

Julián Domínguez, Ingeniero Preventa para España y Portugal, Varonis

"Como sector tenemos la obligación de democratizar la ciberseguridad porque todo el mundo tiene derecho a estar protegido"

Francisco Valencia, CEO, Secure&IT

Trend Micro

"El XDR es un paso totalmente natural para poder combatir los ataques multicapa", dice Alexandre Tovar, Channel Account Manager de Trend Micro Iberia. Explica que el EDR solo cubre la parte del endpoint y que en un Digital Work Place "no podemos obviar otros vectores como el email, la navegación web, los dispositivos móviles". Añade de Alexandre Tovar que es necesario unificar la detección y la respuesta y que un verdadero XDR "extiende sus capacidades al multi cloud, a la red, a los servidores, de tal manera que permite tener trazabilidad de un ataque haya empezado donde haya empezado y se mueva por donde se mueva".

Afirmando que cualquier organización debe hacer esa transición de una seguridad por silos hacia una seguridad integral que contemple el máximo número de capas posible dice Alexandre Tovar que "no hay un tipo de organización a la que XDR encaje y otra a la que no".

Enlaces de interés...

- Las empresas no están satisfechas con el retorno de la inversión de su SOC
- De EDR a XDR: es la propuesta del nuevo servicio gestionado de Trend Micro

"Mi recomendación es huir de la falsa sensación de control que nos dan muchas veces ciertas auditorías o ciertos frameworks que evalúan la seguridad de cada una de las partes de la infraestructura de una organización de manera independiente", dice Alexandre Tovar cuando planteamos qué necesita una empresa que quiere implementar un XDR. Detrás de tal afirmación está el hecho de que XDR implica que es necesario "ver como un todo la estructura de la organización, empezar a pensar cómo unificar las diferentes piezas para obtener la máxima visibilidad".

A la hora de adoptar una solución de XDR hay que "entender que vas a necesitar personal que pueda centrarse en esas alertas que va a destacar el XDR", dice Alexandre Tovar advirtiendo que "es relativamente fácil caer en la tentación de pensar que todo va a ser automático".

Respecto a si el XDR desplazará al EDR dice Tovar que este último "no puede dar cobertura ni respuesta a los ataques actuales, ni va a responder ante un ataque que entre por un vector que no controle, ni tampoco va a ser capaz de detectar muchos movimientos laterales, ni intrusiones dentro de la red". Dice también que el XDR "viene a reducir y refinar la cantidad de alertas que recibe un SIEM, de tal manera que se pueden reducir muchísimo los plazos para que el equipo de respuesta incidentes pueda actuar".

Compartir en RRSS

CloudGuard

Check Point CloudGuard proporciona seguridad nativa en la nube unificada para todos sus activos y cargas de trabajo, lo que le brinda la confianza para automatizar la seguridad, prevenir amenazas y administrar la postura, en todas partes y en todo su entorno.

Más información:

www.checkpoint.com/es

Check Point®
SOFTWARE TECHNOLOGIES LTD

it Digital Security

Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?

Junio 2021

Seguridad proactiva, ¿hasta dónde estás dispuesto a llegar?

La seguridad proactiva es un enfoque más holístico para proteger los sistemas de TI. Se centra en la prevención más que en la detección y la respuesta y es una aproximación que gana peso en las empresas. Según el informe Cyber Risk Alliance, Cybersecurity Resource Allocation and Efficacy Index (CRAE) del segundo trimestre de 2020 las empresas con 500 o más empleados en América del Norte y Europa enfatizaban las medidas de seguridad proactivas para proteger los activos y detectar infracciones, en contraposición a un enfoque de seguridad puramente reactivo.

Un enfoque de seguridad proactivo consiste en comprender dónde se encuentran las vulnerabilidades para poder mitigarlas. La concienciación de los usuarios es una de las medidas de seguridad proactivas que deben tenerse en cuenta ya que permite adelantarse a una ingeniería social u otros ataques de phishing al garantizar que una base de usuarios sabe cómo detectar los signos y trucos reveladores de los estafadores.

Otras medida proactiva son las pruebas de penetración, la monitorización de endpoints y redes o el uso de tecnologías como el Threat Hunting

LA VISIÓN DE LAS EMPRESAS LA VISIÓN DE LA INDUSTRIA IT

itds

Encuentros ITDS

ENCUENTROS ITDS - SEGURIDAD PROACTIVA

CLICAR PARA VER EL VÍDEO

y la inteligencia de amenazas. Los avances en aprendizaje automático están ayudando a que las medidas reactivas sean más proactivas al reducir los falsos positivos y negativos.

Una cosa importante a tener en cuenta es que las regulaciones de protección de datos a menudo exigen un enfoque proactivo de la seguridad. El RGPD de la UE, por ejemplo, requiere un enfoque de "privacidad por defecto y diseño" para la protección de datos, esperando que la protección de datos se integre en un sistema.

Pero lo más importante es que la seguridad proactiva funciona, ya que según el informe CRAE las organizaciones que apuestan por un enfoque proactivo de la ciberseguridad se sentían más seguras de que las medidas funcionaban.

Con el fin de saber lo que está ocurriendo en la empresa española IT Digital Security ha organizado un nuevo Encuentros ITDS bajo el título "Seguridad Proactiva, ¿hasta dónde estás dispuesto a llegar?", en el que han participado Ignacio Pérez, CISO, Aragonesa de Servicios Telemáticos (AST) (Gobierno de Aragón); Judit Closa Ribalta, CISO de Habitissimo; Joan Massanet, CTO y CISO de Maximice Events Group; Mónica de la Huerga, CISO de Sopra Steria; José Luis Paramio Martínez, CISO de Userlytics; Raül Albuixech Gandia, director de servicios y soporte técnico de ESET España; Raúl Dopazo, Arquitecto de Soluciones de One Identity; Francisco Valencia Arribas, Director General de Secure&IT; Sergio Martínez Hernandez, Country Manager Iberia de SonicWall y Raúl Nuñez Herrero, Ingeniero Preventa de Trend Micro.

LA VISIÓN DE LAS EMPRESAS

AST Gobierno de Aragón. Ignacio Pérez, CISO

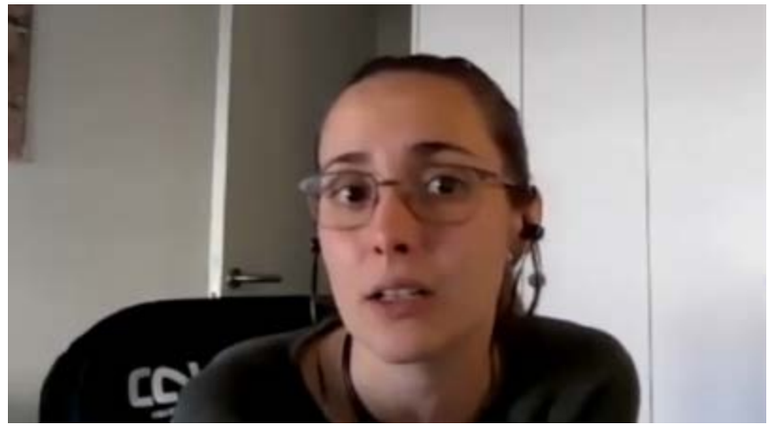
El control de la superficie de exposición es una de las principales preocupaciones de Ignacio Pérez, CISO de AST (Aragonesa de Servicios telemáticos) del Gobierno de Aragón, quien es el responsable de todos los elementos TIC de la región “con un modelo de negocio complicado porque nada tiene que ver un centro de salud con un juzgado o una oficina de empleo” y por lo tanto dónde poner las capas de seguridad en cada momento “es uno de los grandes quebraderos de cabeza” a los que se enfrenta.
Para Ignacio Pérez la proactividad en la seguridad no está tanto en la tecnología como en el proceso. Apuesta por la inteligencia, “tanto en la adquisición, en el Threat Intelligence de donde sacamos nuestras fuentes, como en el análisis que hacemos de ello, y en la respuesta”, y asegura que, en

"El Threat Hunting nunca va a ser un producto"

Ignacio Pérez, CISO, AST

la medida en que somos capaces de automatizar alguna de estas fases, ganamos en rapidez, “pero al mismo tiempo no puedes quitar el factor humano del que está indagando”.
Asegura este CISO que es tanto la capa tecnológica que te facilita una respuesta mucho más rápida de lo que podrías hacerlo con humanos, como la capacidad de tus procesos que te permiten detectar esos problemas
“El Threat Hunting nunca va a ser un producto. No puede serlo por su naturaleza”, dice Ignacio Pérez, quien asegura que el coste de llevar la securización a todas las superficies de exposición es inasumible; “para que sea viable hay que adecuar el nivel de securización al ámbito que quieres proteger, no es lo mismo un centro de educación secundaria que el centro de protección civil 112”.
Al final se pone el foco en dos cosas: la información y los servicios esenciales; “y para mí la información es muy importante, pero que no se me caiga la monitorización de las UCIs también, y ahí no hay ningún dato especialmente relevante”.

“Yo pediría sobre todo sinceridad”, dice Ignacio cuando se le plantea qué pediría a los fabricantes o proveedores de servicios; “dime lo que hace y cómo lo hace”. Menciona también la orquestación unificada como un Santo Grial y “el compromiso, el soporte, el acompañamiento”.



HABITISSIMO. Judit Closa, CISO

“Siempre habrá nuevas amenazas y superficies de exposición no controladas, y el poder priorizar, el poder escalar el riesgo para que la situación se asuma a nivel de negocio es el paso principal”, dice Judit Closa, CISO de habitissimo, añadiendo que amenazas concretas como el ransomware, o el phishing más básico, son algunos de los retos a los que se enfrentan los responsables de ciberseguridad de las empresas.

"La monitorización es lo que te ayuda a tener una postura de seguridad más proactiva"

Judit Closa, CISO, HABITISSIMO

Para Judit Closa, "todas las tecnologías que tengan que ver con la monitorización de tu red, de tus activos", son las que ayudan adoptar una postura de seguridad más proactiva. Añade la directiva de habitissimo que "tener tu superficie de exposición más controlada implica que la tengas bajo monitorización, con un centro de operaciones que te responda en unos tiempos adecuados para tus requerimientos de negocio".

Sobre el Threat Hunting y la Deception, que son tecnologías que buscan cazar y poner trampas al ciberdelincuente, dice Judit Closa que no es que la empresa española no esté preparada para su uso, sino que se incluye dentro de actividades de inteligencia, o que son parte de los servicios de monitorización que te puede dar un SOC, y no algo que habitualmente se haga de forma aislada.

Destaca Judit la importancia de la comunicación, tanto con los usuarios como con las juntas directivas y los propios proveedores mencionando que debe quedar muy claro lo que se está incluyendo en un servicio, a veces saturado de añadidos que te van dando funciones diferentes. "Hay que fortalecer la comunicación, tanto pre-venta como post-venta, y los lazos que hay con los servicios de soporte, que deben ser próximos", dice la CISO de habitissimo, añadiendo que siempre cuesta conseguir que un proyecto llave en mano realmente se acabe implementando bien, porque cada empresa se organiza de una forma diferente.

"La comunicación es básica para cualquier tipo de relación, así como asegurar unas buenas implementaciones", concluye Judit Closa.

MAXIMICE EVENTS GROUP. Joan Massanet, CISO y CTO

"Los ataques de ransomware están siendo nuestra gran preocupación", dice Joan Massanet, CTO y CISO, Maximice Events Group. Apunta dos motivos: el cifrado de datos en sí mismo y la denegación de servicios que conlleva.

"Es el soporte lo que aporta el valor a la solución"

Joan Massanet, CTO y CISO, Maximice Events Group

"La herramienta perfecta para los CISO sería una calculadora de ROI que nos diera siempre positivo porque al final todo se basa en el beneficio que va a generar y no es los gastos", asegura Joan Massanet, añadiendo que a nivel tecnológico y como herramienta diaria apuesta por los IRM (Information Rights Management) para la gestión de los datos y los documentos. Hablando de datos, "la extorsión es una de las cosas más graves que nos puede pasar porque si el cliente pierde confianza en ti, ahí ya no puedes tener ingresos de ningún tipo".

Otras tecnologías que destaca Massanet son las herramientas de parcheado virtual de vulnerabilidades y "el XDR para poder visibilizar los ataques dentro de nuestra propia red".

Apunta también el CISO de Maximice Events Group que le preocupa el uso de la inteligencia artificial en los ciberataques y la computación cuántica "capaz de romper cualquier cifrado en cuestión de segundos", con la consiguiente pérdida de confidencialidad.

Ahora lo que importante es el dato y creo que la arquitectura Zero Trust es algo que deberíamos implementar todos

La interoperabilidad es algo que hace muchísima falta, “sobre todo cuando hablamos de recoger toda esa información, juntarla y saber qué está pasando”, dice Joan Massanet, quien pediría a los fabricantes reducir la cantidad de información para poder ir al grano de lo que hace un producto. Menciona también el tema de los costes de las soluciones y los presupuestos con los que se trabajan en las empresas puntualizando que no cree que haya un producto mejor que otro y que “es el soporte lo que aporta el valor a la solución”.

SOPRA STERIA. Mónica de la Huerga, CISO

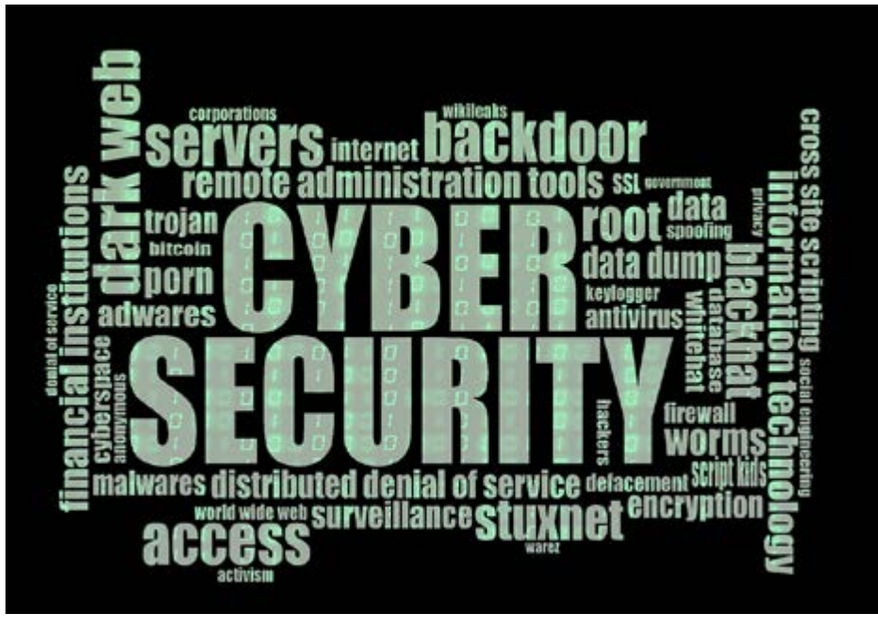
Además de prevenir los ataques de ransomware “lo importante es proteger el dato, que es el objetivo”, dice Mónica de la Huerga, CISO de Sopra Steria,

"En España estamos en la fase del EDR"

Mónica de la Huerga, CISO, SOPRA STERIA

cuando preguntamos cuáles son los retos a los que se enfrentan los responsables de ciberseguridad. Haciendo referencia a la pandemia, “que pensábamos que eran 15 días y llevamos ya año y medio”, también se ha convertido en un reto el control de los accesos “porque el perímetro que antes teníamos bien acotado se ha ido a las casas de nuestros colaboradores y proveedores, y es un poco más difícil de controlar, gestionar y verificar”. Añade Mónica de la Huerga que el control de la cadena de suministro es otro de los aspectos que los responsables de ciberseguridad de las empresas deben tener muy en cuenta.

Cada uno debe saber muy bien cuáles son los riesgos, alinearlos con los objetivos de negocio y adecuarse a los presupuestos, dice Mónica de la Huerga. Añade la CISO de Sopra Steria que se debe evitar caer en una avalancha de datos que te impidan hacer tu trabajo y encontrar la aguja en el pajar. Coincide con el resto de ponentes en el que el factor humano se debe tener en cuenta, porque por muchas medias tecnológicas que tengas “si al



final me llega un intento de phishing y hago clic en el enlace porque voy con prisa, ya han superado una de las capas de seguridad”.

“El Threat Hunting lo hacemos modularizando en función del análisis de riesgos, de ese presupuesto que nos validan, etc.”, dice Mónica de la Huerga. Añade que no sólo hay que tener en cuenta la búsqueda de vulnerabilidades, sino el poder desplegar todas las soluciones para corregirlas, el poder detectar una vía de ataque y eliminarla, “y eso como tal no lo estamos haciendo en España. Estamos en la fase de EDR”.

Un dashboard unificado y simplificado, “que casi sea como un semáforo de rojo, verde y porque tenemos muchas soluciones de diferentes fabricantes y la interoperabilidad no es tan simple” es algo

que pediría a los fabricantes. Añade que analizar qué información es importante o no es complicado cuando tienes un entorno complejo, y que lo que diferencia un producto de otro es el soporte; “no digo que todos sean exactamente iguales pero el diferencial es el soporte que te dan, ese acompañamiento para poder aprender a sacar el máximo partido a esas soluciones que has comprado”.

USERLYTICS CORPORATION. José Luis Paramio, CISO

Además del del phishing, el ransomware..., “cambiar los usos y costumbres de algunos empleados es uno de los retos a los que yo, por lo menos personalmente, me enfrento”, dice José Luis Paramio, CISO de Userlytics Corporation. Dice también que seguridad es la palabra de moda y está en boca de todos, “aunque cuando la pronuncien no sepan la carga que lleva detrás” y que “la cantidad ingente de oferta en herramientas y en soluciones de seguridad” es otro de los retos a los que deben enfrentarse los responsables de ciberseguridad. El presupuesto, asegura, es importante, tanto como acertar con la herramienta que necesita la empresa.

Para una empresa como Userlytics Corporation, con presencia en Miami, Tejas, Portugal, Madrid, Taiwán... “la mejor tecnología es la nube”, dice José Luis Paramio. Trabajar en la cloud “nos permite acotar bastante la superficie por la que podemos ser atacados, y además el tipo de alertas al que tenemos que estar pendiente”. Se añade que la compañía que protege realiza cursos y pruebas sobre ciberseguridad de manera periódicos, porque más que la tecnología a veces son las personas las que tienen que ayudar.

Ante la pregunta de qué le pediría a un fabricante o proveedor de servicios, hace referencia José Luis Paramio a la cantidad de información que se aporta asegurando que “un exceso de información es absolutamente inservible”. Afirma que una cuantiosa información te vale cuando ya tienes una experiencia con el producto en sí y menciona también curvas de aprendizaje algo elevadas. El resultado

es que las empresas contratan el producto que ya conocen y con el que ya tienen experiencia sus empleados, “o bien contratan al empleado que tiene experiencia con el producto que han contratado, o lo subcontratan todo a un tercero”.

Finaliza pidiendo más capas de abstracción, el hacer más sencillas las soluciones y el que se puedan hablar entre ellas, “porque yo abro cada mañana mi navegador y tengo 14 pestañas en lugar de un solo dashboard con toda la información”. Resumiendo: compatibilidad entre las soluciones, servicios unificados y más capa de abstracción.

"La mejor tecnología de seguridad es la nube"

José Luis Paramio, CISO, Userlytics Corporation

LA VISIÓN DE LA INDUSTRIA IT

ESET ESPAÑA. Raül Albuixech, director de servicios y soporte técnico

"Los fabricantes llevamos tiempo trabajando en la creación de soluciones y herramientas para ser algo más que un simple antivirus basado en firmas", dice el director de servicios y soporte técnico de ESET España. Añade que las empresas son cada vez más conscientes de que hace falta adoptar medidas de seguridad adicionales y que, además de visibilidad e inteligencia, la seguridad proactiva necesita la educación del usuario final, una educación "que solucionaría la gran mayoría de incidencias habituales.

Menciona el problema del presupuesto asegurando que, aunque los fabricantes ofrezcan mejores herramientas y mejores soluciones a un mejor precio, "hay tantos frentes de batalla que es imposible llegar a cubrirlos todos y hay que priorizar". El último punto para adoptar una seguridad más proactiva es la educación del usuario final; "educar en una buena praxis a la hora de trabajar con datos e información sensible".

Para Raül Albuixech, tan importante es crear herramientas o soluciones que te brinden toda la información posible como piezas herramientas estén bien optimizadas y bien configuradas para que puedas extraer el 100% de los datos que tienes. Añade que los fabricantes deben crear soluciones

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE ESET

CLICAR PARA VER EL VÍDEO

"Además de visibilidad e inteligencia, la seguridad proactiva necesita la educación del usuario final"

Raül Albuixech, director de servicios y soporte técnico, ESET España

de inteligencia, “pero sobre todo crear soluciones que puedan extraer la aguja en un pajar de manera automatizada”.

Por otra parte, de poco vale implementar una solución y olvidarse de ella, por lo que destaca la importancia de los servicios que se ofrecen durante la vigencia del contrato o licencia, no sólo relacionados con la configuración, puesta en marcha y optimización, sino en lo que se refiere a la monitorización y comprobar que todo está funcionando bien.

En opinión de Raül Albuixech el Threat Hunting no ha empezado a despegar en España, donde la palabra de moda es EDR. Añade que le quedan algunos años para que su uso esté más generalizado y que habrá diferentes formas de consumirlo, ya sea en un modelo directo o a través de un servicio

ONE IDENTITY. Raúl D’Opazo, Arquitecto de Soluciones, consultor de Ventas EMEA

Confirma el portavoz de One Identity que sí se está viendo una seguridad más proactiva en las empresas al tiempo que asegura que el discurso debe ir por hablar de prioridades y aplicar estrategias de seguridad, “y no tanto de comprar una solución, implementarla en tres meses y olvidarte”. Menciona algunas de las barreras que frenan esa proactividad, como es no involucrar al negocio o a recursos humanos, “o a cualquier departamento que realmente sea el propietario de los datos que nosotros queremos proteger desde el punto de vista tecnológico”.

También comenta Raúl D’Opazo durante su intervención que en ocasiones los proyectos se quedan en unas capas tan básicas que “esa idea de crear algo más proactivo es muy

"No involucrar al negocio o a recursos humanos frena la proactividad"

Raúl D'Opazo, Arquitecto de Soluciones One Identity

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE ONE IDENTITY

CLICAR PARA VER EL VÍDEO

itds

Encuentros ITDS

LA VISIÓN DE LAS EMPRESAS | **LA VISIÓN DE LA INDUSTRIA IT**

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE SECURE&IT

CLICAR PARA VER EL VÍDEO

"La tecnología que más ayuda a la prevención es la visibilidad"

Francisco Valencia, CEO, Secure&IT

complicado, aunque después tecnológicamente tengas la capacidad e incluso tu estrategia sea la correcta".

A la hora de hablar de las soluciones que pueden ayudar a la adopción de una postura más ofensiva señala Raúl D'Opazo que hay dos vectores de los que preocuparse: la identidad y el dato, que ahora mismo están deslocalizados. Menciona

el directivo de One Identity el machine learning como el elemento al que cualquier fabricante de cualquier segmento de mercado de seguridad está dando mucha consistencia, así como la importancia de construir aplicaciones que pueden hablarse con el resto del ecosistema para intentar ser un poco proactivo.

SECURE&IT. Francisco Valencia, CEO

"Muchas veces el CISO no sabe qué es lo que está pasando y no hay herramientas que le arrojen una visibilidad global de lo que está sucediendo en la infraestructura, en casa de las personas, en sus móviles, en la nube…", asegura Francisco

Valencia, Director general de Secure&IT, apuntando un segundo reto al que se enfrentan los responsables de ciberseguridad: la socialización del riesgo.

Dice también este directivo que la protección de la información “va mucho más allá de la informática” y que es importante “conseguir socializar el riesgo y que todos los departamentos sean conscientes de los riesgos y sean partícipes en la solución”.

Respecto a si se está adoptando una seguridad más proactiva, no tiene claro Francisco Valencia si se está produciendo desde el punto de vista del fabricantes o desde la organización “por el miedo y el compromiso que ahora empiezan a adquirirlos los órganos directivos, consejos de administración y comités de dirección”.

El reto al que se enfrenta Secure&IT no es lo que detecta y para la solución del fabricante, “sino lo que no es capaz de parar”. El SOC de la compañía recibe 600 millones de eventos cada día y tiene unas 10.000 alarmas diarias, y aunque se consiguen automatizar parte de las alarmas, “hay otra gran parte que se tienen que analizar a mano”. Explica el directivo que la tecnología que más ayuda a la prevención es la visibilidad, “y para conseguirlo lo ideal es tener una buena herramienta capaz de integrarlo todo, con un dashboard facilito en el que pueda verse todo lo que está pasando en la compañía y, en función de los que se vea, se puedan tomar acciones”.

Para Francisco Valencia el Threat Hunting es una pieza de un servicio o producto que está más cerca de los SOCs que de las empresas. “Un cliente no compra directamente y de forma aislada un Threat Hunting, sino que forma parte de un producto/servicio”.

En relación a los reducidos presupuestos de las administraciones públicas, del que es representante Ignacio Pérez, compañero de debate, dice Francisco Valencia que “el problema viene derivado de una de una grave falta de conocimiento por parte de la alta dirección”, que muchas veces no saben determinar cuánto vale la información que manejan”.

SONICWALL. Sergio Martínez, Country Manager Iberia

Según datos aportadas por Sergio Martínez en este debate, el 70% de los CISOs no se sienten

cómodos con las herramientas de seguridad que tienen desplegadas, y cerca de 60% se sienten preocupados por los usuarios que están al otro lado de la pantalla, lo que demuestra que “la formación es un aspecto muy importante”. Por otra parte, el Cyber Threat Report de Sonicwall señala que el ransomware se ha incrementado un 62% a nivel mundial, y un 20% los intentos del intrusión, “lo que nos lleva a plantearnos si se ha desplegado el modelo correcto de seguridad y si estamos en la fase de reducir riesgos”, unos riesgos que se han multiplicado con el teletrabajo y a los que solo podemos enfrentarnos con una defensa proactiva que vaya de extremo a extremo, que detecte lo desconocido, nos ofrezca visibilidad sobre lo que está ocurriendo, verifique la identidad de los usuarios… “y todo esto con un TCO adecuado para que salgan los números”.

“Nuestra estrategia es una defensa por capas, encima de la cual tiene que haber una monitorización que te de una visibilidad única de todo lo

ENCUENTROS ITDS - SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE SONICWALL

CLICAR PARA VER EL VÍDEO

> "Más que una tecnología, el Threat Hunting es un proceso"
>
> Sergio Martínez, Country Manager Iberia, SonicWall

que está ocurriendo en tu infraestructura”, explica Sergio Martínez cuando preguntamos qué tipo de tecnologías ayudan a generar una postura de seguridad más proactiva. Añade el directivo de SonicWall la capacidad de la compañía de detectar lo desconocido gracias a la inteligencia artificial y a una tecnología de sanboxing con tres motores que permite a los clientes “detectar y reaccionar a las ciberamenazas en tiempo real y de una forma casi automática”.

Sobre el Threat Hunting apunta Sergio Martínez que más que una tecnología es “un proceso de búsqueda de malware y de amenazas dentro de nuestras infraestructuras”.

SEGURIDAD PROACTIVA. PROPUESTA TECNOLÓGICA DE TREND MICRO

CLICAR PARA VER EL VÍDEO

"Hay que dar visibilidad, y cuanto más unificada mejor"

Raúl Núñez, Ingeniero Preventa, Trend Micro

TREND MICRO. Raúl Núñez, Ingeniero Preventa

Explica el portavoz de Trend Micro que en los primeros tiempos los fabricantes de seguridad se centraron en parar lo malo, pero que "actualmente con esta aproximación no vas a ningún sitio y tenemos que dar visibilidad y saber si un comportamiento es anómalo", que es hacia donde los fabricantes desarrollan su estrategia en pro de una seguridad más proactiva.

Destaca Raúl Núñez tres elementos que ayudan a conseguir una ciberseguridad más proactiva, empezando por la concienciación porque "por mucho dinero que gastes en producto tienes que concienciar a tus empleados entrenándolos"; un segundo elemento que considera esencial es la compartición de inteligencia de la manera más sencilla posible; el tercer elemento importante es la monitorización a través del SIEM y el XDR, "que no deja de ser un SIEM por detrás pero desarrollado por cada uno de los fabricantes".

Como conclusiones señala que "hay que dar visibilidad, y cuanto más unificada mejor", que los fabricantes deben acompañar al cliente no sólo en la venta sino a posteriori ya que "podemos tener el mejor producto, pero mal instalado no sirve para nada" y que hay que fomentar la interoperabilidad entre fabricantes para que sea mucho más fácil la búsqueda de amenazas.

17
JUNIO
11:00 CET

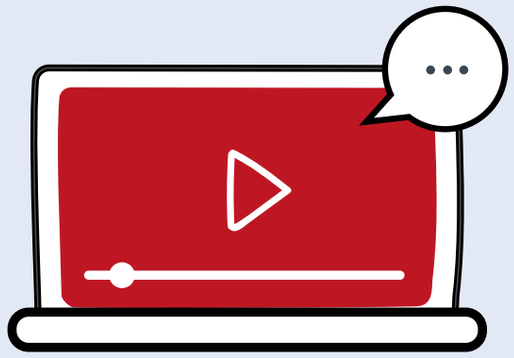
REGISTRO

El fenómeno del Device as a Service y las oportunidades para el canal TI

24
JUNIO
11:00 CET

Mejorando la experiencia del trabajador remoto

REGISTRO



#ITWEBINARS

29
JUNIO
11:00 CET

Entendiendo la Era del dato: tecnologías y propuestas para gestionar la “datificación”

REGISTRO

Nuevos retos de seguridad en entornos financieros

Su impacto en el modelo de negocio

Patrocinadores:

El sector financiero ante el reto de la ciberseguridad:

la digitalización abre la puerta a nuevas amenazas

Los riesgos de las TIC representan un enorme desafío para las entidades financieras y subrayan la importancia de implementar una adecuada estrategia de seguridad que abarque, desde la protección de infraestructuras hasta la seguridad de datos y usuarios. La formación y concienciación del usuario son también clave, a fin de que este se convierta en un eslabón más de la cadena en la protección.

NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

A lo largo de la última década, las entidades financieras, principalmente los bancos, han acometido un importante cambio en su modelo de negocio, apostando claramente por la digitalización como motor de innovación y puntal clave en su relación con el cliente. Así las cosas, este sector ha ido avanzando desde una huella digital básica hasta un entorno basado en la omnicanalidad, con el desarrollo de nuevos productos y servicios y un mejor y mayor aprovechamiento de tecnologías disruptivas, como la inteligencia artificial, el blockchain, la analítica y las tecnologías basadas en la nube.

Sin duda, esta creciente digitalización ha favorecido importantes beneficios: el customer centric es una realidad cada vez más consolidada, pero también ha generado significativos retos y riesgos no financieros, como la dependencia de proveedores y nuevos jugadores y la proliferación de ciberataques y amenazas online, exposiciones que se han multiplicado por el aumento de dispositivos electrónicos, la migración a la nube y la apertura de puertas y ventanas que han terminado por diluir el perímetro de la red. En este sentido, datos facilitados por el Fondo Monetario Internacional (FMI) apuntan que el número de ciberataques se ha triplicado en la última década, convirtiéndose en una amenaza para la estabilidad financiera. Según esta organización, en 2020 se produjeron 1.500 casos, frente a los 400 de 2012.

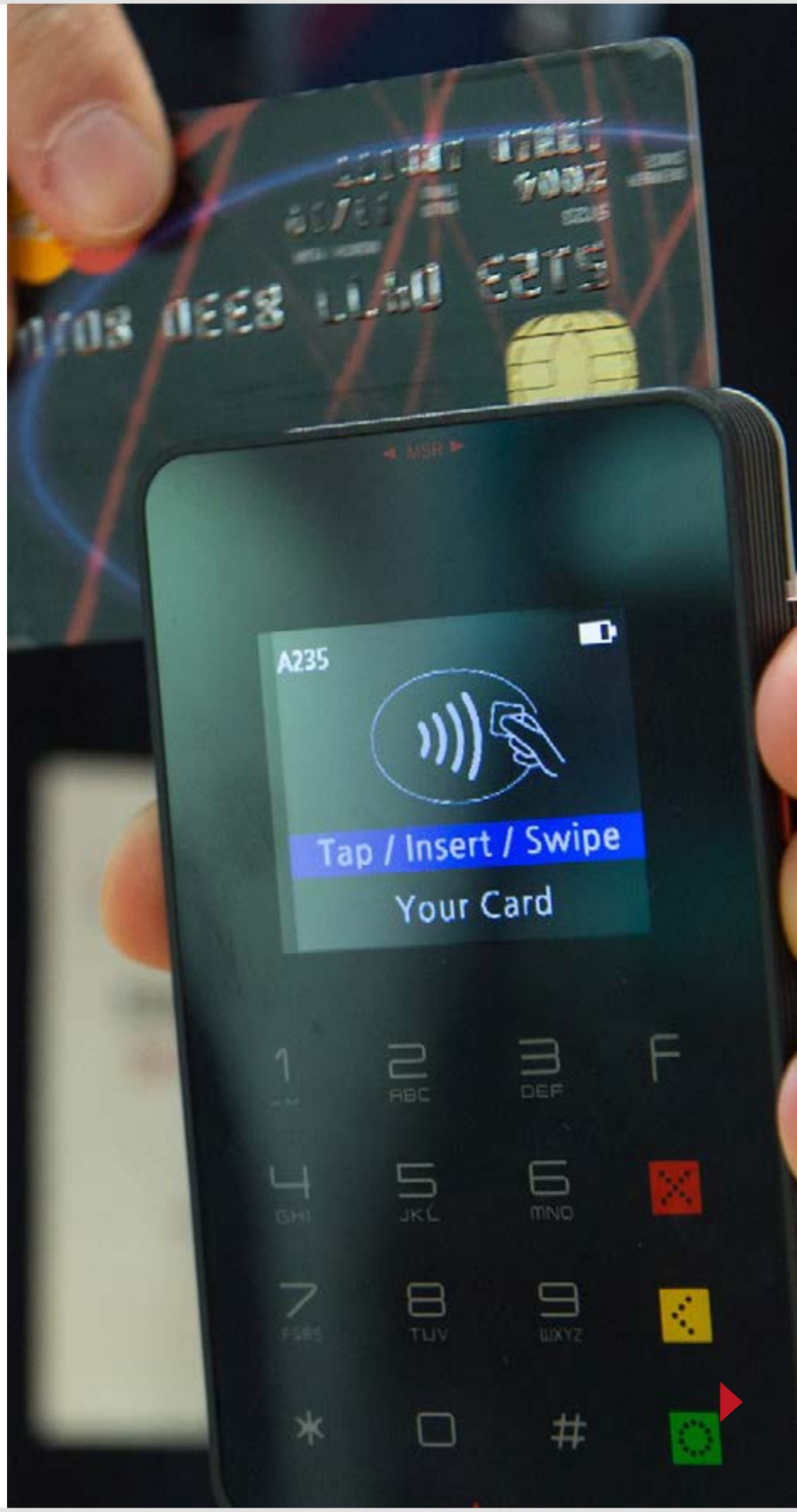
Del mismo modo, la aceleración de los planes de digitalización de estas compañías y, sobre todo, la generalización del teletrabajo a causa de la Covid-19, ha dilatado el nivel de riesgo, al abrirse nuevas vías de ataques que los ciberciminales han sabido aprovechar.

Así, este nicho ha experimentado la segunda mayor proporción de ciberataques relacionados con COVID-19, solo por detrás del sector de la salud, con un coste promedio por brecha de datos de 5.85 millones de dólares en 2020, frente a los 3.86 millones de dólares del promedio mundial, según datos de la última edición del informe anual Cost of a Data Breach Report de IBM.

EL DESAFÍO DE LA CIBERSEGURIDAD

La banca se enfrenta, por tanto, a un panorama difícil en materia de ciberseguridad, con ataques cada vez más complejos, muchos de los cuales se dirigen contra el usuario, el eslabón más débil, contra la propia infraestructura o hacia proveedores externos (ataques a la cadena de suministro). Así, a ofensivas de relleno de credenciales, fraude de apropiación de cuentas, correos electrónicos de phishing o malware (troyanos), se unen otras amenazas como el ransomware, que incluye vectores de doble extorsión y factor humano, junto con la creciente demanda de desencriptación de datos, y los ataques DDoS.

Detrás de estos ataques se esconden no solo criminales cada vez más osados, sino también estados y atacantes patrocinados por estados



que saben que por la sensibilidad de los datos que custodian, los bancos son un blanco fácil. Tanto es así, que, hoy por hoy, el ciber riesgo se encuentra en tercer lugar en el ranking de riesgos de entidades financieras, después de los lucros cesantes y el riesgo pandémico, según el 10º Barómetro de Riesgos de Allianz 2021.

Afortunadamente, y por los activos que gestionan (dinero, datos sensibles y reputación) en el sector financiero siempre ha existido una gran concienciación sobre la seguridad, tanto en la vertiente física como lógica. Se trata de un factor de confianza. Así, las entidades financieras destinaron en 2020 el 10,9% de su presupuesto a ciberseguridad, frente al 10,1% del año anterior. En términos de gasto por empleado, esto supone alrededor de 2.700 dólares, según una encuesta de Deloitte y FS-ISAC.

Ahora bien, es necesario que esta seguridad evolucione al mismo ritmo que lo hacen las tecnologías, los servicios provistos y la regulación (PSD2, Mifid2, CRD2...), sin olvidar, por supuesto, como lo hacen también la tecnología de ataque y los hackers, alumnos aventajados.

Por ello, y además de proteger infraestructuras como los ATMs, es necesario apostar por soluciones centradas en el resguardo del endpoint, la red, email, servidores o workloads en la nube, como antivirus, plataformas EDR, XDR o con capacidades de aprendizaje automático. Asimismo, estas entidades deben avanzar hacia un enfoque proactivo, que dé prioridad a la prevención, para interrumpir los ataques antes de que el malware o la amenaza maliciosa -sin archivos- pueda siquiera comenzar a ejecutarse. También, la monitorización y gestión de lo que ocurre en redes botnets o en la Deep Web ayudará a prevenir y a mejorar la seguridad, con planes de respuesta. Esto incluye la formación de los empleados en materia de concienciación sobre la seguridad, la limitación de los privilegios de los administradores y una estrategia de confianza cero que abarque la gestión de la identidad y el acceso, así como la seguridad de la red. Importante igualmente es la colaboración entre entidades y con terceros, a fin de garantizar la resiliencia operativa digital.

EL RIESGO DE LA BANCA MÓVIL

Adicionalmente, la expansión de los servicios basados en dispositivos móviles (banca móvil) y la mayor dependencia de los clientes de las aplicaciones de banca electrónica ha ampliado su vulnerabilidad, convirtiéndose estos usuarios en blancos potenciales para los actores maliciosos, que utilizan una variedad de técnicas, incluidos troyanos bancarios basados en aplicaciones bancarias falsas, para atacarles. Así, la actividad de los troyanos bancarios se ha intensificado un 15%, según un estudio de Check Point, y estos

se orientan, sobre todo, a atacar el segundo factor de autenticación, principalmente SMS, para además de robar datos de acceso o credenciales, hacerse con otros más personales.

Ante esta situación y para protegerse, los bancos deben integrar metodologías o tecnologías que ayuden a asegurar las transacciones electrónicas, como la criptografía, o que faciliten la autenticación del usuario para evitar la suplantación de identidad, como los sistemas de tokenización. Igualmente, y de cara a ser más precisos, es fundamental securizar y custodiar las claves que protegen esa información (claves de cifrado) y la gestión de su ciclo de vida, sobre todo ahora, cuando se está produciendo una clara orientación a los servicios en la nube. En este sentido, los HSMs, capaces de almacenar y proteger claves criptográficas en consonancia con las normas más rigurosas de la industria, como la Directiva Europea de Pagos PSD2, son una opción.

PROTEGER EL DATO

La progresiva implantación de modelos comerciales, como el open banking, asentado en el intercambio de datos entre bancos y terceros (Bigtech) a través de APIs, está ocasionando distintos problemas de protección, sobre todo en el ámbito de la seguridad (de usuarios y entidades) y el análisis de datos. Según McKinsey & Company, los bancos son responsables de mitigar el riesgo de fraude y deben implementar controles, que incluyan análisis avanzados (por ejemplo, para va-

Blockchain: riesgo u oportunidad

Los bajos tipos de interés, la reducción de márgenes, y los nuevos requerimientos regulatorios están presionando a la banca para buscar nuevas fórmulas que le permitan ganar en competitividad y rentabilidad. En este contexto, tecnologías como blockchain, suenan cada vez con más fuerza, en tanto en cuanto permiten realizar directamente entre partes, transacciones seguras con el apoyo de máquinas y algoritmos.

Asociada esta tecnología a las criptomonedas, una de las formas más populares y conocidas de usar blockchain, sus capacidades van sin embargo más allá de su almacenaje e intercambio, desde transacciones en tiempo real hasta tokenización de activos, préstamos y créditos, valores, prevención del fraude e identificación de los clientes. Además, sus capacidades de seguridad, apoyadas en la descentralización de la información, así como, en la eliminación de intermediarios, y la implementación de criptografía y firma digital para asegurar las transacciones, favorecen que estas operaciones (y sus datos) tengan la mayor seguridad, privacidad y autenticidad posible.

Sin embargo, y aunque Blockchain es una tecnología bastante segura en su diseño, su incorporación en mercados y entornos regulados, como el financiero, está produciéndose lentamente. Aún se tienen que garantizar aspectos de su seguridad, muchos de ellos relacionados con la ausencia de estándares tecnológicos, la falta de interoperabilidad entre distintas plataformas de cadenas de bloques o el uso de contratos inteligentes, que puedan ser origen de fugas de datos de carácter personal, y que hace necesario incorporar metodologías de seguridad por diseño desde las primeras fases de desarrollo, para evitar riesgos como: minado de cadenas laterales o paralelas (sidechain) o ataques DDoS, entre otros.

También y en lo que tiene que ver con el sistema de autenticación de la gestión de accesos a los sistemas blockchain, y aunque la normativa europea obliga a la banca a tener sistemas de autenticación de doble o triple factor, es necesario avanzar, sobre todo, por su relación con otros sistemas de información de la empresa.

Estos aspectos podrían solucionarse con la creación segura de claves o que el proceso de firma de cada una de las transacciones que se lanzan al bloque sea invulnerable. Es necesario validar el uso de blockchain como registro fundamentado y vinculante de evidencias digitales, definiendo en qué condiciones es válido. No hay duda de que si alguien descuida la custodia de sus claves éstas podrían acabar en manos de un atacante que podría así suplantar su identidad en la aplicación correspondiente. También hay que tener en cuenta que, debido al potencial de esta tecnología, es previsible que los ciberdelincuentes busquen oportunidades para atacar cualquier vulnerabilidad, tanto humana como técnica, en el ecosistema de blockchain.

lidar el origen de las llamadas entrantes a la API), modelos de autenticación segura del cliente y herramientas sólidas para detectar ataques de fraude, de acuerdo a PSD2. Estas normas también requieren que los bancos proporcionen un "sandbox" protegido a los proveedores de servicios de pago para las pruebas y el desarrollo continuo de servicios que utilizan la interfaz del banco.

Además de involucrarse en oportunidades de negocio innovadoras y potencialmente lucrativas abiertas por PSD2, el sector financiero se ha lanzado de lleno hacia una mejora real en la eficiencia, escalabilidad y flexibilidad de la mano de la Nube, para asegurar, en tiempos de pandemia, una fuerza de trabajo a distancia y garantizar la capacidad de recuperación. De este modo, y con los usuarios, dispositivos, aplicaciones y datos fuera del centro de datos empresariales y la red, la necesidad de proteger esos activos, así como de poseer una visibilidad completa del entorno se ha hecho imperativo. A este respecto, IDC Research confirma que cualquier solución de seguridad para cloud ha de incluir tres elementos: integración nativa, protección amplia y gestión y automatización. En torno a esta premisa han surgido marcos de seguridad como SASE, que esboza una convergencia de múltiples funciones de seguridad, como acceso de red Zero Trust (ZTNA), Gateway Web Seguro (SWG) de próxima generación, Agente Seguro de Acceso a la Nube (CASB), Gestión de la Postura de Seguridad Cloud (CSPM) o Firewall como Servicio (FWaaS); entregados desde la nube.

Además de la nube, la externalización de las funciones y servicios de las TIC, que ha cobrado mayor importancia durante la actual crisis sanitaria, puede plantear también retos relacionados con la gestión del riesgo de terceros, la confidencialidad y la protección de los datos de los consumidores. Igualmente, la inclusión del aprendizaje automático y de la inteligencia artificial están acrecentando esta vulnerabilidad, cuando, por ejemplo, los datos corruptos no detectados se introducen en los algoritmos y se utilizan en la toma de decisiones, según Bank for International Settlements (BIS). Por último, y en el caso de sufrir un episodio de ransomware, la recuperación de los datos, podría tornarse muy compleja, y las dudas sobre la exactitud de la información recuperada podrían hacer que el problema se prolongue durante un largo periodo de tiempo.

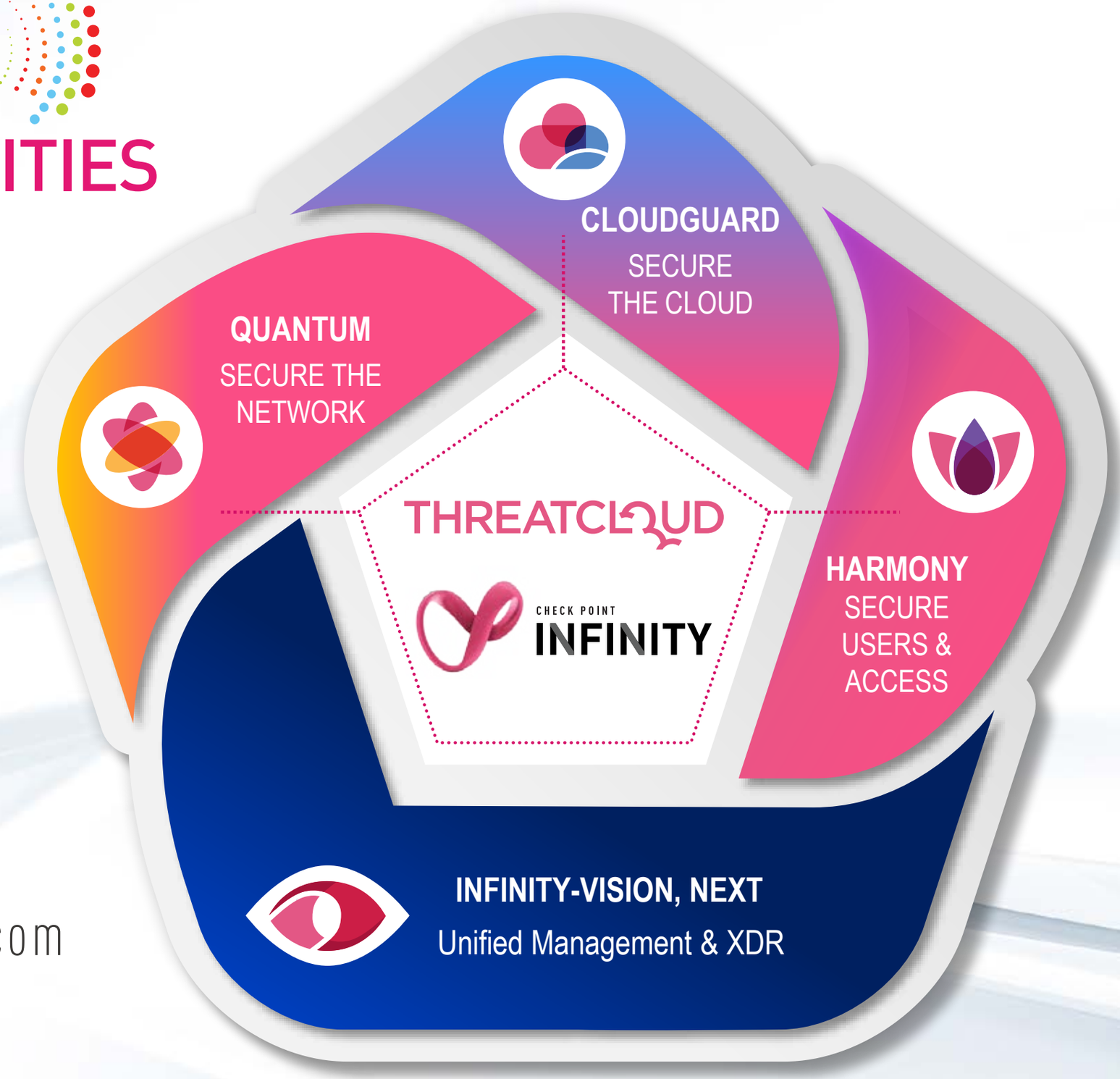
No hay duda, por tanto, que el gran volumen de datos generados por la banca requiere de la facultad de analizar y proteger dicha información, manteniendo y acatando, al mismo tiempo, las estrictas normas de la UE en materia de privacidad y protección de datos. Asimismo, el aumento de la demanda de servicios financieros en línea, y la progresiva modernización de los sistemas de pago, según el dinero en efectivo va perdiendo preponderancia, llevan a cuidar todos los aspectos de la seguridad. Cualquier incidente podría socavar la confianza del cliente, por lo que la ciberseguridad es más esencial que nunca. ■

MÁS INFORMACIÓN

- Incremento de ciberataques en la ultima década
- Ciberataques relacionados con la Covid-19
- Cost of a Data Breach Report
- 10º Barómetro de Riesgos de Allianz 2021
- Madurez en la ciberseguridad y riesgos en las instituciones financieras
- Actividad de los troyanos bancarios
- Directiva Europea de Pagos PSD2
- PSD2 y la disrupción en el open banking
- El efecto de los datos corruptos
- Bajos tipos de interés

Check Point®
SOFTWARE TECHNOLOGIES LTD

NEW WORLD
NEW OPPORTUNITIES
2021



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

Nuevos retos de seguridad en entornos financieros;
su impacto en el modelo de negocio

Más tarde o más temprano las entidades financieras pueden ser víctimas de un ciberataque. Con esa idea en mente, deben prepararse para responder a las amenazas de hoy pero también a todas aquellas que van surgiendo al amparo de las nuevas tecnologías.

MESA REDONDA IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

El sector financiero, sobre todo la banca, lleva años sumido en una profunda transformación digital que le ha llevado a afrontar una serie de cambios, tanto en el modo de ofrecer y prestar sus servicios como en el de atender a sus clientes. Asimismo, la situación derivada de la COVID-19 ha transformado el comportamiento del consumidor, desde las preferencias de canal hasta el método de pago, y ha abierto una importante brecha en ciber-

“Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataque. Afortunadamente hay bastante concienciación en ciberseguridad”

EUSEBIO NIEVA,
DIRECTOR TÉCNICO DE CHECK POINT

seguridad, al incrementarse la digitalización y, por ende, la superficie de ataque. Por todo ello, ¿cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente entidades y servicios financieros? Para hablar sobre ello y conocer cómo afrontan los nuevos ataques y amenazas; su grado de concienciación al respecto de la ciberseguridad; cómo se ha adaptado este sector a tecnologías emergentes como blockchain o las nuevas normativas como PSD2; o cuál debe ser el siguiente paso en la adopción de nuevas tecnologías de seguridad, hemos contado con la participación en esta Mesa Redonda IT de Eusebio Nieva, Director Técnico de Check Point; Javier Sánchez, Territory Sales Manager de Entrust; Luis Javier Suárez, Presales Manager de Kaspersky; Jesús Rodríguez, CEO de Realsec; Igor Unanue, CTO de S21sec; Alfonso Martínez, Country Manager, Data Protection de Thales; y José de la Cruz, Director Técnico de Trend Micro Iberia.

RETOS EN CIBERSEGURIDAD

La creciente digitalización ha abierto la puerta a importantes retos en materia de ciberseguridad que, aunque extensibles a todos los verticales, en el financiero se perciben aún más. En este sector se maneja algo que todos los atacantes quieren: “dinero”, asegura Eusebio Nieva, por lo que no se debe confiar en sistemas tradicionales como protección frente a amenazas desconocidas. “Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataques”. Afortunadamente hay bastante concienciación en ciberseguridad.

Efectivamente, la cada vez mayor sofisticación por parte de los cibercriminales lleva a un nuevo paradigma en el que, según Luis Javier Suárez, “ya no basta con confiar en soluciones que aseguren un elevado grado de prevención, sino que se ha de plantear la hipótesis de poder estar siendo comprometido y no saberlo”. Aquí ya entra la parte de recoger ciertas métricas, telemetrías o anomalías para poder hacer un análisis y ver cómo cambian las normas del juego.

En idéntica línea, José de la Cruz recurre al planteamiento Zero Trust; “hay que asumir que

va a existir una brecha, y estar preparados para detectarla y actuar". Además, destaca dos retos que apuntan a la protección de las infraestructuras, donde hay una amalgama de tecnologías tradicionales y modernas combinadas, y a los usuarios, externos e internos. "Debemos dotarles de una seguridad que les aporte visibilidad sobre lo que ocurre en sus entornos".

Sobre estos retos, Igor Unanue considera, que, por el propio proceso de digitalización, estas organizaciones integran nuevas tecnologías, aplicaciones... que están atrayendo nuevos tipos de ataques, como los de tipo hacking, que permanecen en las redes internas largo tiempo sin ser descubiertos, causando importantes daños. "Van a seguir descubriéndose nuevas amenazas. La banca debe mantenerse alerta y estar corrigiendo para poder protegerse mejor".

UN NUEVO CONCEPTO DE BANCA

La progresiva digitalización ha marcado una senda de cambios. Se ha pasado del cliente físico al cliente móvil, de los centros de datos al cloud, ampliándose, al mismo tiempo, los vectores de ataque, lo que ha supuesto una mayor vulnerabilidad. ¿Cómo está enfocando la banca estos cambios?

Desde la perspectiva de este desarrollo, Javier Sánchez, observa que, en la actualidad, el vector de relación entre la banca y el usuario es la aplicación, por lo que hay que protegerla. "Las apps son un riesgo para los usuarios, que pueden ver comprometidos sus datos, y para los bancos, por el desprestigio para su negocio". Sobre la nube, donde cada vez residen más datos, incluso críticos, Sánchez estima que estarán seguros mientras el control de las claves que los cifran, no viaje con ellos.

Sobre este proceso de transformación, Jesús Rodríguez destaca que, a consecuencia de la pandemia, muchos desarrollos se han precipitado. "El uso del efectivo ha caído y canales que se iban a desarrollar de forma natural se han precipitado". Cada vez se hacen más operaciones utilizando dispositivos móviles y fórmulas, como el open banking, están cambiando el modo en que se utilizan los servicios bancarios. "Esto incide en la necesidad de proteger las transacciones (crip-

"Mediante la utilización de criptografía se van a proteger las transacciones, y con los sistemas de tokenización se va a autenticar a los usuarios. La suplantación de identidad es uno de los mayores riesgos para la banca"

JESÚS RODRÍGUEZ, CEO DE REALSEC

“La concienciación, incluso la formación, no dejan de ser responsabilidad del banco. El usuario tiene que ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO IBERIA

tografía) y al usuario (sistemas de tokenización para evitar la suplantación de identidad).

Por su parte, Alfonso Martínez defiende la idea que con la gran evolución que ha tenido la banca en estos últimos años, esas entidades no pueden seguir protegiéndonos como hace 10 o 15 años. “Al igual que el abanico de opciones se multiplica, las amenazas también y son más sofisticadas. Los fabricantes no podemos quedarnos atrás. Tenemos que dar soluciones a las tendencias tecnológicas que van surgiendo, y ofrecer esa completa seguridad alrededor de la información”.

LA CONCIENCIACIÓN DEL USUARIO

El usuario es el centro de todo. Sin embargo, es importante encontrar un equilibrio entre la experiencia de usuario y la seguridad. ¿Cómo conseguirlo?

Para Eusebio Nieva, este equilibrio pasa porque el usuario perciba que la seguridad es útil. “Las medidas de protección pueden interferir en el usuario, en el acceso o en el dato”. Sin embargo, se debe intentar que el cliente distinga estas pautas como una ventaja, que aprecie que con estos mecanismos evita perder dinero, mientras consigue que las transacciones sean fiables y sus datos estén seguros. “A la vez que protege, la propia tecnología debe mostrar sus beneficios”.

Este componente de concienciación también es apreciado por Luis Javier Suárez, quien distingue dos desafíos para los bancos: conseguir que la experiencia del usuario no sea invasiva, mientras se recogen comportamientos y detectan anomalías que permitan tomar medidas para la detección temprana del fraude; y trabajar la concienciación, tanto dentro de la propia empresa como de cara al usuario. “Es importante trasladar las buenas costumbres adquiridas en la banca tradicional al mundo digital”.

La importancia de la concienciación, y de la formación, es destacada por José de la Cruz. “No deja de ser responsabilidad del banco proteger los activos de sus usuarios, que deben ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”. Además, es clave comprender que la seguridad se ha de implementar en la fase de diseño, para que la integración sea mucho más transparente y sencilla y no interfiera en la agilidad o experiencia de usuario.

Para referirse al valor que le da el usuario a esta agilidad, Igor Unanue cita el doble factor

de autenticación, que no se implementó hasta que no fue obligatorio por ley, para no interferir en el acceso. “Es un tema de concienciación, de cultura. Cuando nos habituemos a utilizar determinadas tecnologías de seguridad también lo haremos en la banca”. No obstante, estas tecnologías han de resultar naturales para el usuario. “La seguridad debe ser cada vez más efectiva y más sencilla”.

PSD2 Y OTRAS REGULACIONES

Las entidades financieras siempre han estado a la cabeza en cuanto a modelos de transformación digital y en la adopción de medidas de seguridad, siempre han querido ir un paso por delante. Sin embargo, ha habido casos más complicados, como con la regulación PSD2. ¿Se ha logrado de una manera efectiva su adopción? Ahora, cuando ya se vislumbra el reflejo de PSD3, toca preguntarse si la banca está preparada para lo que está por venir.

Al respecto de la observancia de PSD2, Jesús Rodríguez refiere cómo las entidades se han estado preparando, primero, con el desarrollo de APIs para poner a disposición de terceros información de los clientes, y, después, con el establecimiento de un sistema de autenticación de doble factor. “En España no podemos hablar de incumplimiento, aunque la mayoría de entidades no han adoptado un sistema de tokenización; han optado por el envío de un SMS. A futuro, con la PSD3 en el horizonte, habrá que buscar otras soluciones basadas en token”.

Sobre la aceptación de estas medidas, Alfonso Martínez reconoce el gran esfuerzo realizado al abrir estas APIs para favorecer el open banking. Sin embargo, expone la importancia de implementar la seguridad desde el principio, en consonancia con PSD2, y para cumplir con otras nor-

“La seguridad debe estar habilitada desde el principio. Solo si los fabricantes ofrecemos las tecnologías adecuadas, las entidades van a poder acatar las distintas normativas y procurar los servicios (seguros) apropiados”

ALFONSO MARTÍNEZ, COUNTRY MANAGER, DATA PROTECTION DE THALES IBERIA

> "A causa de las normativas, los bancos están aplicando cada vez más niveles de seguridad sobre sus accesos a la red SWIFT. Pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes saben aprovecharlo"
>
> IGOR UNANUE, CTO DE S21SEC

mativas. En este punto el papel de los fabricantes es clave. "Debemos ofrecer las tecnologías adecuadas para que estas entidades puedan procurar los servicios (seguros) apropiados".

ATAQUES A LA RED SWIFT, UN RIESGO SISTÉMICO

Otro tema que cada vez está resultando más relevante son los ataques contra la red SWIFT, que se han multiplicado en los últimos tiempos. Ahora bien, ¿qué impacto están teniendo y en qué consisten estas ofensivas?

"Por tratarse de una red en la que fluye el negocio y circula el dinero, SWIFT es un claro objetivo para los hackers, que intentan interceptar transacciones para sacar beneficio", explica Eusebio Nieva. Para su salvaguarda, la tecnología puede ayudar muchísimo, sobre todo para el análisis de fraude y la securización de ciertos puntos que todavía son un poco débiles. "Al final se trata de aplicar la tecnología en esas transacciones. Protección y fiabilidad en todos los extremos".

Mitigar y securizar es crucial, pero antes hay que conocer cómo se producen estos ataques. En este sentido, Luis Javier Suárez, destaca que los más eficientes son los dirigidos contra la cadena de suministro. "Los atacantes manejan una cantidad abrumadora de inteligencia sobre los organismos que operan en la red SWIFT. Conocen qué vulnerabilidades pueden ser explotadas dentro de los sistemas y aprovechan esta información para saber dónde atacar y alcanzar ese objetivo".

Sobre las razones que explican los ataques a la red SWIFT, Igor Unanue revela que, por tratarse de una red externa, las medidas de seguridad son más laxas. "Sin embargo, ahora, sobre todo por las normativas, se están aplicando mayores niveles de seguridad a estos entornos, pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes la están aprovechando bien. Al final es una red de comunicación más, y como tal hay que protegerla".

La cadena de suministro es reconocida también por José de la Cruz, como el elemento más débil, y, dentro de ella, los bancos pequeños,

con medidas de seguridad menos robustas, el eslabón más frágil". No obstante, todos deben asumir que antes o después se producirá un ataque, por lo que las entidades deben dotarse de una visibilidad que les permita conocer lo que está ocurriendo, tanto en su entorno como con los flujos de información que existen con terceros.

TECNOLOGÍAS EMERGENTES

Tecnologías emergentes como blockchain, IA o IoT están empezando a impactar en los servicios financieros. ¿Cómo se están adaptando los bancos a ellas?

Sobre este punto, Javier Sánchez, expresa que "están en proceso". Los bancos custodian tanto el dinero como la confianza de sus clientes por lo que tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que formen parte de su proceso de negocio. En el caso de una blockchain pública no hay nadie al otro lado, por lo que los bancos no pueden comprometer su confianza con una tecnología que puede no ser segura.

Ahora mismo, la banca necesita ganar en competitividad y en rentabilidad por lo que, según Jesús Rodríguez, necesita hacer uso de tecnologías innovadoras como IA, donde están más adelantados. Otras como blockchain, muy ligada a las criptomonedas, y donde se "avanzará con una regulación", también son utilizadas para cifrar bloques o firmar smart contract, pero no cuando hablamos de claves, donde el nivel de exigencia es muy alto. Otras como IoP despegarán en un futuro.

Desde la perspectiva de representar a una empresa que fabrica tecnología que ayuda o habilita para el uso de innovaciones como blockchain, Alfonso Martínez considera que falta mucha labor de comunicación. "Estas tecnologías luego hay que aplicarlas a la vida real y, en ese sentido, falta información tanto, para los usuarios finales, que tienen que saber qué es blockchain y cómo utilizarlo como para las entidades financieras, para entender cómo lo pueden monetizar.

TECNOLOGÍAS IMPRESCINDIBLES

Ante toda esta innovación, el sector financiero no puede bajar la guardia en su seguridad. ¿Cuáles son aquellas tecnologías de seguridad que puede ser consideradas imprescindibles en la actualidad? Y ¿a futuro?

"Los bancos custodian tanto el dinero como la confianza de sus clientes. Tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que estas formen parte de su proceso de negocio"

JAVIER SÁNCHEZ, TERRITORY SALES MANAGER DE ENTRUST

“Cualquier organización tiene que asumir que puede ser comprometida. Este paradigma nos lleva a la gestión del incidente y al gobierno de algo que se ha impulsado desde el sector financiero: la gestión de indicadores de compromiso”

LUIS JAVIER SUÁREZ, PRESALES MANAGER DE KASPERSKY

Eusebio Nieva reconoce una alta concienciación en ciberseguridad, pero recomienda no bajar la guardia. “Estas entidades deben optar por tecnologías específicas para abordar amenazas actuales, como el ransomware, los ataques a la cadena de suministro o la protección del endpoint, pero también, por enriquecer sus sistemas con diferentes soluciones que protejan contra los peligros surgidos al calor de innovaciones, como las tecnologías cloud, y que las organizaciones financieras están convirtiendo en el core de sus servicios y de sus negocios”. Deben evolucionar y adaptarse según progresan sus tecnologías. La protección de la red o del endpoint era algo que había que hacer, y ahora hay que proteger las claves. En este sentido, Javier Sánchez respalda la importancia del cifrado, que ahora, además, es percibido tanto por otros fabricantes de seguridad como por las propias entidades del sector financiero como una solución necesaria para proteger la información. “Se ha producido una concienciación en torno a la importancia de securizar las claves, por lo que su adopción está ocurriendo de un modo natural en la banca”.

En línea con esta innovación hay un componente de concienciación importante. A este respecto, Luis Javier Suárez valora la trascendencia de que las empresas financieras desarrollen un plan de concienciación, ya sea de forma individual o con el respaldo de una empresa especializada. “También, deben asumir que su ciberseguridad puede verse comprometida, por lo que el uso de indicadores de compromiso resulta efectivo, sobre todo para compartir con terceros la información que contienen (inteligencia y patrones de ataques) y medir la afectación”. Asimismo, es esencial la explotación de inteligencia de amenazas, para ir a la par con los atacantes.

MEDIDAS PROPORCIONALES

Decidir qué solución o qué conjunto de recursos son los más adecuados para proteger las infraestructuras de las entidades financieras es complicado. “La realidad”, expresa Jesús Rodríguez, es que los riesgos están ahí, y las medidas han de ser proporcionales, así como las políticas

y los procedimientos de seguridad que se establezcan. No obstante, se deben proteger los activos de negocio, los riesgos de fraude e implantar medidas contra la suplantación de identidad o el malware. Por otro lado, el despliegue de nuevos canales de pago ha promovido un mayor uso de la criptografía, mientras que el crecimiento de los datos, precisa de medidas de protección que requieren el uso del cifrado, para cumplir con normativas como PSD2 o PCI DSS.

En la misma línea, Igor Unanue reitera que allí de donde vengan las amenazas es donde la banca más tendrá que invertir en ciberseguridad. En cuanto a futuro desafíos, señala la persistencia del malware (malware bancario) y de otros procedentes de servicios cloud, por el incremento de servicios de colaboración, que derivará en muchos riesgos. "Imperativo será también proteger el endpoint y, en general, todo aquello donde la banca perciba una amenaza".

Alfonso Martínez, coincide en que hay "mucho vector que proteger y el dato debe salvaguardarse así mismo con el cifrado". El cifrado puede ser en la nube, en máquinas virtuales, incluso en movimiento o viajando de una nube a otra. Lo importante es entender que detrás de esos sistemas tan complejos existe una inteligencia real a la que hay que ayudar para que la gestión sea sencilla y la criptografía no se convierta en un dolor de cabeza. "Debemos darles las herramientas para poder gestionarlo todo de manera centralizada y correcta".

Para José de la Cruz, la banca se enfrenta a un panorama heterogéneo, con diferentes tecnologías, proveedores y entornos, que le provocan un grado de exposición muy alto. La respuesta ante eso es visibilidad y control. "Visibilidad de lo que se protege, para conocer el origen y alcance de un ataque, y control sobre aplicaciones que no han sido diseñadas con la seguridad en mente y que hay que resguardar de un modo transparente". En lo que respecta a servicios como DevOps o cloud, un enfoque Cloud Security Posture Management ayuda a dar esa capa de visibilidad, y a identificar riesgos, para mitigarlos. ■

MÁS INFORMACIÓN

- Mesa Redonda IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

JOSE FRANCISCO PEREIRO, GLOBAL HEAD OF PRIVACY TECH | RISK, BNP PARIBAS

“Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos”

En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas.

¿Cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente los servicios financieros?

Uno de los principales retos es gestionar el riesgo de terceras partes, la cadena de suministro se está transformando con velocidad y creciendo en volumen. Adicionalmente a la colaboración histórica con grandes multinacionales tecnológicas, es cada vez más frecuente en el sector financiero la colaboración con startups, fintech y multitud de nuevos socios. Estas organizaciones aportan sin duda innovación y nuevos modelos de negocio, pero es necesario evaluar con detenimiento los riesgos de seguridad y ayudarles a mitigarlos antes de comenzar una iniciativa conjunta.

Otro de los retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados. Contra esto, además seguir trabajando en el diseño e implementación de nuevos controles técnicos para detener los ata-

ques, es fundamental entender el factor humano, puesto que muchos de estos ataques tienen como base de entrada la ingeniería social, que intenta explotar las debilidades que todos tenemos cuando somos expuestos a una situación de falso peligro o urgencia con el objetivo de influir en nuestra conducta. Por esto, ya no es suficiente con disponer de un programa formación en ciberseguridad, sino que es necesario cubrir tres dimensiones: formación, concienciación y entrenamiento. La segunda, la concienciación, hace referencia a la capacidad de crear impacto emocional para protegernos de situaciones de peligro, como muy bien se hace por ejemplo en las campañas de tráfico. La tercera, el entrenamiento, es la más importante y consiste en simular situaciones cercanas a un ataque cibernético para desarrollar las habilidades necesarias y responder adecuadamente cuando se produzca un ataque real.

El tercer reto es la captación y retención del talento en ciberseguridad. Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos, pero es necesario competir en un mercado laboral de nicho en el que cada vez hay más empresas interesadas en reclutar este tipo de profesionales. Por eso, además de desarrollar políticas de atracción para las nuevas generaciones, es necesario darse cuenta de que, muchas veces, el talento está más cerca de lo que se piensa y que una alternativa interesante es formar en ciberseguridad a profesionales que estén trabajando en otras áreas.

¿Cómo se han adaptado los servicios financieros a tecnologías emergentes como Blockchain o IoT?

Las tecnologías emergentes, como el Blockchain, IoT, AI, Big Data, Cloud y muchas otras, ofrecen sin duda una gran oportunidad para desarrollar nuevos modelos de negocio y de relación con nuestros clientes. Las ventajas de estas tecnologías suelen ser evidentes y crean un alto nivel de interés en las áreas de negocio. Sin embargo, por tratarse de tecnologías emergentes, no siempre hay experiencia en la industria que nos permita modelizar y dimensionar los riesgos de ciberseguridad de una forma estándar.

Por ejemplo, las arquitecturas Blockchain o DLT, que son reconocidas como de las más seguras en la actualidad por su base criptográfica, tienen ya algún riesgo identificado como el asociado al compromiso del 51% de los nodos de la red. Si bien ejecutar este tipo de ataque es extremadamente difícil en aplicaciones basadas en Blockchain públicos con decenas de miles de nodos, como es el caso de la criptomoneda Bitcoin, si hablamos de una implementación privada con sólo decenas de sistemas y sistemas homogéneos, el riesgo de este tipo de ataque se incrementa, por lo que es necesario de dotarlo de medidas adicionales.

Un caso particular de tecnología emergente es la computación cuántica que, cuando ésta alcance cierta escala, pondrá en riesgo la seguridad de muchos sistemas a nivel global, al poder romper el cifrado de clave pública en el que se basan muchos algoritmos criptográficos.

Por tanto, la aproximación adecuada con las tecnologías emergentes es la basada en un análisis pormenorizado de los riesgos, mediante una aproximación consultiva, dedicando profesionales de seguridad al estudio de las posibles fallas y la definición de los controles y tecnologías de seguridad necesarios, así como la realización de pruebas exhaustivas antes de su salida a producción.

¿Qué regulaciones están afectando al sector financiero y cómo se está haciendo frente a ellas?
El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo. Esto nos ha permitido disponer de una estructura empresarial y cultura organizativa que permite asimilar nuevas regulaciones con relativa ventaja a empresas de otros sectores. Dicho esto, y con relación al tema que nos ocupa, las regulaciones de privacidad que están surgiendo a lo largo del planeta, y en particular la GDPR en la zona europea, están teniendo un impacto significativo en los sistemas de información y en las medidas de ciberseguridad asociada.

Por un lado, se ha regulado el concepto de protección de datos en el diseño de nuevas aplicaciones y servicios, que tiene inherentemente asociada un componente de ciberseguridad. De esta forma, cada vez que se desarrolle un nuevo producto que procese datos de carácter personal, este deberá tener en cuenta las necesidades regulatorias y de seguridad. Además, la GDPR, en su artículo 32, establece la obligatoriedad de implementar las medidas de seguridad necesarias para proteger los datos proporcionalmente a los riesgos a los que está expuesta. La privacidad debe ser embebida en todas las arquitecturas y soluciones IT, por ejemplo, cuando antes estábamos hablando de tecnologías emergentes, la GDPR afecta en mayor o menor media en diferentes aspectos: el derecho al olvido en Blockchain, las transferencias de datos internacionales en Cloud, las decisiones automatizadas en la Inteligencia Artificial o el tratamiento masivo de datos en el Big Data.

> "Uno de los grandes retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados"

Por último, la privacidad ha tenido un efecto más sutil, pero no menos influyente en el mundo de la seguridad. Hasta ahora, si una tecnología de seguridad se consideraba como buena para mitigar riesgos, se implementaba; pero tras la llegada de las regulaciones de privacidad a diversas partes del mundo es necesario asegurar que dichas tecnologías cumplen con la regulación. Por ejemplo, las tecnologías de detección de anomalías en el comportamiento de usuarios, que permitían detectar si una cuenta de usuario había sido comprometida, ya no podrán ser implementadas si no garantizan los derechos y libertades en materia de protección de datos.

Tras un año de pandemia, ¿qué han aprendido los CISOs del sector financiero?
La enseñanza fundamental es que la seguridad no se puede poner en ERTE. En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas. Además, durante esta crisis ha sido necesario tomar decisiones transcendentes en un plazo muy breve de tiempo, como la de tener que poner centenares de miles de trabajadores españoles a teletrabajar de la noche a la mañana. Estas decisiones, necesarias para la continuidad de negocio, si no son acompañadas por medidas de ciberseguridad que mitiguen los riesgos del nuevo escenario, pueden tener efectos adversos. De igual forma, los servicios bancarios online han pasado de ser una mejora a ser una necesidad, por lo que garantizar su continuidad y fiabilidad 24 horas al día frente a ataques es una de las prioridades.

Es necesario concienciar a la sociedad sobre el peligro real que supone el cibercrimen y hasta donde está dispuesto a llegar. Hemos visto como en los peores momentos de la pandemia han sido atacados los sistemas de información de algunos hospitales.

¿Qué tecnologías de seguridad considera imprescindibles para una empresa perteneciente al sector financiero?
Todas las tecnologías de prevención de fuga de datos son esenciales para evitar la filtración ac-

"El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo"

cidental o intencionada de información sensible. Es fundamental que estas estén integradas en los canales de comunicación con el exterior para monitorizar y bloquear las transferencias de datos sospechosas. Debemos asegurar que cubren todos los canales, no solo el email sino la subida de información a través de servicios web, la extracción de información a través de los puertos del ordenador e incluso también la impresión.

Dicho esto, se debe tener en cuenta que estas tecnologías son inútiles si no se definen e implementan las políticas adecuadas de identificación y bloqueo de contenidos y, para esto, el equipo de ciberseguridad no puede trabajar de forma autónoma, necesitará de la colaboración del negocio y otras áreas. Además, hay que asegurar que se dispone de un equipo de profesionales de seguridad cualificado para analizar y responder a las alertas emitidas. Sin políticas y profesionales, la tecnología DLP tendrá las mismas capacidades de mitigación del riesgo cibernético que instalar un jarrón en nuestro centro de datos, eso sí, muy caro.

Existen muchas otras que son esenciales bajo mi punto de vista, como las tecnologías y servicios para proteger frente a ataques de denegación de servicio, la protección frente al malware, el cifrado, la protección del perímetro, y los cortafuegos de aplicación y bases de datos.

¿Qué tecnologías que todavía no están ampliamente adoptadas, cree que serán imprescindibles en los próximos años?

En los últimos tiempos han aparecido nuevas posibilidades tecnológicas para la protección de los datos que deben ser exploradas por las entidades financieras para mitigar, aún más, los ciber-riesgos asociados a estos. La información es almacenada por las organizaciones en dos formatos: de forma estructurada, como por ejemplo las bases de datos; y de forma no-estructurada, como por ejemplo las hojas de cálculo.

En lo relativo a la protección de la información estructurada, a las técnicas tradicionales de anonimización y pseudo-anonimización, ampliamente empleadas como la tokenización o el masking, se unen nuevas alternativas como el uso de la encriptación homomórfica o los datos sintéticos. Es importante disponer de un portfolio amplio y contrastado de estas técnicas, puesto que no hay ninguna de ellas que, de forma individual, pueda cubrir todos los casos de uso del negocio.

Cuando hablamos de información no estructurada la situación es todavía más compleja, puesto que existen numerosos ficheros que son intercambiados diariamente como parte de la operativa normal del negocio financiero en interacciones internas y externas. Para esto es necesario implementar tecnologías que nos permitan garantizar la seguridad de los datos durante todo su ciclo de vida, siendo especialmente importantes las tecnologías de descubrimiento de la información y clasificación de los datos. Son también muy interesantes las tecnologías denominadas genéricamente como IRM, que nos van a permitir insertar las políticas de seguridad dentro del dato (control de acceso, trazabilidad, caducidad...), disponiendo de esta forma de la capacidad de proteger la información con independencia de dónde se ubique. ■

MÁS INFORMACIÓN

BNP Paribas

Más visibilidad.
Más potencia.
Más control.

¿No pensó estar preparado/a para el EDR?
Ahora lo está.

go.kaspersky.com/es_optimum

kaspersky PREPARADOS PARA EL FUTURO

Objetivos de la ciberseguridad en las entidades financieras:

protección de clientes, dispositivos y empresa ante los ataques

EUSEBIO NIEVA,
director técnico de
Check Point Software para España y Portugal

La ciberpandemia es uno de los peligros que actualmente están amenazando a cientos de compañías. Tras los meses en los que la Covid-19 ha obligado a miles de personas a extremar las precauciones para evitar el contagio y el uso del pago por móvil o la tarjeta de crédito se han instaurado como opciones masivas. Por ello, las entidades financieras se están convirtiendo en uno de los principales objetivos de los ciberataques, sobre todo, por el rédito económico que puede llegar a reportar el atacarlas.

Desde el comienzo de la pandemia, empresas de todos los sectores se han visto obligadas a implantar el teletrabajo con el consecuente incremento de los dispositivos móviles conectados a la red, aumentando considerablemente las brechas de seguridad y mejorando las oportunidades de éxito de los cibercriminales. Los frentes para los negocios se multiplican y contar una buena defensa es la única opción.

Debido a la situación, ahora se están llevando a cabo diferentes tipos de fraude y extorsión contra la banca, para de esta forma vulnerar la privacidad de estas compañías con el objetivo de llenarse los bolsillos. Así los datos respaldan la realidad del sector, ya que según Informe Global de Amenazas DNS 2020 elaborado por IDC de la mano de EfficientIP, en el 2020 cuatro de cada cinco empresas del ámbito financiero (79%) sufrieron más de diez ciberataques DNS a lo largo del año y cada uno de ellos supuso un coste de 1,16 millones de euros de media.

Uno de los mayores desafíos que tienen que afrontar las entidades financieras es la

seguridad móvil, tanto por el lado usuario como por el de sus trabajadores. Ahora más que nunca, el acceso a redes corporativas a través de móviles no securizados es un objetivo. Para ello, Check Point Harmony Mobile protege los dispositivos móviles de los empleados de todos los vectores de ataque (aplicaciones, red y sistema operativo). Este software está diseñado para reducir los gastos generales de los administradores y aumentar la adopción del usuario, escala rápidamente, evita descargas de aplicaciones maliciosas, impide el phishing en todas las aplicaciones previene ataques Man-in-the-Middle, bloquea aparatos infectados para que no accedan a aplicaciones corporativas y detecta técnicas avanzadas de jailbreaking y rooting y vulnerabilidades del sistema operativo.

En la otra cara de la moneda encontramos cómo estas entidades financieras pueden proteger a sus clientes, sus credenciales y datos personales cuando acceden a sus apps. La mejor manera de mantenerlas a salvo de los cibercriminales es contar con una protección adecuada. Impulsado por el motor de IA contextual de Check Point CloudGuard, Check Point CloudGuard AppSec es una solución que bloquea los ciberataques contra las aplicaciones, incluyendo: la desconfiguración del sitio web, la fuga de información y el robo del inicio de sesión del usuario. Para ello, es capaz de analizar cada solicitud en su contexto y asignándole una puntuación de riesgo, para una prevención precisa, eliminando los falsos positivos y evitando los más sofisticados ataques contra una aplicación, incluidos los ataques OWASP Top 10.

> “Todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tenga conexión a su red”

Es imprescindible señalar que la banca debe contar con un software que sea capaz de proteger a la empresa de cualquier tipo de ciberataque a sus centros de datos. Esta herramienta debe mantener a salvo todos los archivos, documentación y datos pertenecientes a la propia sociedad y también de los clientes que forman parte de la misma.

Para lograr el objetivo, en Check Point Software contamos con Check Point Quantum Maestro, una solución que posibilita a las compañías ampliar fácilmente sus gateways de seguridad bajo demanda y crear nuevos servidores y recursos informáticos en la nube pública. Además, este software permite que un solo gateway se extienda hasta alcanzar la capacidad y el rendimiento de 52 en cuestión de minutos, lo que proporciona flexibilidad dinámica y un rendimiento máximo del firewall Terabit/segundo. Esta escalabilidad casi ilimitada permite soportar la alta velocidad de datos y contar con la latencia ultra baja de las redes 5G, una red que lo va a cambiar todo desde este mismo año y que será clave para todas las entidades financieras. Asimismo, hay que destacar el hecho de que llega a proteger a los entornos más extensos y con más recursos, estableciendo nuevos estándares en la seguridad de redes a hiperescala. Finalmente, es importante especificar que Check Point Quantum Maestro tiene la habilidad de extender las capacidades de seguridad Gen V de nuestra arquitectura Check Point Infinity a los entornos de hiperescala.

Si algo ha quedado claro en este último año es que todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tengan conexión a su red para mantener a salvo todos los datos confidenciales que manejan frente a los posibles ciberataques. ■

Salvaguardar las transacciones, proteger al usuario

El financiero es uno de los sectores más afectados por los ciberataques avanzados, ahora muy enfocados en la banca móvil. Proteger al usuario frente a estas amenazas es imperativo, pero sin descuidar otros vectores, como la red SWIFT o los cajeros. La ciberseguridad de la banca debe evolucionar en la misma medida en que lo hacen los servicios.

A causa de los desafíos ligados a la pandemia el uso de la banca móvil se ha incrementado, y con ello el aumento de las ciberamenazas dirigidas contra los dispositivos móviles. Ante esta realidad, Eusebio Nieva, director técnico de Check Point, explica la importancia que tiene para estas entidades desarrollar una estrategia de ciberseguridad que englobe también este canal, con la integración de soluciones avanzadas de ciberseguridad móvil en sus apps.

En Check Point trabajan con varias entidades bancarias a las que proporcionan sus servicios de seguridad en forma de un interfaz de programación de aplicaciones (API) o de un kit de desarrollo de software (SDK) que se pueda consumir. Con esto se consigue trasladar la seguridad al dispositivo desde el cual el usuario está accediendo a los servicios, pero en vez de instalarla en dicho terminal, se pone a disposición de las entidades bancarias, de modo que cuando ellos lancen su propia aplicación de consumo o de servicios bancarios esta estará asociada a los servicios de seguridad de Check Point.

Otra consecuencia de la evolución hacia una banca más móvil, y en general más digital, es que el uso de cajeros automáticos (ATM) ha descendido, al igual que el empleo de efectivo. Hoy en día, y a causa de la pandemia, el dispositivo ubicuo que casi todo el mundo utiliza para hacer pagos es un terminal móvil o una tarjeta de crédito o débito. Sin embargo, y aunque el uso de ATM se ha reducido, lo cierto es que aún se siguen produciendo ataques contra dichas máquinas, por lo que es necesario seguir invirtiendo en su protección. Asimismo, hay que tener en cuenta que la tecnología que integra el cajero es muy antigua, por lo que es trascendental ir actualizando los servicios proporcionados por el cajero, así como la tecnología asociada a los mismos.

Además de no descuidar la defensa de los cajeros automáticos, las instituciones financieras que utilizan el sistema de pagos SWIFT también deben permanecer vigilantes. Las ofensivas contra esta red se han multiplicado en los últimos años, por lo que los bancos están implementando no solo medidas de seguridad estándar, sino también protecciones avanzadas, tecnologías de análisis de fraude, machine learning… para disuadir a los atacantes sobre su explotación, y frenar o impedir las transacciones fraudulentas o los intentos de falsificación de esas transacciones en la red de comunicaciones financieras. Nieva distingue que la tecnología de protección de las tarjetas bancarias o de los dispositivos móviles aún no está a la par con la tecnología de ataque utilizada por los ciberdelincuentes. En este sentido, sería necesario que nuevas metodologías o herramientas entraran en funcionamiento a fin de asegurar las transacciones, sobre todo desde el punto de vista del usuario que es quien las realiza. Con ello se podrían evitarse los fraudes y los ataques a dispositivos móviles con troyanos bancarios, con troyanos de tarjeta de crédito, etc. que pueden ser utilizados contra los usuarios. Por tanto, esta evolución paralela de servicios y ciberseguridad debe ser prioritaria.

Protegeré las claves, protegeré las claves, protegeré las claves…

JAVIER SANCHEZ FUERTES,
Territory Sales Manager,
Data Protections Solutions Entrust

Las empresas de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las regulaciones en evolución. El Repositorio de Confianza es fundamental aquí. La identificación y la autorización de los dispositivos, el cifrado y la verificación de los datos y las actualizaciones del software tienen algo en común, y ese denominador común es la criptografía. Y la base de la criptografía son las claves de cifrado que se necesitan para firmar y validar los certificados de los dispositivos para su identificación y autorización.

La mayoría de la infraestructura desplegada en los servicios financieros utiliza claves para el correcto desarrollo de sus funcionalidades, y en la mayoría de los casos esas claves carecen de la protección adecuada.

Por lo tanto, asegurar estas claves es fundamental, y ahí es donde entra en juego el Repositorio de Confianza para proteger y gestionar las claves de cifrado a lo largo de su ciclo de vida, completamente separadas del resto del sistema con hardware robusto y controles duales para garantizar que ningún individuo o entidad pueda subvertir las políticas establecidas para el uso de las claves.

De esta manera nuestros Hardware Security Module (HSM) nShield forman parte de esta ecuación. ¿Cómo se traduce esto en el mundo financiero?

Los certificados digitales son la forma en que las diferentes partes del ecosistema de pagos establecen la confianza entre sí. Estos certificados suelen ser emitidos por una PKI que se apoya en un Repositorio de Confianza. En la raíz de una PKI se encuentran claves criptográficas fuertes y de confianza creadas en un Hardware Security Module o HSM. Los HSM de Entrust nShield proporcionan una garantía sólida y certificada a un despliegue de PKI al tiempo que facilitan la automatización de la renovación de certificados y firmas, manteniendo las claves criptográficas privadas en un entorno seguro. Pueden desplegarse en otras áreas del nuevo ecosistema de pagos allí donde se requieran servicios criptográficos desde un entorno seguro y de confianza.

Piense en monedas virtuales, seguros, préstamos, grandes minoristas, aplicaciones bancarias móviles, etc. Los HSM de uso general pueden realizar tareas como la protección y validación del PIN, y la gestión de claves, también se despliegan como parte de las soluciones de procesamiento de pagos y puntos de venta móviles con partners de la industria. No olvidando la protección de las claves de firma y el proceso de firma de código de las Apps, el elemento de relación principal entre cliente y entidad financiera.

> “Las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas”

Están surgiendo nuevos servicios de pago al realizar compras en línea o a través del teléfono móvil, especialmente en Europa. El cambio puede ser un resultado directo de la PSD2, la última Directiva de Servicios de Pago. Las organizaciones de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las normativas en evolución. Merece la pena recordar que la certificación de los HSM de nShield según NIST FIPS 140-2 y Common Criteria ofrece a los clientes la garantía de que están seleccionando un producto validado según algunas de las normas de seguridad más rigurosas.

Las organizaciones financieras también siguen adoptando tecnologías nuevas y emergentes, como la nube y los contenedores, que, si bien ofrecen posibles eficiencias y reducciones de costes, amplían la huella digital de la organización. Estas organizaciones necesitan tener el control sobre las claves de cifrado que utilizan los proveedores de nube pública y de esta manera será Entrust con el cliente quienes definan las políticas y permisos asociadas a las mismas. No es una cuestión de confianza sobre los proveedores de nube pública sino de control sobre los datos y a afrontar sus retos de seguridad en la nube.

Uno de los principales obstáculos para la adopción más amplia de Blockchain es la seguridad. A medida que las organizaciones continúan encontrando nuevos e innovadores casos de uso para Blockchain, la seguridad debe incorporarse desde el principio. Entrust ayuda a abordar los desafíos de seguridad fundamentales asociados con las implementaciones de Blockchain: creación de claves, protección del proceso de firma y protección de la lógica de consenso. Debido a que se encuentra alojado dentro de los límites seguros del HSM nShield, CodeSafe ofrece protección certificada FIPS 140-2 Nivel 3 para su código más confidencial.

En definitiva, las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas con los consecuentes riesgos que eso significa. ■

Proteger la clave para salvaguardar el dato

Los desafíos de la regulación y el cumplimiento de la seguridad de los datos son muy altos en el entorno financiero. Por ello y a medida que evolucionan las amenazas cibernéticas, la combinación de integración tecnológica y análisis avanzado es más necesaria nunca.

Por la naturaleza de su negocio, las compañías financieras siempre han tenido que ser pioneras en cuanto al uso de medidas de seguridad, y en concreto en lo que se refiere al uso de cifrado y de Módulos de Seguridad de Hardware (HSM). Ahora, cuando la digitalización avanza rápidamente y la información fluye por distintos entornos (local, cloud, IoT) esto es más importante que nunca. Sobre ello, Javier Sánchez Fuertes, Territory Sales Manager de Entrust, observa que esa actitud pionera sigue manteniéndose, y lejos de quedarse anclada en el medio de pago, ha ido extendiéndose a otros casos de uso dentro del mundo financiero, para, por ejemplo, la protección de la infraestructura de clave pública (PKI), de los procesos de firma electrónica o de los procesos de negocio, entre otros.

Por otro lado, se habla mucho de la seguridad de los datos de manera genérica, pero hay un aspecto específico que es la seguridad de los datos en reposo que a veces pasa desapercibida. ¿Cuál es el reto en estos casos?

Sobre su importancia, Javier Sánchez cree en las empresas en general y en las financieras en particular se realizan importantes inversiones para proteger el entorno de red o el endpoint, abandonando en muchas ocasiones al dato, que por sí mismo no puede defenderse. El desafío, por tanto, pasa por identificar cuáles son los datos críticos para una entidad financiera y, sobre ellos, aplicar medidas de cifrado y por supuesto de protección de las claves. No hay que olvidar que las políticas de cifrado son tan seguras como lo son la protección de las claves.

Parece que la tecnología de cadena de bloques, Blockchain, está llamada a transformar el mundo de la banca. Sin embargo, el despliegue de servicios financieros sobre esta tecnología presenta retos en cuanto a seguridad. A este respecto, Javier Sánchez explica que la adopción de Blockchain en el mundo de la banca debe hacerse con cuidado. Los clientes depositan su dinero en un banco porque confían en dicha entidad.

En este sentido, Javier Sánchez explica que en Blockchain cada transacción que se envía a un bloque va firmada y por ese motivo lleva asociada una clave, y como hay una clave necesariamente debería haber un Módulo de Seguridad de Hardware (HSM). Desde Entrust lo que se propone es la protección de esas claves criptográficas y de esos procesos de firma, incluso de consenso, para que se realicen de forma segura mediante el uso de HSMs.

Además de trabajar en la seguridad y privacidad de Blockchain, las organizaciones financieras deben cuidar y conservar también sus claves, que están más desamparadas. En este contexto, y a raíz del crecimiento de la banca digital y móvil, el número de transacciones a través de estos medios se ha multiplicado. Por ello, Javier Sánchez incide también en lo crucial que resulta salvaguardar la clave utilizada para firmar el código de una app bancaria. Es más, teniendo en cuenta que la aplicación es, al final, el instrumento de relación entre el banco y los clientes, extremar las medidas de seguridad para resguardar esta aplicación no es baladí. De hecho, hoy por hoy, es su principal herramienta de negocio, por lo que hay que custodiarla.

La amenaza del malware financiero

se mantiene constante en España

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

La seguridad financiera es una de las preocupaciones más comunes tanto para los usuarios finales como en el mundo empresarial. Y es que las ciberamenazas en este campo son cada vez más peligrosas, y afectan al bienestar económico de las víctimas, ya sean individuos u organizaciones.

Según señala nuestro último informe anual sobre Ciberamenazas financieras en 2020, España fue el tercer país del mundo y primer país europeo con mayor incidencia de amenazas financieras el año pasado. Los troyanos bancarios, que suelen emplear ingeniería social para engañar al usuario y que los descargue, implica que cualquiera pueda encontrarse en el buzón de entrada de su correo, su WhatsApp o su lista de SMS con mensajes maliciosos que pretenden infectarlo.

De hecho, la incidencia de los virus informáticos diseñados para robar credenciales bancarias se sitúa entre las principales amenazas que afrontan los usuarios en Internet y el correo electrónico es el vector de ataque más habitual. En el mismo los cibercriminales se hacen pasar por una empresa (banco, empresa de envíos…) o por un organismo oficial (la Agencia Tributaria, Correos, DGT…).

Otro de los enfoques habituales utilizados por los atacantes para obtener acceso a las cuentas de los usuarios incautos es asumir el papel de "rescatador", fingiendo ser expertos en seguridad. Los atacantes llaman a los clientes de los bancos haciéndose pasar por expertos de seguridad e informan de cargos o pagos sospechosos para posteriormente ofrecer su ayuda. Bajo ese disfraz, el atacante puede pedir a los clientes

“La clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños”

que verifiquen su identidad mediante un código enviado en un mensaje de texto o una notificación push, que detengan una transacción sospechosa o que transfieran dinero a una “cuenta segura”. También pueden pedir a la víctima que instale una aplicación para la gestión remota fingiendo que es necesaria para la resolución de problemas. Los estafadores suelen presentarse como empleados del mayor banco de la región de la víctima potencial y utilizan un identificador de llamadas falsificado para las llamadas entrantes para hacerse pasar por un banco real.

Un tercer caso clásico es aquel en el que los ciberdelincuentes actúan como “el inversor”. En este caso, los estafadores se hacen pasar por empleados de una empresa de inversión o por asesores de inversión de un banco. Llaman a los clientes ofreciéndoles una forma rápida de ganar dinero invirtiendo en criptomonedas o acciones directamente desde la cuenta del cliente, sin tener que personarse en una sucursal bancaria. Como requisito previo para prestar el “servicio de inversión”, el falso inversor pide a la víctima el código recibido en un mensaje de texto o en una notificación push. El objetivo final siempre es el mismo: engañar al usuario para que haga ‘clic’ y descargue el código malicioso en su equipo. A partir de ese momento, los ciberdelincuentes tienen acceso a la información.

En este tipo de ataques el objetivo principal suelen ser las credenciales bancarias, que luego se venden en la darkweb por precios realmente bajos. Datos de tarjetas de crédito, acceso a servicios bancarios y de pago electrónico son mercancía habitual en este tipo de mercados.

Ante este panorama, la clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños. Así, para ayudar a los particulares y a las empresas a estar protegidos frente a las técnicas de fraude en constante evolución, es importante adoptar una serie de medidas básicas como, por ejemplo, limitar el número de intentos para realizar una transacción, de manera que los ciberdelincuentes no pueden intentar introducir varias veces las credenciales. Otra recomendación que muchas entidades financieras ya han puesto en marcha es informar de forma periódica a sus clientes sobre los posibles trucos que pueden utilizar los ciberdelincuentes, con información para saber cómo identificar el fraude y la mejor manera de comportarse ante estas situaciones.

En cuanto a las medidas de protección, la recomendación es realizar auditorías de seguridad y pruebas de penetración anualmente con el fin de detectar problemas de seguridad en la red de la empresa, contar con un equipo de análisis de fraudes capaz de encontrar y analizar los métodos emergentes que utilizan los defraudadores, implementar la autenticación multifactor para minimizar la posibilidad del robo de cuentas e instalar una solución de prevención del fraude que pueda adaptarse rápidamente para identificar nuevos esquemas y métodos de ataque. ■

MÁS INFORMACIÓN

Todo sobre EDR y MDR

Inteligencia de amenazas para prevenir el fraude

En línea con su evolución tecnológica, el sector de los servicios financieros es un objetivo esencial para los ciberdelincuentes y soporta gran parte de sus ataques. Es por eso que las entidades financieras no deben bajar la guardia. Sobre este aspecto, Luis Javier Suárez, Presales Manager de Kaspersky Lab, destaca que se vienen observando una serie de tendencias dirigidas a integrar metodologías basadas en agile, en la constante evolución de los aplicativos, y que, aunque en ocasiones incluyen la seguridad en el punto inicial, no siempre es así. Por ello, es crucial no descuidar la protección y seguir estrategias DevSecOps que siempre tienen la seguridad en mente.

A esta problemática se unen otros asuntos como la heterogeneidad de sistemas o la persistencia de sistemas legacy, que contrastan con nuevos desarrollos y la evolución hacia otros entornos como cloud. Sobre la nube, Luis Javier Suárez cita la falta de visibilidad como un inconveniente acuciante, ya que no tener conocimiento de lo que allí ocurre puede derivar en peligros como el Shadow IT.

El ritmo de evolución de las tecnologías también tiene que ser tenido en cuenta, sobre todo, porque es bidireccional. Bajo esta premisa y para poder contrarrestar ataques cada vez más sofisticados, es importante contar con servicios o programas de inteligencia de amenazas que ayuden a identificar y analizar las ciberamenazas dirigidas contra la empresa.

Sin embargo, añadir mayor seguridad puede perjudicar la experiencia del usuario, algo que en este sector es muy importante. ¿Cómo se puede aplicar seguridad sin impactar en la experiencia de usuario?

Para Luis Javier Suárez transformar la seguridad en algo que no sea invasivo e incómodo para la experiencia del usuario es complicado, máxime cuando desde el punto de vista de gestión de proyectos se pone mucho foco en esta experiencia. En este sentido, observa que existe una tendencia en el mercado hacia la integración de plataformas o entornos que sean Secure by Design, los cuales, por otra parte, sería conveniente acompañar también de un ciclo de adopción y mantenimiento. Además, no hay que olvidar que la integración de nuevas tecnologías puede traer consigo nuevos vectores de ataque y que tanto el actual auge del comercio electrónico como la preponderancia del cliente como eje central de la experiencia (customer centric) hacen necesaria la existencia de sistemas para apoyar esa seguridad. También debe haber una capa de información (sistemas antifraude) que permita detectar posibles campañas a fin de poder actuar en la fase más temprana.

A raíz de la creciente digitalización y teniendo en cuenta la sensibilidad del activo que aquí se gestiona, el dinero, Luis Javier Suárez valora que, aunque no habrá grandes cambios en cuanto a técnicas de ataque, si se incrementarán las campañas de ransomware dirigido, ataques contra cajeros automáticos (ATMs) y otros fraudes derivados del aumento de los canales digitales. El auge del mercado cripto también traerá consigo campañas focalizadas, desde phishing a otras más sofisticadas.

Por ello, y para asegurar la protección de sus activos, Luis Javier Suárez incide en la importancia de la concienciación de empleados y usuarios, y en la resiliencia. En este contexto, recomienda la adopción de tecnologías Endpoint Detection and Response (EDR), que permiten tener una visibilidad extendida de lo que ocurre dentro del entorno, y también la implantación de un Plan de Respuesta a Incidentes para, llegado el momento, poder aplicar una serie de medidas para contrarrestar el incidente. Este plan ayudará a alcanzar un nivel mayor de resiliencia.

Pagos, transacciones y dinero digital:

una realidad que ha venido para quedarse

JESÚS RODRÍGUEZ,
CEO Realsec

Hace algo más de un año todo cambió en nuestras vidas y un claro ejemplo de ello es la diferente forma en la que hoy compramos y hacemos uso de los medios de pago, donde la transformación digital es la protagonista de esta nueva situación social y económica.

Todo esto, se evidencia en diferentes acciones como el incremento de las compras a través de los sistemas de comercio electrónico, cuyo crecimiento, durante 2020 en España, ha sido de un 67% junto con la proliferación de la banca electrónica y la banca móvil, que ha pasado de un 44% a un 57% en su ratio de uso. Así mismo, se ha multiplicado el uso de las Apps de pago sobre teléfonos móviles, lo que se conoce como Open Banking (Amazon Pay, Samsung Pay…), las tarjetas virtuales prepago, los sistemas wallets, los pagos contactless, el Internet de los Pagos (IoP) a través de dispositivos inteligentes conectados en la red de Internet de las Cosas y la tokenización de las tarjetas. Todo ello, sumado a una gran expansión de nuevos agentes financieros como las Fintechs y la consolidación de las "finanzas descentralizadas" o DeFi, donde tienen su origen las criptomonedas, los smarts contracts y las Apps construidas en tecnología Blockchain.

El número de transacciones de este nuevo ecosistema financiero digital representa un porcentaje superior a las operaciones de pago en efectivo, cuyo descenso en 2020 se cuantifica en un 45%, aunque no debemos olvidar que, para su efectividad, transparencia y confianza, es fundamental implementar una securización robusta.

“Esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales”

El riesgo de fraude online crece, exponencialmente, asociado al crecimiento de los medios de pagos digitales; es por ello, que las entidades financieras necesitan reforzar la seguridad implementando medidas como la autenticación de doble factor en base a la Directiva PSD2 o mayor transparencia y gobernanza en el caso de utilizar tecnologías como Blockchain para realizar pagos digitales transfronterizos, operaciones de compensación bancaria o intercambio de cédulas de pago internacional. Así como en la gestión confiable de los cripto-activos o la securización de los entornos de pago asociados al Internet de las Cosas “Blockhain of Things”

Aunque hoy la tecnología disruptiva Blockchain por inmutabilidad, descentralización y transparencia puede considerarse confiable para determinados procesos de negocio, podemos robustecerla, en el ámbito financiero, con la implementación de módulos criptográficos HSM (Hardware Security Module) que fortalecen la infraestructura de la red Blockchain, ya sea ésta pública, privada o híbrida, tanto para las operaciones financieras, gestión de criptomonedas y la protección de otros procesos de negocio.

El crecimiento de los pagos digitales en más de un 30%, a nivel mundial durante el último año, junto con los nuevos canales digitales, en detrimento del uso del efectivo, sumado a la proliferación de las monedas digitales (CBDC) y criptodivisas en un mercado no regulado (salvo excepciones como el caso del e-Yuan chino, pero con anuncios y expectativas de una futura regulación por parte de muchos Bancos Centrales del mundo, como el BCE con la creación de Euro Digital) supone asumir la realidad de una nueva economía. La que muchos denominan “Cripto-economía”, puesto que aquí la criptografía desempeña un papel clave para la protección y la seguridad de los activos financieros que traerá consigo una mayor adaptación y confianza, tanto a los usuarios del nuevo espectro digital como a las entidades financieras, interesadas siempre en minimizar los riesgos de seguridad en los medios de pago, como la suplantación de la identidad o el fraude.

Sin duda, esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales en el que las nuevas tecnología disruptivas, como el Blockchain, cumplan con los mismos o superiores niveles de exigencia, en materia de seguridad, a los exigidos por la Banca, como es el uso una criptografía robusta para proteger las transacciones financieras, avalada por un organismo acreditado internacionalmente, como la Certificación PCI HSM PTS en el ámbito de los medios de pago.

Para conocer más sobre la situación y el estado del arte de esta tecnología en España y América Latina les animamos a leer el II Informe de Blockchain de REALSEC, elaborado junto con IDC. ■

La ciberseguridad como factor de confianza

El sector financiero se enfrenta a un ambiente regulatorio estricto, con muchas normas que acatar y exigencias en cuanto a protección y seguridad muy explícitas. Tal situación, no obstante, ha favorecido que se haya convertido en uno de los nichos más avanzados en cuanto a ciberseguridad. A este respecto, Jesús Rodríguez, CEO de Realsec, destaca que, si bien antes de la pandemia la banca ya trabajaba en determinados procesos de transformación digital, el confinamiento ha acelerado extraordinariamente este desarrollo. Sin embargo, el crecimiento de la banca electrónica y móvil ha repercutido también en un incremento de los ciberataques y en un mayor riesgo de fraude, activando la demanda de soluciones y sistemas de cifrado para la protección de transacciones y de otros procesos de negocio.

No obstante, Jesús Rodríguez aclara que la banca siempre ha cuidado mucho todo lo relacionado con ciberdelincuencia. Es un factor de confianza, el mayor de todos, por lo que a medida que el nivel de ciberriesgo ha evolucionado, se han ido implantado soluciones de protección para mitigar estas amenazas. Adicionalmente, y en lo que respecta a la parte de medios o sistemas de pago, la tecnología de criptografía bancaria ha prosperado como sistema de protección, al igual que la orientada al tratamiento seguro de las transacciones electrónicas, la protección de la información y de los datos mediante el cifrado.

La usabilidad de la tecnología de blockchain también se ha extendido, y no solo para la gestión de criptoactivos, sino para otros procesos de negocio como la compensación electrónica o los pagos transfronterizos. Sin embargo, esta tecnología debe considerarse, además de por sus capacidades de eficiencia y trazabilidad, por sus características de seguridad. Los bloques pueden ser cifrados y dentro de la tecnología de blockchain se pueden utilizar contratos inteligentes (smart contract).

Aunque fue el año pasado cuando la normativa PSD2 entró en vigor, su acatamiento ha estado posponiéndose durante los últimos años a través de varias moratorias. En ese tiempo, las entidades bancarias han estado preparándose, trabajando en una doble dirección: el desarrollo de APIs, para permitir el acceso a nuevos actores en el ámbito financiero y en la autenticación de doble o triple factor para cumplir con la directiva de pagos PSD2. Al respecto de su acatamiento, y aunque no se puede decir que ningún banco español esté cumpliendo con la directiva en sí, si se puede aseverar que no todas las entidades financieras están utilizando soluciones de tokenización para su observancia. Dichas soluciones han sido reemplazadas por SMSs con una clave adjunta que el usuario utiliza para demostrar que es quién realmente dice ser durante la operación financiera.

La banca está ahora mismo viviendo una situación revuelta; una fase de adaptación. La crisis económica generada por la pandemia está obligando a sus entidades a adoptar una serie de medidas para no perder competitividad y rentabilidad. Así, y aunque los bancos llevan tiempo trabajando en la gestión de activos, en las criptomonedas, se está produciendo una tendencia creciente a cambiar activos financieros y efectivo por criptodivisas. Sobre ello, Jesús Rodríguez considera que según avance la regulación, esta realidad irá asentándose. Previsiblemente se avanzará hacia un euro digital regulado (algo en lo que está trabajando el Banco Central Europeo) y se extenderá la usabilidad del blockchain hacia otros procesos de negocio, como los arriba comentados.

Síguenos en:

SOLUCIONES DE CIBERSEGURIDAD_

- HSM de Propósito General
- HSM Financiero
- Remote Key Load
- Soluciones de Cifrado, Firma Digital y Sellado de Tiempo
- Soluciones PKI
- Ciberseguridad Blockhain&IoT

www.realsec.com

realsec
La clave para proteger su negocio

OFICINAS CENTRALES
C/ Infanta Mercedes 90. Planta 4. 28020 Madrid
Tfno.: +34 91 449 03 30 - E-mail: info@realsec.com

MÉXICO
Avda. Ejército Nacional, 1112 Despacho 404 Piso 4
Colonia Los Morales C.P. 11510. Ciudad de México
Tfno.: + 52 (55) 44 35 00 46 - E-mail: infomexico@realsec.com

USA
303 Twin Dolphin Dr Suite 600 Redwood City, CA 94065
Tfno.: +1 (650) 632 4240 - E-mail: sales@realsec.com

SINGAPUR
REALSEC Inc.12 Marina Boulevard.
MBFC Tower 3. Level 17-01. Singapore 018982
Tel. +65 6809 5001 • infoapac@realsec.com

El sector financiero, en el punto de mira de los cibercriminales

IGOR UNANUE,
CTO S21sec

La ciberdelincuencia es, desafortunadamente, un factor de riesgo para varios sectores como el sanitario, el público o el educativo, pero la industria financiera es y seguirá siendo uno de los sectores más vulnerables a los ciberataques. Desde siempre, el sector financiero ha estado expuesto al cibercrimen, ya que en el 90 por ciento de los casos la motivación de los atacantes es puramente económica. Tal y como detectamos en 2019, los ataques hacia entidades financieras aumentaron de forma notable y los cibercriminales encontraron vías muy sencillas de penetración en dichas organizaciones a través de simples ataques de ingeniería social vía correo electrónico. Desde entonces, los cibercriminales cuentan con más y mejores recursos.

Este año, además de sufrir el típico malware financiero, el sector financiero podría ser víctima de ataques de robo de información relacionada con credenciales bancarias, datos de tarjetas de crédito o sufrir ataques Zero-Day, donde los cibercriminales se aprovechan de las vulnerabilidades y utilizan códigos maliciosos para desplegar los ataques. Muchas entidades financieras ya cuentan con sus propios sistemas de protección para hacer frente a ataques recurrentes como el phishing o el envío de información falsa mediante correo electrónico. No obstante, hay muchos nuevos software maliciosos que van surgiendo y que no son tan fáciles de identificar.

En este sentido, desde S21sec nos encargamos de monitorizar la actividad de los cibercriminales y de detectar todas las nuevas

“Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque”

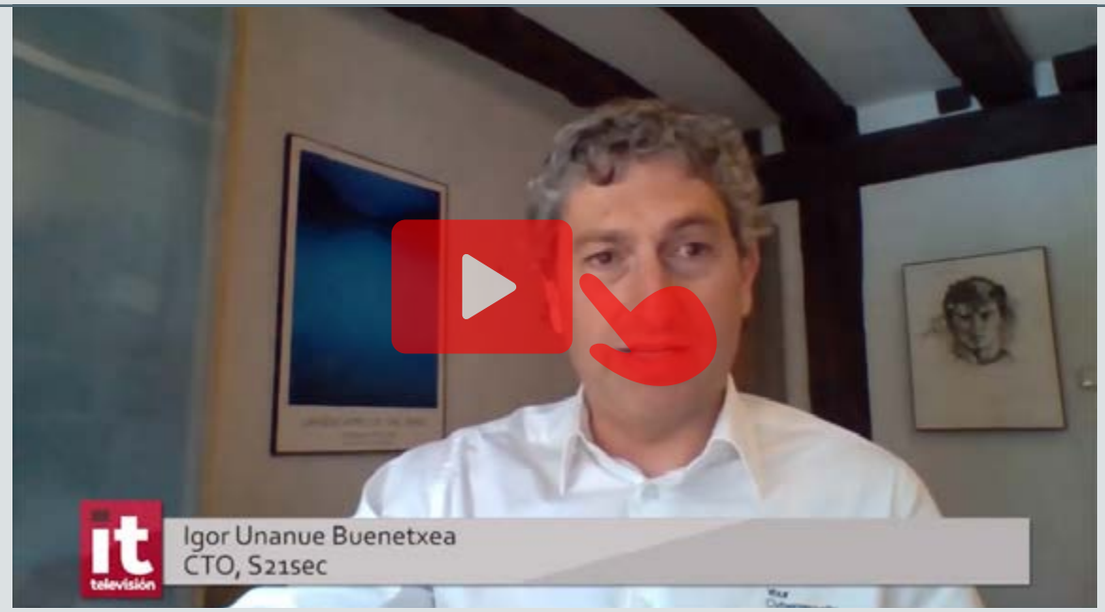
amenazas que puedan afectar al sector financiero. Cada día, se identifican casi 15.000 malware diarios y la clave reside en averiguar a qué tipo de entidades afectan y qué banco en concreto está siendo víctima de dicho ataque. Nos encargamos de recuperar la información robada, además de proporcionar nuestros servicios de SOC y equipos de servicios profesionales que trabajan en proyectos de integración, consultoría o en la parte de auditoría. La consultoría en entidades financieras es muy importante debido al cumplimiento normativo que les impone implantar medidas de seguridad.

Otro aspecto a tener en cuenta es que debe haber un equilibrio entre la seguridad y la experiencia del cliente; es decir, añadir mayor seguridad puede perjudicar la experiencia del cliente, y en el sector financiero, no es fácil limitar el acceso mediante seguridad porque las entidades deben seguir funcionando. Además, la pandemia ha impulsado el teletrabajo y el uso de la banca online, con lo que es complicado imponer una seguridad total en este sentido. La única solución al respecto es estar alerta y seguir controlando la seguridad en paralelo, identificando los puntos más débiles que puedan suponer un riesgo para la compañía. En S21sec consideramos que esa es la gestión del riesgo que toda entidad y compañía financiera debe realizar, ya que imponer medidas de seguridad extremas supondría entorpecer el funcionamiento de la compañía, debiendo hacer un esfuerzo por identificar correctamente el punto de entrada más vulnerable para así implantar medidas de seguridad, como por ejemplo establecer reglas de correlación, puntos de control y sistemas preventivos.

No hay que olvidar que los cibercriminales siempre llevan a cabo sus ataques aprovechando las vulnerabilidades de los grandes fabricantes y, por ello, es imprescindible mantener los sistemas parcheados y protegidos para evitar cualquier fuga de información; es algo que el sector financiero debe tener muy claro para protegerse contra los ciberataques. Asimismo, también es importante saber que muchos de los ataques recientes han sido silenciosos y difíciles de detectar porque utilizan nuevos sistemas de ataque, de manera que los ataques son lentos y no se identifican inmediatamente.

Por ello, desde S21sec recomendamos a todo el sector financiero tener un sistema de monitorización constante y estar siempre alerta ante nuevas amenazas. Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque. Además, también es recomendable que estén al tanto de todo lo que ocurre en las redes, visualizar las vulnerabilidades y tener en cuenta que las entidades financieras estarán siempre expuestas al riesgo de los ciberataques. ■

Seguridad gestionada para mitigar los riesgos



El sector financiero siempre ha estado en el punto de mira de los cibercriminales, dado que, además, en el 90% de las ocasiones estos actores se rigen por una motivación financiera. No obstante, Igor Unanue Buenetxea, CTO de S21sec, reconoce que no es el que sufre el mayor número de ataques, aunque si al que llegan los más tradicionales, como los dirigidos contra sus clientes.

Aunque el malware financiero siempre ha existido y seguirá en activo, desde S21sec consideran que, durante 2021, tendrán mayor relevancia las vulnerabilidades Zero Day y los ataques dirigidos destinados al robo de información (credenciales, datos personales, tarjetas de crédito).

Asimismo, Unanue alerta sobre el cibercrimen bancario, el cual se está expandiendo sin pausa, y al que desde la propia empresa hacen frente a través de la monitorización de los cibercriminales, para no dejar escapar malware nuevo. En este contexto, S21sec analiza diariamente más de 15.000 muestras, lo que le permite averiguar a qué tipo de entidades afecta, incluso un banco concreto. Adicionalmente, S21sec recupera credenciales robados, monitoriza constantemente la Deep Web en busca de tarjetas de crédito e información robada a las entidades financieras (análisis en profundidad continúo). También ofrece servicios de seguridad gestionada en remoto (SOC) 24/7 y cuenta con un equipo de servicios profesionales que trabaja en proyectos de integración, auditoría y consultoría.

Sobre este último, Igor Unanue reconoce que la acción de consultoría es muy importante para este tipo de organizaciones, ya que deben implementar medidas de seguridad concretas para acatar el cumplimiento normativo. Estas, además, deben estar muy bien implantadas, ya que serán auditadas por el Banco Central Europeo (BCE).

No obstante, a veces, añadir mayor protección pueden perjudicar la experiencia del usuario; por lo que el reto está en obtener ese equilibrio para aplicar seguridad sin impactar en la experiencia de usuario

A este respecto, Igor Unanue comenta la dificultad que entraña conjugar ambos aspectos. Limitar el acceso o las comunicaciones con mecanismos de seguridad no es tan sencillo, más si cabe, ahora, con la mayor parte de las plantillas teletrabajando y los clientes operando a través de banca digital. Hay que dejar abiertas ciertas puertas para que la comunicación fluya, la economía funcione, mientras se controla la seguridad, sobre todo en los puntos de mayor riesgo. Para ello es necesario llevar a cabo una monitorización 24/7, desplegar sistemas preventivos, reglas de correlación… En definitiva, aplicar medidas de seguridad optimas sobre ese punto, para monitorizar y no siempre bloquear.

Además de desplegar una estrategia de gestión de riesgo basada en la defensa de los puntos más sensibles, desde S21sec recomiendan vigilar las vulnerabilidades Zero Day que se producen, ya que últimamente se han detectado un alto número en productos de grandes fabricantes (desplegados en organizaciones financieras). En este sentido parchear los sistemas es clave, así como mantenerlos actualizados y monitorizados. También el despliegue de un sistema de detección Endpoint Detection and Response (EDR) para poder detectar movimientos laterales, de malware y otro tipo de ataques en los puestos finales y servidores, además de monitorizar y gestionar todo lo que ocurre en las redes y que les pueda aplicar a ellos como entidades financieras. No en vano, siempre van a estar en el punto de mira de los ciberdelincuentes.

Gestión de la seguridad de los datos en tiempos de crisis para las instituciones financieras

ALFONSO MARTÍNEZ,
Country Manager Iberia, Thales Digital Identity & Security

En una crisis mundial sin precedentes como la de la COVID-19, las organizaciones que han implantado nuevas tecnologías y han elaborado un enfoque coherente de su planificación de la continuidad de la actividad y de gestión de crisis, parecen salir mucho mejor paradas.

Esto es especialmente cierto para las instituciones financieras que ahora se enfrentan a nuevos retos de ciberseguridad debido a la pandemia. Según el último informe Modern Bank Heists, la pandemia de COVID-19 se ha relacionado con un aumento del 238% en los ciberataques contra bancos de todo el mundo.

Dado que una filtración de datos puede afectar significativamente a múltiples funciones dentro de una organización, la protección de los datos debe ser responsabilidad de todos los departamentos, además del equipo ejecutivo, para garantizar la continuidad del negocio sin fisuras.

Para ilustrar esto aún más, a continuación se muestra cómo las brechas de datos pueden afectar a funciones cruciales en una institución financiera:

1. FINANZAS

Según el "Informe sobre el coste de una filtración de datos en 2019" ("2019 Cost of a Data Breach Report ") realizado por el Ponemon Institute, el coste medio de una brecha de datos se cifra en 3,92 millones de dólares a nivel mundial. Esta cifra es testimonio del importante daño financiero que cualquier in-

“La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad”

cidente de brecha de datos puede causar a una organización.

2. LEGAL

La mayoría de las normativas de protección de datos, como el Reglamento General de Protección de Datos (RGPD), el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS)... obligan a seguir procesos estrictos para proteger los datos sensibles y prescriben sanciones rigurosas en caso de incumplimiento. El incumplimiento de estos mandatos legales puede costar caro a una empresa, como ha experimentado recientemente el operador de telecomunicaciones italiano TIM, que ha sido sancionado con 27,8 millones de euros por la Autoridad de Protección de Datos italiana, Garante, por incumplimiento del GDPR.

3. LÍNEA DE NEGOCIO (LOB)

Las brechas de datos pueden comprometer drásticamente las aplicaciones empresariales básicas, como los sistemas de gestión de créditos, los sistemas de gestión de las relaciones con los clientes (CRM), los sistemas de bases de datos de tarjetas de crédito/débito, etc. La indisponibilidad de estas aplicaciones críticas (que a menudo son el objetivo de los piratas informáticos) puede causar una pérdida significativa de la confianza de los clientes y del negocio.

En este contexto, es fundamental que las instituciones financieras refuercen su resistencia cibernética con herramientas y soluciones adecuadas.

La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad.

A continuación, se presentan tres mejores prácticas para construir una ciberseguridad sin fisuras para una óptima protección de los datos de la empresa.

1. Cifrar los datos sensibles

Busque en los servidores de archivos, las aplicaciones, las bases de datos y las máquinas virtuales los datos en reposo, y rastree los datos en tránsito que fluyen por la red corporativa entre ubicaciones lejanas. Una vez identificados y rastreados estos datos sensibles, es crítico cifrarlos para hacerlos inútiles a los hackers en caso de un ciberataque.

2. Almacenar y gestionar de forma segura las claves de cifrado

Las claves de cifrado pasan por múltiples etapas a lo largo de su vida: generación, distribución, rotación, archivo, almacenamiento, copia de seguridad y destrucción. Gestionar estas claves en cada etapa de su ciclo de vida a través de una solución de gestión de claves centralizada, es fundamental para la protección de los datos.

3. Implantar políticas sólidas de gestión de accesos

Implemente políticas sólidas de gestión de acceso para evitar el acceso no autorizado a los datos cifrados y a las claves de cifrado. Esto es especialmente importante en condiciones de trabajo remoto, para garantizar que sólo el personal autorizado pueda acceder a los datos sensibles en función de la necesidad de conocerlos.

Thales ha estado a la vanguardia para ayudar a las organizaciones a proteger de forma cohesiva sus datos empresariales, y continuar con la actividad habitual incluso en situaciones de crisis. Las soluciones de cifrado de datos y de gestión de claves de Thales, protegen los datos sensibles en todos los dispositivos, procesos, plataformas y entornos, cumpliendo al mismo tiempo con todos los mandatos normativos. ■

Proteger las claves y la gestión de su ciclo de vida

En un mundo cada vez más digital, el uso de certificados y claves criptográficas es imprescindible y por tanto las entidades financieras tienen que poner el foco en cómo se custodian esas claves, además de en la firma digital de las transacciones.

La banca lleva años embarcada en una evolución tecnológica orientada a la provisión de nuevos servicios de valor añadido que le permitan satisfacer las demandas y mejorar la experiencia de sus clientes, además de reducir costes. El avance de los servicios digitales es palpable, está ahí. Sin embargo, Alfonso Martínez, Country Manager España & Portugal del negocio de seguridad e identidad digital de Thales, advierte que tal desarrollo lleva aparejado un incremento de la complejidad, lo que a veces impide a estas organizaciones asegurarse de que las soluciones de seguridad de la información que implementan son realmente capaces de proteger los datos sensibles, confidenciales, que entran y salen de la entidad.

Al respecto de esta protección, Alfonso Martínez explica que las empresas financieras no deben plantearse si están cifrando bien o mal sus datos, si no, más bien, si tienen desplegada una adecuada estrategia de cifrado. De nada sirve implementar una solución de cifrado muy potente o novedosa si al final las claves criptográficas están expuestas o no están protegidas de manera conveniente. Conviene separar el tesoro de la llave, más aún cuando se está produciendo una creciente orientación a servicios en la nube. En este sentido, es primordial que los bancos mantengan la custodia y la propiedad de esas claves criptográficas con las que están cifrando datos sensibles en la nube.

El financiero es un sector hiper-regulado, con muchas normativas a las que hacer frente: PCI DSS, P2PE, PSD2 o GDPR. Sin embargo, Alfonso Martínez explica que además de poner foco en su observancia y en la implantación de soluciones tecnológicas que, como los Módulos de Seguridad de Hardware (HSM), pueden ayudar en su cumplimiento, no hay que pasar por alto otras realidades muy en boga, como el blockchain (con las criptomonedas, los smart contract, IoT) y otras más sencillas, como las facturas electrónicas o el uso de los certificados SSL de los servidores. Al final, en este mundo digital, el uso de certificados y claves es imprescindible, por lo que es muy importante cuidar la forma en que se custodian esas claves y la firma digital de las transacciones.

Sin duda, las entidades financieras no solo se enfrentan a ciberataques, muchos problemas vienen también de las brechas de datos. Sobre ello, Alfonso Martínez especifica que se han visto casos muy cercanos de filtraciones en entidades financieras en las que no solo se han revelado datos bancarios sino también personales (nombre, DNI…). El problema aquí es claro: un número de tarjeta se puede cambiar, pero una identidad u otros datos personales asociados a una cuenta particular es imposible.

Para defender esta información, que también "viaja" a las nubes, ya sea privada, pública o híbrida, Thales propone una estrategia de seguridad que pasa primeramente por descubrir dónde reside la información sensible, por ejemplo, en qué servidores, y de qué tipo de datos se trata (una tarjeta de crédito, una dirección de correo…) para seguidamente proceder a su cifrado. No obstante, ese cifrado hay que asegurarlo poniendo el foco en la custodia de las claves criptográficas y, por supuesto, en una gestión de un ciclo de vida de esa clave para saber a quién pertenece, cuándo ha sido generada o cuando caduca. Se trata, por tanto, de proteger las claves criptográficas y la gestión de su ciclo de vida.

La industria financiera ante nuevos retos y viejas amenazas

JOSÉ BATTAT,
director general de Trend Micro Iberia

En 2020 las ciberamenazas no dieron tregua –la pandemia no ayudó–, y 2021 no está siendo diferente. El cambio de año no ha modificado las ciberamenazas de siempre, implicando que el robo de datos y el ransomware -a menudo en el mismo ataque-, así como el Business Email Compromise (BEC), los troyanos bancarios, el phishing o el malware de minado de monedas sigan copando titulares. Solo en 2020 Trend Micro detectó más de 62.600 millones de ciberamenazas, el 91% de las cuales se originaron en el email. Aunque la mayoría podrían estar vinculadas con ataques automatizados y básicos, podría decirse que son las más dirigidas y personalizadas las que suponen la mayor amenaza para los resultados y la reputación de la empresa.

Algunos sectores pueden verse más afectados que otros este año, pues los ciberdelincuentes siempre van a por el fruto más fácil: las oportunidades de generar el máximo rendimiento de los ataques. Así, aunque bancos y entidades financieras siempre han destacado que la seguridad está entre sus prioridades, el sector y sus clientes siguen estando entre los principales objetivos de los atacantes, a pesar de las nuevas normativas para reforzar aún más la ciberseguridad y la privacidad. Además de las florecientes oportunidades de negocio que han abierto las empresas de e-commerce y tecnología financiera (FinTech), la constante conectividad de los dispositivos móviles inteligentes conectados 24x7 supone para los ciberdelincuentes el acceso para estudiar y observar las lagunas de seguridad, lo que sitúa a los usuarios y a las empresas financieras como

“Los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques”

blancos más fáciles para las transacciones fraudulentas y las brechas.

LA ESTRATEGIA DE SEGURIDAD COMIENZA AQUÍ

Si aún no lo ha hecho, evalúe los ciberriesgos para averiguar cuáles son sus puntos débiles y elabore un plan para solucionarlos.

El enfoque por adoptar dependerá de la predisposición al riesgo de la organización, del sector al que pertenezca y de la madurez de su posición actual de seguridad. Sin embargo, cualquier iniciativa debe incluir formación y concienciación de los usuarios; actividad que debe ser continua e incluir simulaciones de phishing y BEC del mundo real, y debe comunicarse regularmente al personal en pequeños fragmentos. Adapte las sesiones de formación a las últimas campañas de phishing y asegúrese de que sus herramientas ofrecen información detallada sobre las personas para centrarse en los empleados más débiles. Recuerde que todos los empleados, desde el director general hasta el último trabajador, deben asistir, incluidos los trabajadores temporales y los contratistas. Solo hace falta un clic erróneo para meter a la organización en problemas.

Otro enfoque que está ganando en popularidad es el de zero-trust. En un mundo de trabajo distribuido, dispositivos móviles y aplicaciones SaaS, la máxima de “nunca confiar, siempre verificar” se impone. Centre sus esfuerzos en la autenticación de los usuarios con herramientas multifactor (MFA), y despliegue la microsegmentación de red para restringir el acceso a recursos. Este enfoque también se relaciona muy bien con las herramientas SASE basadas en la nube para dar a los equipos de seguridad visibilidad de todo el tráfico entrante y saliente.

Los riesgos asociados a una plantilla distribuida también exigen herramientas de seguridad y gestión de endpoints basadas en la nube para obtener la máxima flexibilidad, visibilidad y control. La detección y respuesta a amenazas adquiere especial importancia, sobre todo las soluciones que incorporan IA para ayudar a los equipos de seguridad a priorizar la forma de hacer frente a los sofisticados ataques entrantes. De hecho, la IA seguirá facilitando la vida de los profesionales de la seguridad al detectar patrones sospechosos en el tráfico de red que los humanos podrían pasar por alto, detectando estilos de escritura anómalos en los emails de BEC y añadiendo automatización a la detección y repuesta.

En definitiva, los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques. Como parte de la “vieja guardia” que se ve obligada por la tecnología a innovar y seguir desarrollándose, la concienciación en seguridad, la vigilancia, la formación y la integridad siguen siendo constantes sólidas en el sector en todo momento. ■

Protección y visibilidad de todos los vectores de ataque

Una mayor conectividad por parte de los usuarios y una evolución hacia una banca cada vez más digital han servido como reclamo para los ciberdelincuentes, que han incrementado el ritmo y la dureza de sus embestidas contra este mercado. Bajo esta situación, José de la Cruz, Director Técnico de Trend Micro, explica cómo la evolución de los ataques y amenazas contra este sector debe ser evaluada desde una doble dimensión.

Desde el punto de vista de TI, con empleados y usuarios interactuando permanentemente con aplicaciones, se aprecia cómo el ransomware ha cobrado una nueva dimensión, con campañas masivas para infectar al mayor número de compañías posible y la subasta de la información sustraída en la Dark Web. Estos ataques son cada vez más diversificados, sobre todo, en cuanto a la tecnología que utilizan para propagarse, y los vectores han cambiado. Así, y aunque el correo electrónico sigue siendo el más utilizado para iniciar un ataque, una vez emprendido este, otros vectores se involucran en el proceso, desde la comunicación a través de las distintas redes hasta la propagación desde endpoints a servidores, cloud, etc.

En lo que respecta específicamente a la banca, las amenazas se dirigen principalmente a tres elementos: infraestructuras, aplicaciones bancarias, y empresas de terceros.

Los cajeros automáticos (ATM) son las infraestructuras más atacadas, y aunque si bien es una tendencia descendente en España, no se debe bajar la guardia. Distinto es cuando se trata de aplicaciones bancarias, con ataques que se dirigen a aplicaciones de uso móvil, y donde el objetivo es el segundo factor de autenticación; y los destinados a los servicios de la entidad expuestos en Internet, aplicaciones y APIs. Por último, destacan las agresiones a la cadena de suministro, donde hay proveedores que interactúan con el banco y que, en muchos casos, no cuentan con las mismas medidas de seguridad.

Además de prepararse para luchar contra estas amenazas, la banca tiene que lidiar también con reglamentaciones como la PSD2, o incluso la futura PSD3. Sobre ello, José de la Cruz confirma que, si bien la PSD2 empezó con brío, por su orientación a fomentar la integración y el pago colaborativo, está empezando a quedarse obsoleta. Y es que, aunque los criterios de colaboración con los que fue creada sí se están cumpliendo, no se puede considerar que exista una homogenización en cuanto a estándares, APIs o modos de colaboración con terceros. En este punto, se espera que la PSD3 establezca una estandarización a nivel de API, lo que implicará además unas condiciones de seguridad más robustas.

A la luz de cómo están evolucionando los ataques y amenazas contra el sector financiero, es vital contar con una visibilidad total de la red, para luchar contra el ransomware; implementar mecanismos de control de dispositivos, de supervisión de integridad, para salvaguardar los ATMs; y optar por un segundo factor de autenticación mucho más robusto, y que no dependa de los SMS, para proteger las aplicaciones móviles.

De igual modo, sería recomendable contemplar el enforcement de políticas de seguridad, a fin de que los usuarios acaten unos requisitos mínimos cuando se conecten con el banco; proteger aplicaciones y containers; y, cuando se trate de cloud, vigilar el CSPM (Cloud Security Posture Management) para el cumplimiento de normativas. Por último, y para defender la cadena de suministro, es clave implementar mecanismos para proteger no solo a la entidad sino también a terceros.

S21 SEC

DFIR

Digital Forensics & Incident Response

¿Sabes cómo enfrentar un incidente grave de seguridad?

No serás juzgado por el incidente, sino por la velocidad en resolverlo.

¡Contáctanos ahora para obtener más información!

marketing@s21sec.com

www.s21sec.com/es/dfir-incidentes-seguridad/

Permitir la productividad en Internet con el más alto nivel de seguridad

La misión de Check Point es "proporcionar a cualquier organización la capacidad de realizar su trabajo en Internet con el más alto nivel de seguridad". Abordan las necesidades de ciberseguridad más inminentes de las organizaciones basándonos en tres principios básicos:

1. Enfoque de prevención en primer lugar: implementar protecciones de usuario preventivas para eliminar las amenazas antes de que lleguen a los usuarios.

2. Gestión Gold Standard: panel único para gestionar todo el patrimonio de seguridad.

3. Solución consolidada: obtenga una protección preventiva completa contra las amenazas más avanzadas mientras logra una mejor eficiencia operativa.

SECURE YOUR EVERYTHING CON CHECK POINT INFINITY

En esta nueva normalidad, permiten a los clientes mantener la productividad mientras permanecen protegidos en todo lo que hacen. Dondequiera que se conecte, a lo que se conecte y como quiera que se conecte: su hogar, sus dispositivos, su privacidad y los datos de su organización deben estar seguros y protegidos de cualquier amenaza cibernética. Para hacer realidad su visión, en 2021 han recalibrado su oferta de productos Infinity para enfocarlas hacia aquellas tecnologías y capacidades que brindarán seguridad sin concesiones basada en estos tres principios básicos.

Check Point consolida más de 80 productos y tecnologías y los ha organizado en tres pilares principales: Harmony, CloudGuard y Quantum, con Infinity-Vision como base.

HARMONY: EL MÁS ALTO NIVEL DE SEGURIDAD PARA USUARIOS REMOTOS

Check Point Harmony protege a los empleados remotos, los dispositivos y la conectividad a Internet de ataques maliciosos, al tiempo que garantiza un acceso remoto seguro y de confianza cero a cualquier escala y en cualquier aplicación corporativa. Check Point Harmony proporciona conectividad segura y de punto final (SASE), como una solución consolidada y unificada basada en la nube que incluye acceso remoto fácil y seguro (basado en la adquisición de Odo), navegación segura por Internet, punto final y seguridad mó-

vil y seguridad del correo electrónico. La solución ofrece la cobertura más amplia de vectores de ataque con la prevención de amenazas impulsada con Inteligencia Artificial.

Harmony presenta tecnologías que admiten entornos híbridos seguros de trabajo desde cualquier lugar (WFA). Asegurar a los empleados en el domicilio se ha convertido en una de las principales prioridades de las organizaciones de todo el mundo. La nueva familia de productos Harmony reúne más de siete categorías de productos para proporcionar una protección preventiva completa para los usuarios remotos. Incluye conectividad segura desde cualquier lugar y un entorno de trabajo seguro en cualquier dispositivo, incluidos los dispositivos móviles, personales y administrados por la empresa, tanto cliente como sin cliente.

CLOUDGUARD: NUBE SEGURA DE FORMA AUTOMÁTICA

CloudGuard optimiza la protección de las cargas de trabajo críticas en la nube, tanto públicas como privadas. Ofrece gestión de la postura en la nube, seguridad serverless y una nueva generación de firewalls de aplicaciones web con tecnología de Inteligencia Artificial contextual que protege las API, las aplicaciones web y los servidores web alojados y on-premise.

CloudGuard proporciona seguridad consolidada y prevención de amenazas en todos los entornos, activos y cargas de trabajo de la nube. Alineado con la naturaleza ágil del desarrollo y la implementación en la nube, CloudGuard ofrece una solución tanto para los profesionales de la seguridad en la nube como para las DevOps en la nube, desde la fase inicial de DevSecOps, pasando por la seguridad de la red en la nube hasta la seguridad de las aplicaciones en la nube (WAAP), así como la protección de contenedores y funciones sin servidor.

QUANTUM: SEGURIDAD DE LA RED EMPRESARIAL PARA EL PERÍMETRO Y EL DATACENTER

En 2021, la compañía seguirá aprovechando Maestro, su solución de rendimiento escalable única y disruptiva. Acelerarán la innovación en el firewall del centro de datos con la introducción de un gateway de firewall súper rápido con un rendimiento de firewall de 200 Gbps y una latencia de menos de 3 microsegundos.

Quantum refleja la solución de seguridad de red más completa para cada organización, perímetro y centro de datos, que abarca IoT Nano-Security hasta superredes Terabit y ofrece los más altos niveles de seguridad y rendimiento para administrar entornos de centros de datos.

Las puertas de enlace de seguridad de Check Point Quantum brindan una seguridad superior más allá de cualquier firewall de próxima generación (NGFW) y están diseñadas para administrar los requisitos de políticas más complejos. Con más de 60 servicios de seguridad, estos gateways previenen la quinta generación de ciberataques.

Además, tienen previsto el lanzamiento de una nueva serie de dispositivos para sucursales y oficinas dirigidos a las pequeñas y medianas empresas: Quantum SPARK.

INFINITY-VISION

Pensada para lograr una gestión de seguridad unificada y un 100% de prevención de brechas de seguridad. Permite la administración todo el patrimonio de seguridad con Check Point Infinity Portal, una gestión de seguridad como servicio (SMaaS) basada en la nube. Entregue políticas, supervisión e inteligencia unificadas desde un solo punto. Exponga, investigue y bloquee los ataques más rápido, con una precisión del 99,9% con las capacidades SOC y XDR utilizadas por Check Point Research. ■

MÁS INFORMACIÓN

- Quantum
- Harmony
- CloudGuard
- Infitiny Vision

Entrust ayuda a las empresas de servicios financieros a mejorar la seguridad de sus datos y el cumplimiento de la normativa

Empresas de servicios financieros de todo el mundo confían en Entrust para abordar sus desafíos de seguridad. Entrust cuenta con una gama de soluciones de hardware y software para ayudar a las empresas a reducir el riesgo, cumplir los distintos reglamentos y mejorar la agilidad mientras persiguen objetivos estratégicos en torno a tecnologías emergentes de pago y transacciones:

- Sólida administración de claves.
- Entorno de ejecución seguro.
- Alineación con los estándares regulatorios y de cumplimiento global en varios entornos.
- Listo para aplicaciones de Blockchain.

LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Los módulos de seguridad de hardware (HSMs) nShield de Entrust son dispositivos reforzados y resistentes a manipulaciones indebidas que protegen los datos más confidenciales de su empresa. Estos módulos con certificación FIPS 140-2 realizan funciones criptográficas como la generación, administración, protección de claves y proceso de firma seguro, así como la ejecución de las funciones sensibles dentro de sus límites protegidos.

Para adecuarlos con su entorno específico, la familia de productos de HSM nShield incluye los siguientes modelos:

- **nShield Connect:** dispositivos conectados a la red
- **nShield Edge:** Módulo portatil con conexión USB
- **nShield Solo:** Tarjetas PCIe para integrar en dispositivos o servidores
- **nShield as a Service:** Solución por suscripción para acceder a HSM nShield en la nube

FUNCIONALIDADES DE LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Interfaces de servicios web compatible con la nube

El nShield Web Services Option Pack optimiza la interfaz entre sus aplicaciones y HSM al ejecutar comandos a través de llamadas de servicio web.

Soporte contenerizado en instalaciones o en la nube

El nShield Container Option Pack proporciona un conjunto de scripts preempaquetados que simplifican en gran medida la integración de los HSM nShield y de esa manera proveed servicios

de criptografía a las aplicaciones desplegadas en contenedores.

*** Administración de claves para sus datos en la nube con nShield BYOK**

nShield BYOK (Bring Your Own Key) le permite generar claves robustas en el HSM nShield ubicado en las instalaciones y exportarlas de forma segura a sus aplicaciones en la nube, ya sea si utiliza Amazon Web Services, Google Cloud Platform, Microsoft Azure, o las tres.

*** Optimización de operaciones utilizando Administración y Monitorización remota**

nShield Monitor y nShield Remote Administration, disponibles para los HSM nShield Solo y Connect, le ayudan a reducir los costos operativos a la vez que se mantiene informado y en control 24x7 de sus estados de HSM.

*** Configuración remota**

Los modelos nShield Connect XC ofrecen una opción de consola en serie simplificando la instalación física del HSM para alinear, cablear y aplicar potencia. Esto facilita la implementación y la reimplementación sin necesidad de revisitar el centro de datos.

*** Arquitectura altamente flexible de Security World**

La arquitectura de Security World de nShield admite HSM nShield de Entrust mediante la creación de un entorno de administración de claves flexible y exclusivo. Con Security World de nShield, usted puede combinar diferentes modelos de HSM nShield para construir un ecosistema unificado que ofrece escalabilidad, perfecta tolerancia a fallos y balance de carga.

SOLUCIONES DE CIFRADO DE WORKLOAD, GESTIÓN DE CLAVES INTEGRADA PARA ENTORNOS MULTI-NUBE

Gestión universal de claves para workload cifrados

Entrust KeyControl es un servidor KMIP certificado por VMware, escalable y con muchas funciones, que simplifica la gestión de claves para los workload cifrados. Sirve como KMS para los clientes encriptados de VMware vSphere y vSAN, así como para otros productos compatibles con KMIP.

Cifrado de datos, gestión de claves multi-nube y seguridad del workload

Entrust DataControl asegura las workloads multi-nube a lo largo de su ciclo de vida y reduce la complejidad de proteger las cargas de trabajo a través de múltiples plataformas de nube. Funciona en las instalaciones y con las principales plataformas de nube pública, así como con soluciones de hiperconvergencia y almacenamiento. DataControl incluye el servidor de gestión de claves (KMS) de Entrust KeyControl, certificado por VMware.

ALIANZAS CON LÍDERES DE LA INDUSTRIA

Entrust a través del programa de sus socios tecnológicos, colabora para integrar los HSM nShield en una variedad de soluciones de seguridad incluyendo la creación de credenciales y PKI, seguridad de base de datos, firma de códigos, firmas administración, gestión de cuentas privilegiadas, entrega de aplicaciones, inteligencia en la nube y los big data. ■

MÁS INFORMACIÓN

- Uno de los diez bancos más importantes del mundo implementa los HSMs de Entrust para ofrecer servicios fiables y de confianza a sus clientes y colaboradores
- Protección de Blockchain
- Estudio Global de Tendencias de Cifrado 2021
- Protección de claves en entornos híbridos

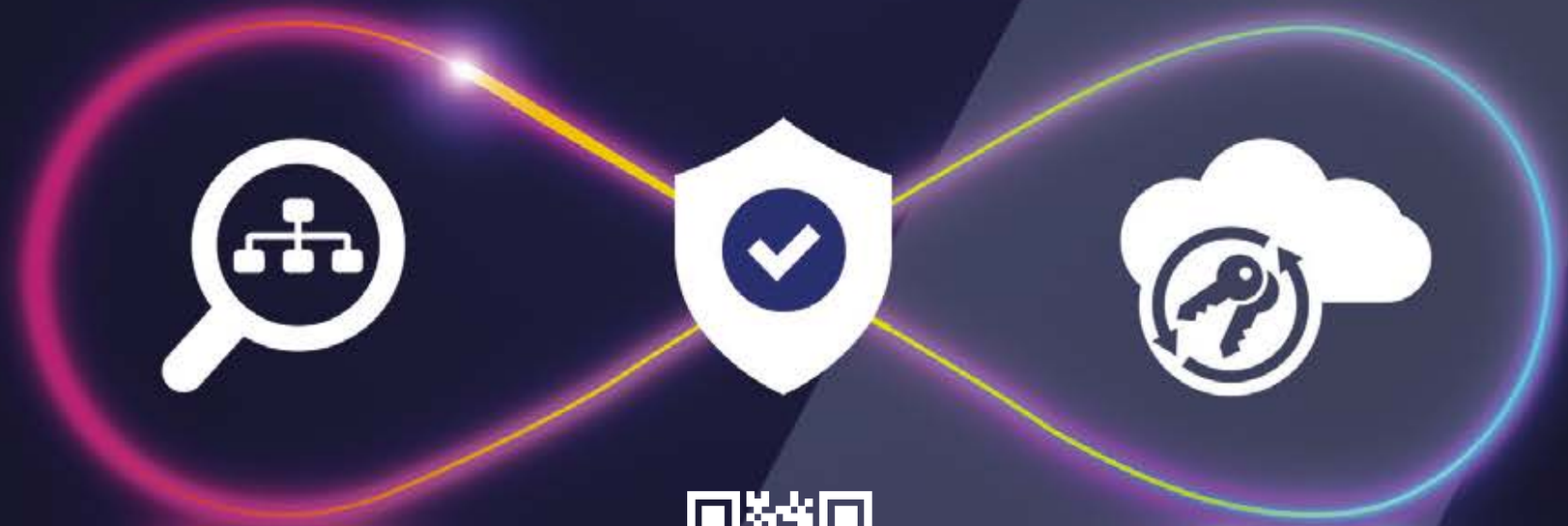
cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar Proteger Controlar



Empiece a localizar, proteger y controlar sus datos hoy mismo

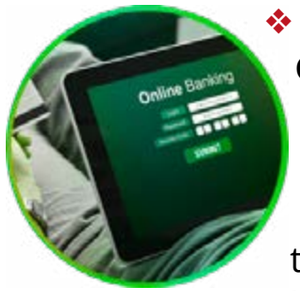
Protección para entornos financieros

RealSec dispone de una serie de soluciones de seguridad, tanto de propósito general como orientadas al segmento financiero. Aquí repasamos algunas de ellas.

SOLUCIONES DE CIBERSEGURIDAD

❖ **HSM de Propósito General/ Cryptosec LAN**

Se trata de un servidor criptográfico en red, de altas prestaciones y seguridad, diseñado para servicios de cifrado y aplicaciones de firma digital, independientemente del sistema operativo dónde éstas residan. Ofrece generación, almacenamiento y custodia de claves y certificados capaces de integrarse con aplicaciones de firma electrónica, PKI, cifrado de archivos y BBDD, blockchain...



❖ **HSM Financiero / Cryptosec Banking**

HSM financiero para pagos en red, de muy alto rendimiento, que proporciona toda la operativa y funcionalidad criptográfica específica para el ámbito de Banca, Fintech y la industria de los Medios de Pago. Cumple con todos los requerimientos y estándares definidos por el consorcio PCI (VISA, MASTERCARD...).

❖ **Remote Key Load / Cryptosec RKL**

Automatización de la carga de Claves en los ATM utilizando cifrado asimétrico, en sustitución del antiguo proceso de carga manual, tan costoso como ineficiente. Es la solución del mercado más avanzada, madura y eficiente que ofrece servicio multiempresa y está homologada por las marcas más importantes y reconocidas de ATM internacionales, cumpliendo con los requerimientos definidos por el consorcio PCI.

SOLUCIONES CIFRADO Y FIRMA DIGITAL

❖ **Servidor de firma digital/ CryptoSign Server**

Servidor Integrado de Firma Digital que incluye en un único dispositivo (hardware y software) los elementos necesarios para que, en un entorno de red, se pueda realizar cualquier proceso de firma con las mayores garantías de seguridad y gestionar los certificados digitales.

❖ **Autoridad de Sellado de Tiempo/ Cryptosec Openkey TSA**

La Firma Digital asegura quien ha realizado una determinada acción, pero no es válida para certificar que la acción se ha producido en un determinado instante de tiempo. Para ello, se requiere de una Autoridad de Sellado que afirme y certifique que los documentos electrónicos firmados han existido desde un determinado momento, y que son válidos desde ese instante.

❖ **Servidor de cifrado y firma digital de correo electrónico/ Cryptosec Mail**

Sistema centralizado de firma digital y/o cifrado del correo electrónico capaz de alma-

cenar y administrar, de forma segura, las claves de los certificados ya que está orientada a minimizar los riesgos del «Phishing» y a conseguir la total confidencialidad del contenido de los correos mediante su encriptación.

❖ **Autoridad de Validación/ Cryptosec Openkey VA**

Con la Autoridad de Validación podemos conocer el estado de revocación de los certificados digitales emitidos bajo una determinada infraestructura. ■

AUTORIDAD DE SOLUCIONES PKI

❖ **Certificación/ Cryptosec Openkey CA**

La Autoridad de Certificación es el elemento más importante y al que más hay que proteger en una infraestructura de clave pública (PKI). Es el componente de confianza emisor de los certificados y que determina su validez en el tiempo.

❖ **Autoridad de Registro/ Cryptosec Openkey RA**

La Autoridad de Registro es el punto de acceso de los usuarios finales a la Autoridad de Certificación. Al mismo tiempo que es el instrumento en el que se generan las solicitudes de certificación y las solicitudes de revocación.

MÁS INFORMACIÓN

- Segundo Informe Blockchain
- Cifrado y Firma Digital para Organizaciones Inteligentes
- Fintech y Banca. Tendencias de seguridad & HSM

Cobertura completa de riesgos de ciberseguridad en los procesos de negocio

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

S21sec es, tal y como se define a sí misma, "la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones".

Una plantilla de más de 500 expertos refleja las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC

global distribuido en cuatro localizaciones, garantizando la integridad de múltiples organizaciones en España, Portugal y México.

S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

Una plantilla de más de 500 expertos re-fleja las capacidades de S21sec para inves-tigar, detectar y prevenir amenazas

- **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
- **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
- **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
- **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
- **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
- **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse.

PROPUESTA DE SOLUCIONES

S21sec aúna soluciones diferentes de manera transversal y está diseñado en torno a cinco necesidades:

1. **Identificar:** análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.
2. **Proteger:** diseño y despliegue de arquitecturas y tecnologías, servicios de formación y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

3. **Detectar:** SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.
4. **Responder:** CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.
5. **Recuperar:** Continuidad de negocio y planes de respuesta ante ciber-desastres. ■

MÁS INFORMACIÓN

- Threat landscape report
- Test autoevaluación cyberGRC

Soluciones de cumplimiento y seguridad de datos para la banca y servicios financieros

Los proveedores de servicios financieros de todo tipo están ampliando sus ofertas para competir a escala global, ahorrar costes y mejorar la experiencia del cliente con servicios de valor añadido. Pero a medida que evolucionan los servicios financieros, deben asegurarse de que sus soluciones de seguridad TI sean realmente capaces de proteger los datos confidenciales que se adquieren y transmiten.

Thales ofrece soluciones integrales de gestión de acceso y protección de datos que aseguran los datos en dispositivos, procesos y plataformas in situ y en la nube. Estas soluciones ayudan a las organizaciones a cumplir con los requisitos de cumplimiento de los servicios financieros, facilitan la auditoría de seguridad, protegen a sus clientes y evitan el daño a su reputación causado por brechas de datos.

En cuanto a seguridad, el sector financiero se enfrenta a varios desafíos:

- **Cubrir los requisitos de cumplimiento de los servicios financieros.** El cumplimiento normativo puede llegar a ser abrumador para los servicios financieros. Las normativas que abarcan requisitos de seguridad de datos incluyen PCI DSS para información relacionada con tarjetas de crédito, el RGPD y PSD2 en la UE, SOX/J-SOX, leyes de notificación de brechas de datos y de residencia locales, y muchas más en todo el mundo.
- **La protección de los datos.** Para evitar multas costosas y proteger su reputación, las empresas del sector bancario y financiero y sus ejecutivos deben salvaguardar los datos financieros confidenciales contra la exposición accidental, información privilegiada deshonesta, APT y otras amenazas conocidas y desconocidas. Y no solo deben existir procedimientos para proteger los datos, sino también para identificar y alertar a la organización cuando se produce un acceso no autorizado.

¿CÓMO THALES LES PUEDE AYUDAR?

Thales cuenta con una oferta de soluciones en diferentes áreas que incluyen:

✱ **Soluciones de cifrado.** Las soluciones de protección de datos CipherTrust Transparent Encryption y CipherTrust Application Data Protection , incluídas en la solución CipherTrust Data Security Platform de Thales, proporcionan un único marco extensible para proteger los datos en reposo bajo los diversos requisitos de la industria de servicios bancarios y financieros en la más amplia gama de plataformas de sistemas operativos, bases de datos, entornos de nube e implementaciones de Big Data. El resultado es un bajo costo total de propiedad, así como una implementación y operación simples y eficientes.

✱ **Administración de claves robusta.** Las soluciones de administración de claves de Thales, permiten la gestión centralizada de claves de cifrado para otros entornos y dispositivos, incluido el hardware compatible con KMIP, claves maestras TDE de Oracle, SQL Server...

✱ **Protección de datos de pago.** Las soluciones de Thales están diseñadas específicamente para aplicaciones de pago. El módulo payShield 10K, la quinta generación de HSM de pago de Thales, ofrece un conjunto de funciones de seguridad de pagos comprobadas en entornos críticos y que incluyen el procesamiento de transacciones, protección de datos confidenciales, emisión de credenciales de pago, aceptación de tarjetas móviles y tokenización de pagos. payShield 10K de Thales atiende lo último en requisitos de seguridad obligatorios y en mejores prácticas para una amplia gama de organizaciones que incluyen EMVCo, PCI SSC, GlobalPlatform, Multos, ANSI, así como las varias marcas y redes de pago globales y regionales.

Por otro lado, CipherTrust Tokenization with Dynamic Data Masking permite a los administradores establecer políticas para devolver un campo completo tokenizado o enmascarar dinámicamente partes de un campo. Con las capacidades de tokenización de la solución que preservan el formato, los administradores pueden restringir el acceso a activos confidenciales y, al mismo tiempo, formatear los datos protegidos de una manera que les permita a muchos usuarios hacer su trabajo.

VENTAJAS DE LAS SOLUCIONES THALES

Las soluciones de Thales ofrecen:

❖ **Cumplir las obligaciones reglamentarias.** Con sus productos de Data Security, la industria bancaria puede cumplir con los estándares regulatorios y de seguridad de datos en reposo mientras protege la información de brechas de datos en toda la empresa, en la nube y en entornos de Big Data.

❖ **Rápida de instalar.** Thales puede instalar las soluciones de seguridad de datos CipherTrust en semanas en lugar de meses. Las soluciones de Thales funcionan con la mayoría de los principales sistemas operativos, incluidos los servidores Linux, UNIX y Windows en entornos físicos, virtuales, en entornos de datos de titulares de tarjetas (CDE) de la nube y Big Data.

❖ **Fácil de usar.** Su oferta CipherTrust Data Security Platform simplifica la resolución de problemas de seguridad y cumplimiento al proteger simultáneamente los datos en bases de datos, archivos y nodos de Big Data, en nubes públicas, privadas, híbridas e infraestructuras tradicionales. La administración centralizada de toda la plataforma de seguridad de datos, facilita la ampliación de la protección de seguridad de los datos, y la satisfacción de los requisitos de cumplimiento en toda la empresa, creciendo según sea necesario, sin agregar nuevo hardware ni aumentar las cargas operativas. ■

MÁS INFORMACIÓN

Cifrado Total

The Key Pillars for Protecting Sensitive Data

payShield Brochure

Soluciones más robustas gracias a la inteligencia de amenazas compartida

Trend Micro trabaja para ayudar a que el mundo sea seguro para el intercambio de información digital. Aprovechando los más de 30 años de experiencia en seguridad, investigación de amenazas globales e innovación continua, la firma permite la resiliencia de las empresas, gobiernos y consumidores con soluciones conectadas a través de cargas de trabajo en la nube, endpoints, correo electrónico, IIoT y redes.

Su estrategia de seguridad XGen impulsa sus soluciones con una combinación intergeneracional de técnicas de defensa frente a amenazas que están optimizadas para los entornos clave y aprovecha la inteligencia de amenazas compartida para una mejor y más rápida protección.

SOLUCIONES Y PRODUCTOS

Trend Micro ha innovado para adaptar su oferta a la evolución de las amenazas y a las necesidades de empresas y usuarios. Cuentan con un amplio catálogo de productos que permiten ofrecer protección en cualquier entorno, ya sea físico, virtual, en la nube y en contenedores.

El catálogo de Trend Micro ofrece una mayor cobertura, pues busca cubrir todos los vectores de ataque posibles (endpoint, cloud, navegación, email, entornos colaborativos, redes privadas/cloud, OT...), y por tecnología, ya que combinan tecnología de última generación junto con la experiencia que les aporta su trayectoria en el mercado.

Un ejemplo de esta evolución es la Tecnología XDR, introducida en el mercado por Trend Micro, que aprovecha la información recabada por los distintos vectores (endpoint, servidores, correo, red...). XDR extiende las capacidades del EDR tradicional aportando contexto a los ya citados ataques multivector, permitiendo a los clientes identificarlos y bloquearlos de manera prematura.

Por otro lado, Trend Micro estructura su oferta en torno a los siguientes ejes:

❖ **Solución Hybrid Cloud Security:** agrupa seguridad cloud simplificada gracias a la plataforma de servicios Trend Micro Cloud One. Protege entornos físicos, virtuales, en la nube y en contenedores con control y visibilidad centralizados; proporciona un conjunto completo de prestaciones de seguridad; reduce el número de herramientas de seguridad necesarias para proteger entornos híbridos y satisfacer los requisitos de cumplimiento; ahorra recursos y reduce los costes con una seguridad optimizada del entorno y políticas automatizadas. Disponible como software, como servicio, o en los marketplaces de AWS y Microsoft Azure, cuenta con tecnología de seguridad XGen, que ofrece un conjunto intergeneracional de controles de seguridad optimizados para entornos líderes.

❖ **Network Defense Solution:** área desde el que ofrece protección contra amenazas conocidas, desconocidas y ocultas, es decir, aquellas vulnerabilidades de las que no se tiene visibilidad y que residen en la red. Mediante la integración de las soluciones de Intrusion Prevention (IPS) y Advanced Threat Protection (incluido sandboxing), Trend Micro proporciona una combinación de técnicas intergeneracionales y de detección de defensas avanzadas para aumentar al máximo la protección e ir más allá de lo conocido y desconocido, ofreciendo protección más inteligente, logrando tiempos de reacción más rápido, mayor rendimiento y protección automatizada que se adapta a entornos híbridos.

❖ **User Protection Solution:** brinda protección avanzada e inteligente a los usuarios con la técnica adecuada en el momento adecuado, en cualquier dispositivo, aplicación y lugar. Se trata de una seguridad conectada y que utiliza varias capas para detener las amenazas emergentes y reducir los gastos de gestión. Seguridad optimizada para funcionar en su entorno por un proveedor de confianza y con visión de futuro que siempre trabaja en una nueva generación de seguridad. Gracias a Smart Protection Suite, son capaces de proteger a los usuarios desde el gateway hasta el endpoint.

Este catálogo de soluciones, que también abarca el segmento de la pyme, se ve complementado con servicios de soporte al cliente para garantizar un funcionamiento sin problemas y una asistencia superior. ■

MÁS INFORMACIÓN

- The Banking and Finance Industry Under Cybercriminal Siege: An Overview
- Banks Under Attack
- Mobile Banking Trojan

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com

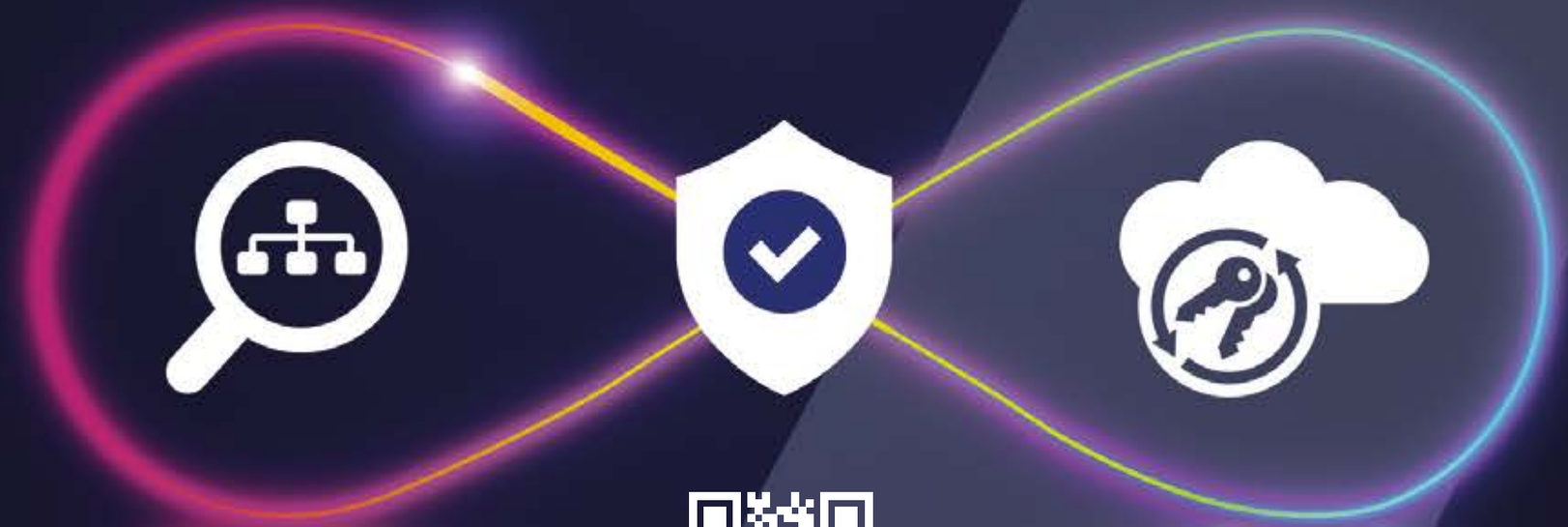
cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar Proteger Controlar



Empiece a localizar, proteger y controlar sus datos hoy mismo

La urgencia de la ciberinteligencia

Cada vez más ciberataques y más sofisticados. La evolución nos ha llevado de hablar de seguridad IT a ciberseguridad, y nos empuja hacia la ciberinteligencia. Es lo que tiene asumir que, antes o después, seremos atacados, que la mejor defensa es un buen ataque, y que la mejor opción es adelantarnos, conocer al enemigo y planificar una seguridad adaptativa capaz de hacer frente a cada tipo de ataque. Comprender cómo las amenazas se dirigen a la información, los sistemas, las personas y las organizaciones ayuda a empresas e individuos a comprender cómo realizar operaciones de búsqueda de amenazas y seguridad, responder a incidentes, diseñar mejores sistemas, comprender el riesgo y el impacto, realizar cambios estratégicos y protegerse del futuro.

La inteligencia de amenazas es el conocimiento que permite prevenir o mitigar los ciberataques; es lo que proporciona un contexto, como quién está atacando, cuáles son sus motivaciones y capacidades, y qué indicadores de compromiso buscar para tomar decisiones informadas sobre su seguridad.

La mayor sofisticación de los ataques, la mayor capacidad para recopilar más datos de cada vez más fuentes y una grave escasez de profesionales son algunos de los retos a los que se enfrentan las empresas a la hora de hacer frente a las ciberamenazas. Una solución de inteligencia de amenazas puede abordar cada uno de estos problemas en tanto en cuanto la mayoría utilizan el aprendizaje automático para automatizar la recopilación y el procesamiento de datos, se integran con soluciones existentes, son capaces de tomar datos no estructurados de fuentes dispares y correlar toda la información proporcionando contexto sobre los indicadores de compromiso (IoC) y las tácticas, técnicas y procedimientos de los actores de amenazas.

Al poder proporcionar contexto de las ciberamenazas, la ciberinteligencia mejora las capacidades de seguridad de las organizaciones. Entre los beneficios que aporta una solución de inteligencia de amenazas destaca un ahorro de costes, ¿por qué? Porque cuanto más lenta sea la respuesta a las amenazas, más le costará a una organización una brecha de seguridad. Al reducir el tiempo de respuesta, la inteligencia sobre amenazas puede ayudar a eliminar problemas y multas asociadas a diferentes regulaciones; además, la inteligencia sobre amenazas ayuda a identificar correctamente los falsos positivos, lo que ahorra tiempo y dinero en respuestas a amenazas innecesarias.

Por otra parte, al utilizar la ciberinteligencia, las organizaciones pueden cuantificar y clasificar mejor las amenazas para saber qué vulnerabilidades representan el mayor riesgo para su negocio. Con una visibilidad continua de su postura de ciberseguridad, puede identificar y clasificar el riesgo de manera

La ciberinteligencia también es necesaria en el SOC, donde los equipos deben lidiar con enormes volúmenes de alertas

CIBERINTELIGENCIA PARA PRINCIPIANTES

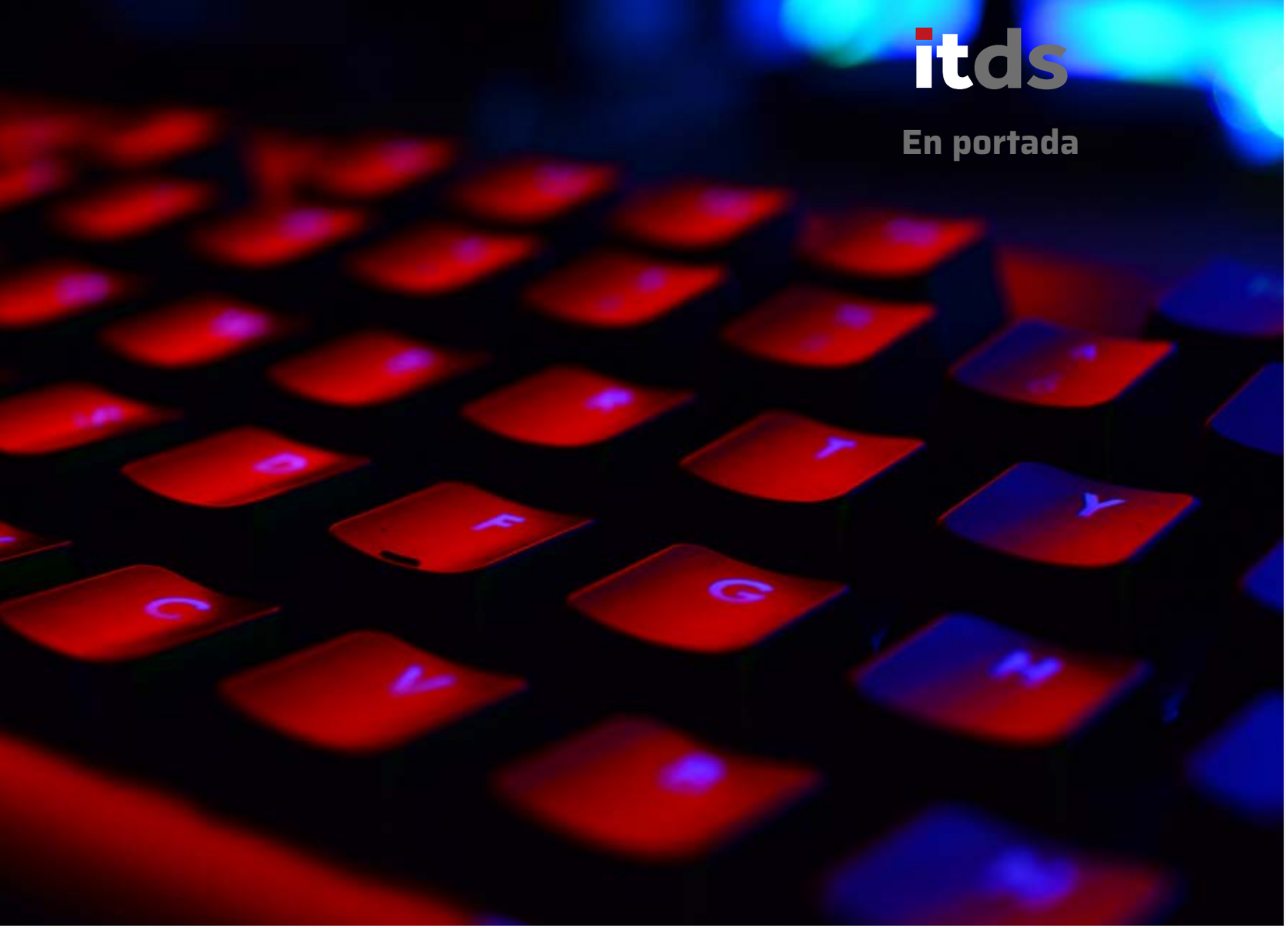
CLICAR PARA VER EL VÍDEO

eficiente, lo que permite la priorización de amenazas que, a su vez, mejora la respuesta al riesgo.

Otro de los beneficios que aporta la ciberinteligencia de amenazas es que elimina las tareas repetitivas y laboriosas de las manos de los humanos. Las máquinas son excelentes para encontrar patrones en grandes cantidades de datos y, a diferencia de los humanos, nunca se cansan ni se aburren, por lo que, al automatizar la recopilación de información sobre amenazas, puede reducir la cantidad de errores en su recopilación de información sobre amenazas y además liberar a los analistas para que examinen la información que ofrece su solución automatizada y decidan qué amenazas son más relevantes para su organización.

Destacar también que una plataforma automatizada ofrece información de seguridad relevante a los miembros del equipo en toda la empresa. Esto significa que todos obtienen la información que necesitan al mismo tiempo, lo que garantiza que la estrategia y procesos de seguridad sean coherentes en toda la organización. Esto es especialmente importante durante un ataque, cuando debe haber una coordinación con los miembros del equipo.

En cuanto a quién puede beneficiar la ciberinteligencia de amenazas, la respuesta es que agrega valor en todas las funciones de seguridad para organizaciones de todos los tamaños. Aseguran los expertos que cuando la inteligencia de amenazas se trata como una función separada dentro de un paradigma de seguridad más amplio en lugar de un componente esencial que aumenta todas las demás funciones, el resultado es que muchas de las personas que se beneficiarían más de la inteligencia de amenazas no tienen acceso a ella cuando la necesitan: a los equipos de operaciones de seguridad les ayuda a priorizar y filtrar las alertas y a los de gestión de vulnerabilidades les permite ser más precisos; por otra parte, la prevención del fraude, el análisis de riesgos y otros procesos de seguridad de alto nivel se enriquecen con la comprensión del panorama actual de amenazas que proporciona la



Para mantener la seguridad no es suficiente con detectar y responder a las amenazas, sino evitar usos fraudulentos de los datos o marca

ciberinteligencia de amenazas, incluida información clave sobre los actores de amenazas, sus tácticas, técnicas y procedimientos, y más de las fuentes de datos en todo el mundo

El ciclo de vida de la Ciberinteligencia

La ciberinteligencia sobre amenazas es el producto final que surge de un ciclo de seis fases en las que se recopilan, procesan y analizan los datos.

- **La primera es la fase de planificación** en la que los equipos de seguridad establecen los objetivos, los alinean con los valores de la organización y pronostican el impacto potencial de decisiones futuras basadas en esta inteligencia. Intentan descubrir más información sobre posibles actores de amenazas, el tamaño de la superficie de ataque y consideran cómo pueden apuntalar sus defensas.

Se parte de hacer la pregunta correcta, cuanto más concreta, mejor. Se priorizan los objetivos en función del impacto y la urgencia y se busca comprender quién consumirá y se beneficiará del producto terminado: ¿la inteligencia irá a un equipo de analistas con experiencia técnica que necesitan un informe rápido sobre un nuevo exploit, o a un ejecutivo que busca una descripción general de las tendencias para informar sus decisiones de inversión en seguridad para el próximo trimestre?

- **Recolección de datos.** Una vez identificados los objetivos, se empiezan a recopilar datos de una variedad de fuentes, tanto internas, como los registros de eventos de la red o registros de respuesta ante incidentes; como externas, donde se incluyen la darkweb o fuentes técnicas.
  Resaltar que generalmente se consideran como datos de amenazas listas de indicadores de compromiso (direcciones IP maliciosas, dominios y hashes de archivos) pero también pueden incluir información de vulnerabilidad, como la información de identificación personal de los clientes, así como texto de noticias, fuentes o redes sociales.
- **Procesamiento.** Una vez recolectados, los datos deben procesarse, o lo que es lo mismo: ordenarse, organizarse y filtrarse para respaldar un análisis más detallado. En esta etapa, se agregan

2021 SANS CYBER THREAT INTELLIGENCE SURVEY

El informe de SASNS Institute destaca que es muy prometedor ver que las organizaciones más pequeñas también avanzan en la adopción de soluciones de inteligencia de amenazas y que la automatización de muchas tareas clave, como la deduplicación y estandarización de datos, así como las mejoras en la automatización de la integración en los sistemas de detección y respuesta, son todas mejoras que respaldarán la eficiencia y la escala de las tareas de ciberinteligencia.

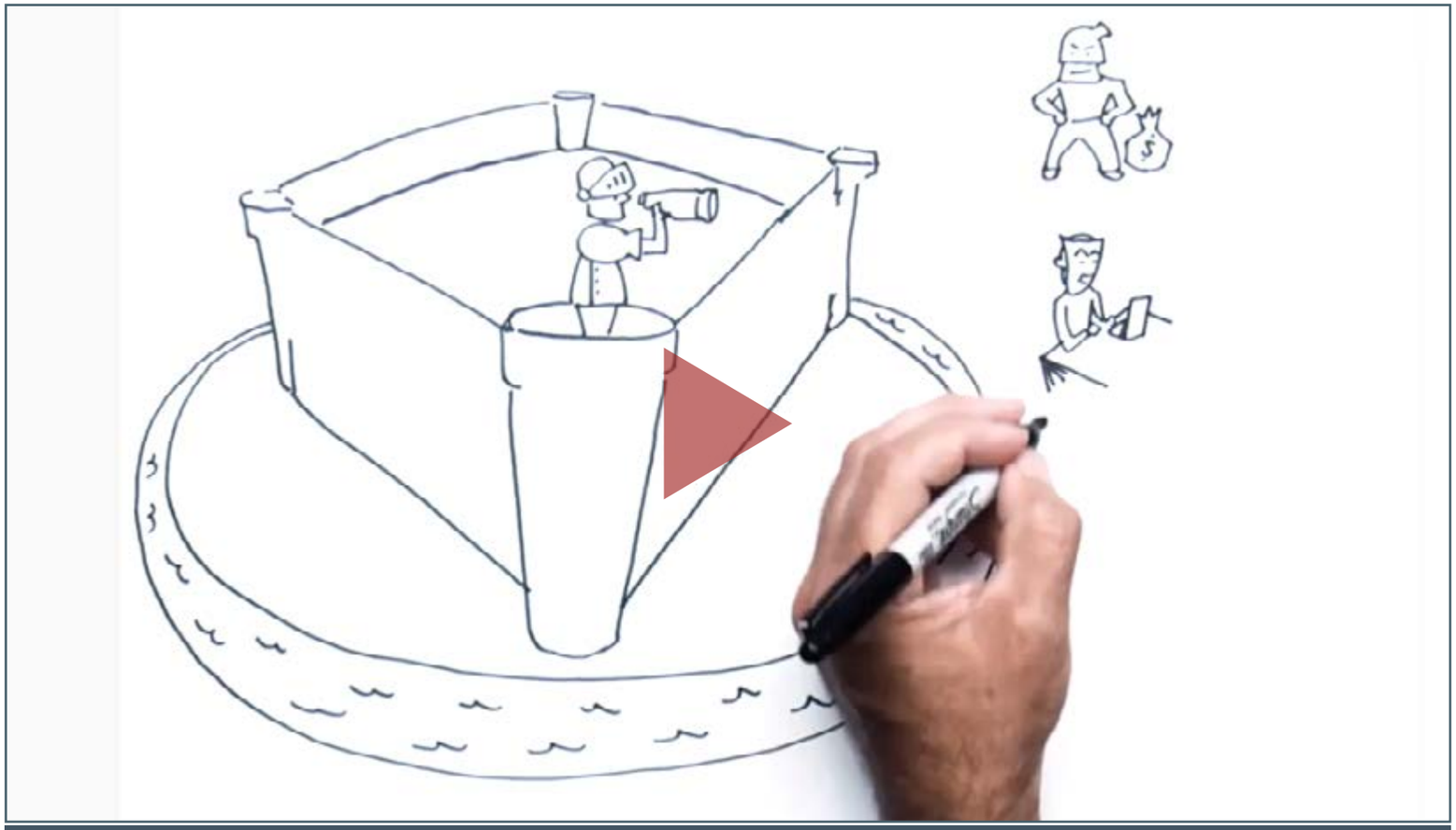
etiquetas de metadatos, se elimina la información redundante, irrelevante y poco confiable. Hacer manualmente todas estas tareas para millones o incluso miles de puntos de datos requiere mucho tiempo y es propenso a errores, por eso la automatización es clave.

Los equipos pueden organizar datos en hojas de cálculo, descifrar archivos cifrados y traducir información de fuentes extranjeras para después convertir los datos a un formato que la audiencia (por ejemplo, los altos ejecutivos) pueda comprender. Puede ser una simple lista de amenazas, una presentación concisa o un informe completo. El equipo también identifica los elementos de acción clave y proporciona recomendaciones relevantes para prevenir o mitigar las amenazas.

- **Análisis.** Tras el procesamiento de los datos, estos deben analizarse para darles sentido y buscar potenciales problemas de seguridad que se notifican a los equipos en un formato que cumpla con los requisitos de inteligencia descritos en la etapa de planificación y dirección.
  La inteligencia de amenazas puede tomar muchas formas dependiendo de los objetivos iniciales y la audiencia prevista, pero la idea es obtener los datos en un formato que la audiencia pueda comprender. El equipo también identifica los elementos de acción clave y proporciona recomendaciones relevantes para prevenir o mitigar las amenazas.
- **Difusión.** Para que la inteligencia de amenazas sea procesable, debe llegar a las personas adecuadas en el momento adecuado. Además, y para

que haya continuidad entre un ciclo de inteligencia y el siguiente, y no se pierda el aprendizaje, también es necesario realizar un seguimiento. En esta fase del ciclo pueden utilizarse sistemas de emisión de tickets que se integran con sus otros sistemas de seguridad para realizar un seguimiento de cada paso del ciclo de inteligencia: cada vez que surge una nueva solicitud de inteligencia, varias personas de diferentes equipos pueden enviar, redactar, revisar y completar los tickets.

- **Feedback y ajustes.** El paso final es cuando el ciclo de inteligencia completa el círculo, lo que lo relaciona estrechamente con la fase inicial de planificación y dirección. Después de recibir el producto de inteligencia terminado, quien hizo la solicitud inicial lo revisa y determina si sus preguntas fueron respondidas y si se requieren ajustes



CYBER THREAT INTELLIGENCE EXPLICADO

CLICAR PARA VER EL VÍDEO

a los objetivos, requisitos, cronogramas de informes, operaciones y procedimientos de inteligencia de amenazas y/o prioridades. Esto impulsa los objetivos y procedimientos del próximo ciclo de inteligencia, lo que nuevamente hace que la documentación y la continuidad sean esenciales.

Tipos de ciberinteligencia

Explican los expertos que para una mejor gestión del conocimiento que se recopila de fuentes totalmente diferentes, es necesario subdividir la inteligencia de amenazas en diferentes tipos en función de los objetivos y la audiencia: Estratégica, Táctica, Operativa y Técnica.

Ciberinteligencia Estratégica

La inteligencia de amenazas estratégica proporciona una amplia visión del panorama de amenazas de la organización, así como la postura de seguridad y el impacto económico de diferentes actividades y tendencias de ataque.

La gestión eficaz de las vulnerabilidades ha pasado de parchear todo, todo el tiempo, a priorizarlo en función del riesgo real.

Esta información es consumida por ejecutivos de alto nivel y la administración de la organización, y por lo tanto la información que se proporciona es generalmente menos técnica. Por cierto, una buena ciberinteligencia estratégica debe proporcionar información sobre áreas como los riesgos asociados con ciertas líneas de acción, patrones generales en las tácticas y objetivos de los actores de amenazas, así como eventos y tendencias geopolíticas.

Por otra parte, se enfoca principalmente en problemas a largo plazo y proporciona alertas de amenazas por períodos de tiempo en los activos vitales de la organización, como la infraestructura de TI, los empleados, los clientes y las aplicaciones. La administración emplea este tipo de inteligencia de amenazas para requerir selecciones comerciales estratégicas e investigar el resultado de tales decisiones. Apoyado el análisis, la dirección asignará un presupuesto cómodo y empleados para proteger los activos de TI vitales y los procesos comerciales.

Las fuentes más comunes de información para la inteligencia de amenazas estratégicas incluyen documentos de políticas de estados-nación u organizaciones no gubernamentales; noticias de los medios de comunicación; documentos técnicos, informes de investigación y otro contenido producido por organizaciones de seguridad

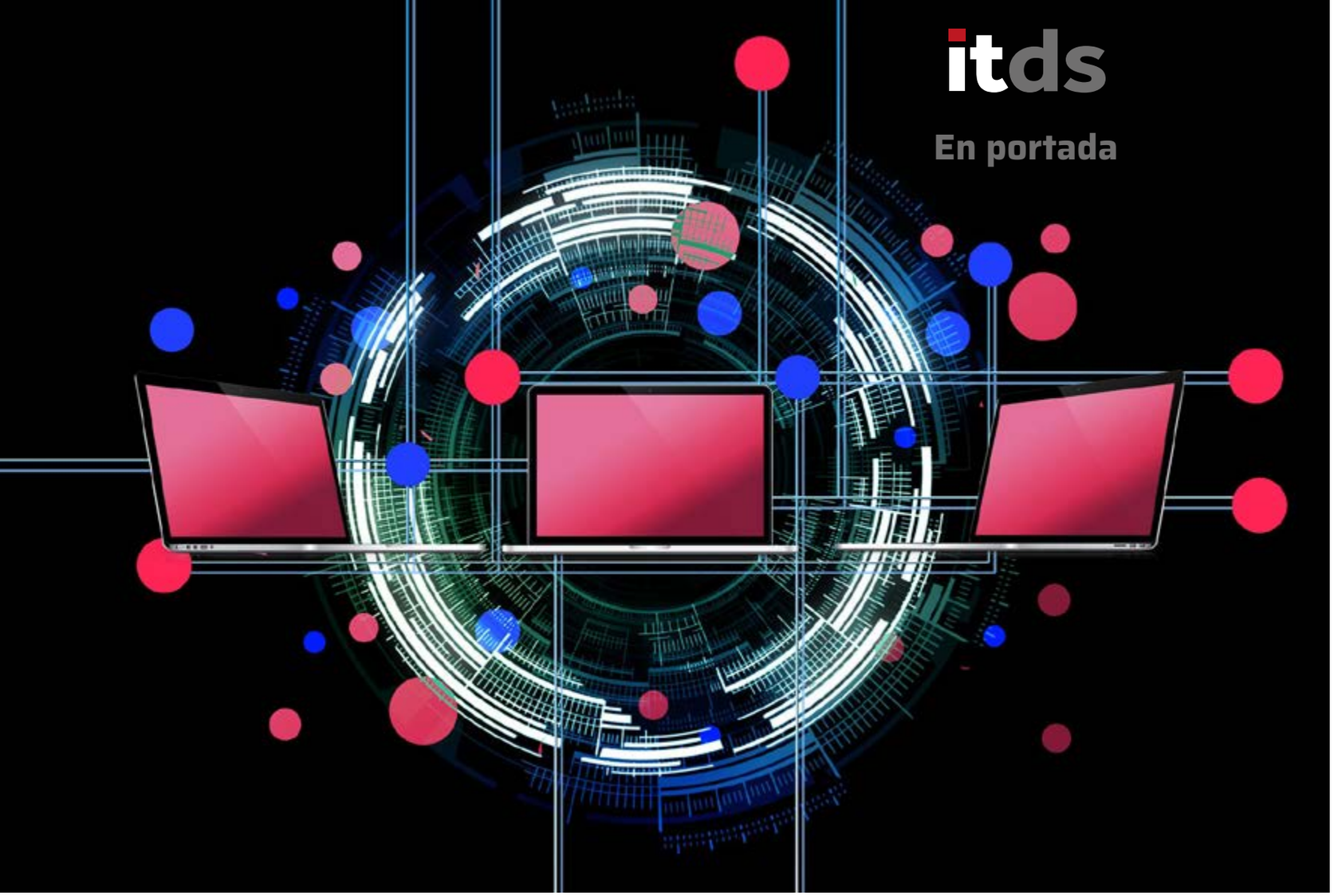
La producción de una sólida inteligencia estratégica sobre amenazas comienza con la formulación de preguntas específicas y enfocadas para establecer los requisitos de inteligencia.

Ciberinteligencia Táctica

La inteligencia de amenazas tácticas juega un papel importante en la protección de los recursos de la organización. Proporciona información relacionada con las tácticas, técnicas y procedimientos utilizados por los ciberdelincuentes para realizar sus ataques. La inteligencia táctica sobre amenazas es consumida por personal directamente involucrado en la defensa de una organización.

Este tipo de ciberinteligencia ayuda a los profesionales de ciberseguridad a comprender, en términos específicos, cómo su organización podría ser atacada. Mediante el uso de inteligencia táctica de amenazas, el personal de seguridad desarrolla métodos de detección y mitigación de antemano gracias a indicadores conocidos, parcheando sistemas vulnerables, etc.

> La ciberinteligencia sobre amenazas es el producto final que surge de un ciclo de seis fases en las que se recopilan, procesan y analizan los datos



La mayor sofisticación de los ataques, la mayor capacidad para recopilar más datos de cada vez más fuentes y una grave escasez de profesionales son algunos de los retos a los que se enfrentan las empresas a la hora de hacer frente a las ciberamenazas

Los informes producidos por los proveedores de seguridad suelen ser la forma más fácil de obtener inteligencia táctica sobre amenazas. Las fuentes de recopilación de inteligencia de amenazas tácticas abarcan información sobre los vectores de ataque, las herramientas y la infraestructura que utilizan los atacantes, incluidos los detalles sobre las vulnerabilidades que están siendo atacadas y los exploits que aprovechan los atacantes, así como las estrategias y herramientas que pueden estar usando para evitar o retrasar detección.

Por otra parte, esta inteligencia se obtiene principalmente mediante la lectura de documentos técnicos, la comunicación con diferentes organizaciones o la obtención de inteligencia de terceros. Incluye información extremadamente técnica como malware, campañas, técnicas y herramientas en forma de informes forenses.

Ciberinteligencia Operativa

La inteligencia operativa es el conocimiento sobre ciberataques, eventos o campañas. Proporciona información contextual sobre eventos e incidentes de seguridad que ayuda a los defensores a revelar riesgos potenciales, ofrecer una mayor comprensión de las metodologías de los delincuentes, establecer actividades maliciosas pasadas y realizar investigaciones sobre actividades maliciosas de una manera mucho más económica. Este tipo de ciberinteligencia es consumida por gerentes de seguridad o jefes de respuesta a incidentes, defensores de redes, análisis forense de seguridad y grupos de detección de fraude.

Ayuda a las organizaciones a comprender los posibles actores de amenazas y su intención, capacidad y oportunidad de atacar, activos de TI vulnerables y también el impacto del ataque si tiene éxito.

La inteligencia operativa sobre amenazas se recopila principalmente de fuentes como humanos, redes sociales y salas de chat, y además de

actividades y eventos del mundo real que conducen a ciberataques cibernéticos. Esta información ayuda a predecir ataques futuros y, por lo tanto, a mejorar los planes de respuesta a incidentes y las formas de mitigación según sea necesario.

Ciberinteligencia Técnica

En ella se utiliza información más técnica, como qué vector de ataque se está utilizando, qué vulnerabilidades se están explotando o qué dominios de comando y control se están utilizando.

Otras fuentes de información sobre ataques específicos pueden provenir de fuentes cerradas como la interceptación de comunicaciones de grupos de amenazas, ya sea mediante infiltración o irrumpiendo en esos canales de comunicación. En consecuencia, existen algunas barreras para recopilar este tipo de inteligencia, ya que los grupos de ciberdelincuentes pueden comunicarse a través de canales privados y cifrados, o requerir alguna prueba de identificación; existe también una barrera de idioma con grupos de amenazas ubicados en países extranjeros; por otra parte, para evitar la detección, los grupos de amenazas pueden emplear tácticas de ofuscación, como el uso de nombres en clave.

Los indicadores de inteligencia técnica sobre amenazas se recopilan de campañas activas, ataques que se realizan en otras organizaciones o fuentes de datos proporcionadas por terceros externos.

Esta información ayuda a los profesionales de la seguridad a agregar los indicadores identificados a los sistemas defensivos, mejorando así los mecanismos de detección utilizados para identificar los ataques en una etapa temprana. También les ayuda a identificar el tráfico malicioso y las direcciones IP sospechosas que se utilizan para difundir malware y correos no deseados.

Casos de uso de la ciberinteligencia

Los diversos casos de uso de la inteligencia sobre amenazas la convierten en un recurso esencial. No sólo ayuda a prevenir un ataque, sino que es una parte útil del triaje, el análisis de riesgos, la administración de vulnerabilidades y la toma de decisiones de amplio alcance.

Teniendo en cuenta la cantidad, la respuesta ante incidentes es una de las tareas más estresantes del mundo de la ciberseguridad. Con una proporción alta de alertas, muchas de las cuales terminan en falsos positivos, la ciberinteligencia reduce la presión de diferentes formas, como identificando y descartando automáticamente falsos positivos; enriqueciendo las alertas con contexto en tiempo real, como puntuaciones de riesgo personalizadas o comparando información de fuentes internas y externas

La ciberinteligencia también es necesaria en el SOC, donde los equipos deben lidiar con enormes volúmenes de alertas. La clasificación de las mismas lleva tiempo, lo que hace que muchas de ellas ni siquiera se investigue. La llamada “fatiga de alertas” lleva a los analistas a cometer errores y la inteligencia de amenazas resuelve muchos de estos problemas, lo que ayuda a recopilar información sobre las amenazas de manera más rápida y

Con ciberinteligencia las empresas pueden reforzar sus defensas y mitigar los riesgos, manteniéndose unos pasos por delante de los ciberdelincuentes

Enlaces de interés...

- El 85% de las empresas utiliza activamente la inteligencia contra ciberamenazas
- La inteligencia de amenazas, cada vez más relevante en las operaciones de seguridad
- 'Las empresas necesitan madurar en el área de ciberinteligencia' (Eutimio Fernández, ThreatQuotient)

precisa, filtrar las falsas alarmas, acelerar la clasificación y simplificar el análisis de incidentes. Con él, los analistas pueden dejar de perder tiempo buscando alertas basadas en acciones que tienen más probabilidades de ser inocuas en lugar de maliciosas; ataques que no son relevantes para esa empresa o ataques para los que ya existen defensas y controles.

La gestión eficaz de las vulnerabilidades ha pasado de parchear todo, todo el tiempo, a priorizarlo en función del riesgo real. Los datos muestran que la mayoría de las amenazas se centran una pequeña proporción de vulnerabilidades y que los ciberdelincuentes son cada vez más rápidos, ya que solo tardan una media de quince días en crear un exploit para una vulnerabilidad recién descubierta. En esta situación, la ciberinteligencia ayuda a identificar las vulnerabilidades que representan un riesgo real para la organización.

El análisis de riesgos es muy útil para que las organizaciones establezcan prioridades de inversión. La inteligencia de amenazas proporciona un contexto que ayuda a esos análisis de riesgos al poder responder a preguntas como ¿qué actores de amenazas están utilizando este ataque y se dirigen a nuestra industria?, ¿con qué frecuencia empresas como la nuestra han observado recientemente este ataque específico?, ¿qué vulnerabilidades explota este ataque?, o ¿qué tipo de daño, técnico y financiero, ha causado este ataque en empresas como la nuestra?

Otro caso de uso de la ciberinteligencia tiene que ver con la prevención del fraude. Y es que para mantener la seguridad de su organización no es suficiente con detectar y responder a las amenazas, sino evitar usos fraudulentos de sus datos o marca. Al recopilar información de comunidades clandestinas, la inteligencia de amenazas proporciona una ventana a las motivaciones, métodos y tácticas de los actores de amenazas, y por tanto permite prevenir fraudes relacionados por pago, compromiso de datos, phishing, etc.

Lo que está claro es que con ciberinteligencia, con inteligencia de amenazas contextual, dirigida y oportuna, las empresas pueden reforzar sus defensas, así como mitigar los riesgos que podrían dañar su reputación y salud financiera, manteniéndolas unos pasos por delante de los ciberdelincuentes. Según datos de Gartner, para 2018 el 60% de las grandes empresas de todo el mundo utilizarán servicios de inteligencia de amenazas para reforzar sus estrategias de seguridad.

Compartir en RRSS

SECURE ACADEMY

TU CENTRO AVANZADO DE FORMACIÓN EN CIBERSEGURIDAD

www.secureacademy.es

Secure&IT by LKS

Ciberseguridad: una oportunidad de transformación y diversidad

ELENA GARCÍA DIEZ

MIEMBRO DEL CONSEJO WOMEN4CYBER SPAIN

Directora de Seguridad de la Información (CISO) en Indra, Elena García es Ingeniera de Telecomunicación con más de 15 años de experiencia en diferentes ámbitos de las tecnologías de la información y la gestión de equipos y proyectos. Previamente a Indra trabajó en diferentes niveles y áreas de actividad en el Instituto Nacional de Ciberseguridad (INCIBE) y en diferentes empresas de servicios y consultoría de telecomunicaciones. Colabora habitualmente en foros especializados y acciones formativas en el sector de la Ciberseguidad. Desde su creación en 2019, colabora como Founder Member de Women4Cyber de ECSO (European Organisation for Cybersecurity) y, a nivel nacional, forma parte de la Junta Directiva del capítulo español del WOMEN4CYBER.

Llevamos meses asistiendo a esta transformación digital obligada que ha supuesto la pandemia para toda la sociedad. Los que tenemos la suerte de trabajar en el mundo de la seguridad de la información o la ciberseguridad disfrutamos en primera línea de los retos y oportunidades que esto supone.

La seguridad de la información ya era una prioridad en la agenda del tejido empresarial a nivel internacional, con ejemplos y reflejo directo en las políticas públicas europeas y nacionales ya desde hace años. Si bien, el contexto actual ha supuesto una aceleración de la transformación digital y nadie tiene duda de que la seguridad y la confianza es una clave estratégica a considerar y desarrollar en todo el proceso.

En España hay una oferta de servicios de seguridad que están efectivamente acompañando a todo el tejido empresarial. Según las encuestas realizadas post pandemia, el 70% de las empresas considera la seguridad de la información como una prioridad ya que los ciberataques y amenazas aumentaron un 80% en estos últimos meses. Lo vemos todos los días en la prensa generalista y en la económica donde cada vez aparecen más informaciones relacionadas con incidentes, diferentes estrategias de comunicación e inversiones en ciberseguridad, etc.

Si destacásemos dos puntos comunes en los diferentes diagnósticos sobre el sector es fácil tener consenso de la importancia de la evolución de las estrategias de seguridad conforme a la evolución del contexto y sobre la necesidad de dotarnos del talento necesario para hacer frente a esta transformación.

Por ejemplo, el informe presentado por SIA y Minsait de Madurez Digital en Ciberseguridad 2020/2021, apalanca en el talento el tercer pilar para la adecuada materialización de las estrategias y respuestas a las amenazas de seguridad

Combinar los tradicionalmente disjuntos planos de la gestión y la tecnología con capacidades de comunicación y liderazgo son clave en el desempeño de cualquier equipo de seguridad

que mantienen, como era de esperar, una evolución constante hacia la profesionalización del cibercrimen y los ataques dirigidos a grandes y pequeñas empresas de todos los sectores.

En cuanto a la transformación de la función de la seguridad, hace tiempo que venimos hablando de cómo los retos que supone la evolución de la sociedad de la información en general y la repercusión de la seguridad de la información demandan que la estructura de responsabilidad de las diferentes organizaciones se desarrolle de forma proporcional. La evolución de la figura del CISO ha sido referencia en esta evolución de responsabilidades y está llamada a seguir siéndolo. Así, el ámbito de actuación del CISO, tradicionalmente más centrado en un ámbito tecnológico, evoluciona hacia la visión global de riesgos de la compañía y su negocio.

En un entorno de transformación el líder de los equipos de seguridad tiene que ser capaz de trasladar a su función el mismo enfoque transformador. Los equipos de seguridad deben ser capaces de definir, impulsar e implantar el marco de seguridad que mejor se ajuste a las necesidades y expectativas del negocio. Combinar pues tecnología, procesos, personas y el enfoque de riesgos adecuado en un contexto de constante evolución.

Estos equipos necesitan no sólo profesionales con un elevado conocimiento técnico, sino que también deben conocer el negocio y los riesgos de seguridad a los que aquél está expuesto, para así tomar decisiones con criterio.

Combinar los tradicionalmente disjuntos planos de la gestión y la tecnología con capacidades de comunicación y liderazgo son clave en el desempeño de cualquier equipo de seguridad.

En este punto nos encontramos con el reto y la oportunidad del talento en seguridad. Un talento que no será completo si no está apoyado en equipos realmente diversos. La diversidad de género aquí es una palanca a aprovechar.

En un contexto de transformación de la seguridad, la diversidad facilitará que nuestra llegada a los usuarios de nuestra información y nuestra tecnología de información adquieran las destrezas necesarias para acompañar la estrategia de seguridad que debemos acometer y en la que, como siempre, ellos jugarán un papel clave.

En los últimos meses, a la hora de implantar mecanismos de seguridad en el entorno de trabajo en remoto, los ciudadanos en general y los

profesionales de todas las compañías en general nos han demostrado que están más preparados para el cambio de lo que creíamos, que proyectos que habíamos pensado desplegar en años podíamos hacerlos realidad en meses.

Pero cualquier esfuerzo es poco cuando hablamos de transformación. La adopción de hábitos y tecnología requiere de mensajes y estrategias diversas. Hace ya tiempo que hablábamos de la necesidad de perfiles de seguridad con una visión más allá de la gestión de consolas de monitorización y tecnologías concretas. Los mapas y las arquitecturas que ahora mismo desplegamos van mucho más allá. Conseguir explotar y sacar el máximo rendimiento depende en gran medida de las estrategias y procesos que seamos capaces de construir y promover.

Ahora, tenemos una nueva oportunidad de generar talento, en los jóvenes, y en los no tan jóvenes que pueden aportar una visión de gestión y de proceso necesariamente complementaria a los equipos de seguridad actuales.

Organizaciones como Women4CyberSpain asumen el reto de potenciar la diversidad en el sector de la ciberseguridad. Apoyarse en estructuras sólidas, buscar y explotar sinergias de nuestro entorno europeo (gracias Women4Cyber de ECSO por apoyar el camino), construir sobre experiencias ya aplicadas en otros países y continuar cada día aprendiendo y evolucionando. Esto no es sólo una carrera, es una línea en la que trabajar de manera continua.

Programas de mentoring, webminars, visibilizar oportunidades laborales y promover el emprendimiento son ejes sobre los que construir el ecosistema para que la igualdad esté cada vez más presente en la ciberseguridad. Equipos con talentos diversos y que ponen en valor experiencias previas multidisciplinares para enriquecer el amalgama de soluciones que necesitan compañías y sociedad en general para mantener una evolución natural, con confianza, con seguridad.

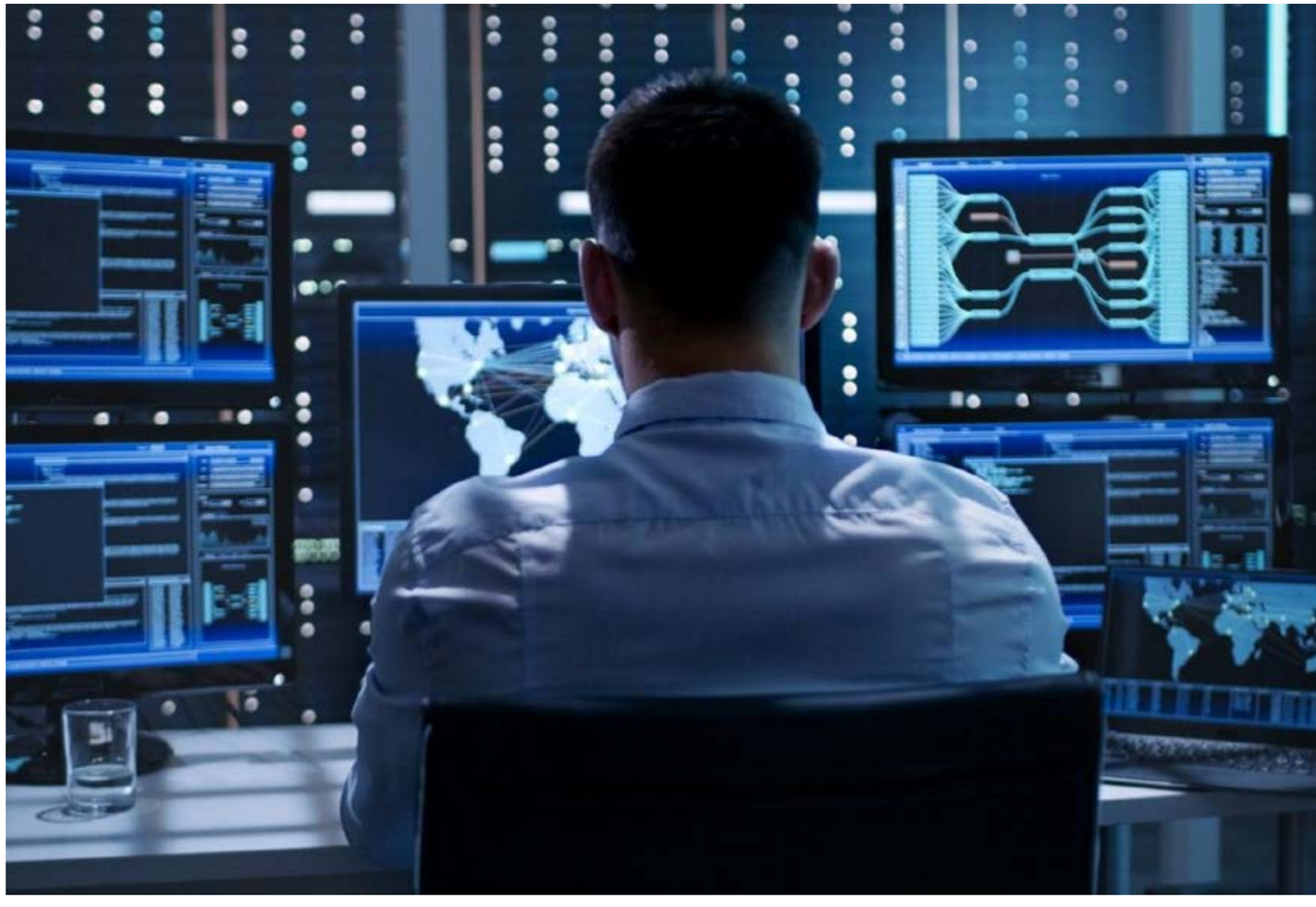
Enlaces de interés...

- La gestión de los datos está en el corazón de la seguridad en la nube
- Women4Cyber Spain en el Día Internacional de la mujer
- Te han 'hackeado', y ahora, ¿cómo se lo comunicas a tus clientes?

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.

El SOC del futuro



El proceso de digitalización de las organizaciones y la cada vez mayor dependencia de los datos para la mejora de las operaciones y el engagement con clientes y empleados abre un tema de discusión interesante desde el punto de vista de la seguridad, ya que se requiere una respuesta más ágil a las condiciones cambiantes del mercado.

JOSÉ CANO

DIRECTOR DE ANÁLISIS Y CONSULTORÍA DE IDC ESPAÑA

Director de Análisis y Consultoría en IDC Research España. Anteriormente, Director de Consultoría Técnica y Desarrollo de Negocio en GAC Grupo (España) y Director Académico del EMBA Blended (Madrid). Ha trabajado en consultoría de estrategia y operaciones en Avantia XXI S.L Global, y asesor ejecutivo para entidades públicas y privadas en el ámbito de la innovación y desarrollo de negocio (Deusto Business School, ICARUM ANS S.L, etc.). También ha sido socio fundador y director de consultoría de estrategia y operaciones en ACL Strategy S.L, y Senior Manager de Innovación en consultoría de sector público (E&O) en Deloitte.

Sin embargo, en este contexto actual se están dando dos hechos fundamentales que impactan en la efectividad de los equipos de seguridad:

- **Gestión de amenazas:** volumen y variedad de amenazas, diversidad de defensas necesarias, amenazas altamente sofisticadas, sigilosas y evasivas, gama de actores de amenazas (ciberdelincuentes, estado nación, ideológico, etc.)
- **Escasez de habilidades de seguridad:** dificultad y gastos de reclutamiento y retención de profesionales de seguridad cualificados de un grupo de mano de obra finito, importancia de evitar el agotamiento de los analistas de seguridad

Aunque las tecnologías de gestión de eventos han evolucionado considerablemente, el incremento del tráfico de datos, amenazas y tipología de herramientas para su gestión hacen que sea necesario abordar un proceso de evolución que permita gestionar de manera efectiva la respuesta y escalado por parte de los equipos de seguridad. Hablamos de modelos de SOC híbridos en los que parte de las funciones de seguridad están delegadas en proveedores de servicios capaces de operar en un entorno 24/7.

> Sin una forma de contextualizar los datos, los equipos del SOC se verán inundados de alertas incapaces de gestionarlas, derivando en una fatiga de alertas que permitan a los atacantes sobrepasar el perímetro de seguridad

Este modelo híbrido permite conseguir un modelo efectivo de gestión de amenazas, ya que ayuda al equipo interno de la organización entregando un modelo con tecnología de automatización que simplifica y ayuda a reducir falsos positivos, ayudando en la priorización de respuestas, lo que tiene su impacto en la reducción del tiempo de detección, respuesta y remediación. Todo ello en la

EL SOC del futuro permitirá contextualizar los datos, generando alertas precisas que habiliten asimismo actuaciones correctamente priorizadas y adaptadas a cada casuística particular

búsqueda de adelantarse a los ataques, mediante la integración de nuevas capacidades de análisis proactivo que ayuden a minimizar la exposición ante amenazas.

El incremento del tráfico actual donde el 70% es cifrado, obliga a la incorporación de tecnologías como la automatización y el uso de IA para poder reducir el esfuerzo de los equipos para responder a este nuevo escenario de amenazas. De esta forma, se introduce velocidad, eficiencia en costes y precisión en la respuesta, logrando un SOC integrado y orquestado que recopila datos más rápidamente, correlaciones más eficientes, así como despliegue de parches de manera más rápida.

Todo ello con el ánimo de lograr una detección proactiva de amenazas.

Pero más allá de los beneficios, el proceso de automatización debe partir de las siguientes premisas para que sea efectivo:

- **Contextualizar las alertas,** esto es, aportar información adicional de contexto a una alerta, de forma que se facilita la priorización y la alerta puede ser potencialmente correlada como un incidente único, lo que posibilita encadenar un posible escenario de ataque.
- **Contextualización del ataque.** Correlada una alerta, la automatización debe permitir ensamblar las alertas en función del tipo de ataque de forma que se pueda generar un patrón de ataque que

El incremento del tráfico actual donde el 70% es cifrado, obliga a la incorporación de tecnologías como la automatización y el uso de IA para poder reducir el esfuerzo de los equipos para responder a este nuevo escenario de amenazas

amplíe el posible espectro de posibles casuísticas derivadas de un mismo tipo de ataque.

- **Gestión proactiva y permanentemente actualizada** sobre las últimas amenazas de ciberseguridad, que se adelante a los posibles ataques mediante el conocimiento de la secuencia de pasos que un atacante realizará para desplegar un ataque complejo. Anticipándonos al siguiente paso y buscando las evidencias y pruebas necesarias para correlar la información y automatizar el tipo de respuesta, se puede evitar el ataque.

Por todo ello, la evolución natural del SOC será hacia un SOC híbrido con capacidades de automatización e IA que permitan minimizar los tiempos de respuesta, reduciendo el error humano y, fundamentalmente, eliminando (o al menos reduciendo) la fatiga de la alerta.

Si bien existe evidencia de que el 90% de las brechas de seguridad se producen por errores humanos, también lo es que en el contexto actual de crecimiento exponencial de tráfico y amenazas (más de 350.000 ataques de malware diarios), mantener la capacidad de prevención y detección en las organizaciones es muy complicado. Por ello, sin una forma de contextualizar los datos, los equipos del SOC se verán inundados de alertas incapaces de gestionarlas, derivando en una fatiga de alertas que permitan a los atacantes sobrepasar el perímetro de seguridad.

Este modelo de SOC del futuro permitirá contextualizar los datos, generando alertas precisas que habiliten asimismo actuaciones correctamente priorizadas y adaptadas a cada casuística particular. Todo ello conduce a equipos eficientes. Sin embargo, la clave estará en un correcto balance entre la automatización en el SOC aprovechando las herramientas existentes, pero evitando en la medida posible la introducción de complejidad. Y esto puede extenderse a la totalidad del marco de seguridad de la empresa. Según datos de IDC, el 55% de las empresas españolas acometerán procesos de consolidación y racionalización de soluciones de seguridad en la búsqueda de un framework unificado de seguridad (análisis de ciberseguridad, inteligencia, respuesta y orquestación), donde el apoyo del proveedor de servicios de seguridad aporten la capacitación que requiere el talento de la empresa, a la vez que asegure la integración y orquestación de aplicativos y soluciones de seguridad que permitan a la empresa abordar la gestión integral de la seguridad.

Enlaces de interés...

- La falta de personal hace que el 70% de los equipos de los SOC estén sobrecargados
- El 45% de las alertas que reciben los analistas de seguridad son falsos positivos
- Las empresas no están satisfechas con el retorno de la inversión de su SOC

it Reseller
TECH&CONSULTING

Oportunidades para el canal de TI en torno a los Fondos NextGenEU, a debate

Inteligencia y analítica de datos como oportunidad para el canal, a debate

Nuevos retos de seguridad en entornos financieros
Su impacto en el modelo de negocio

nº 68
JUNIO 2021

IA e IoT
Nuevas oportunidades, nuevos retos

it Reseller
TECH&CONSULTING

Cada mes en la revista,
cada día en la web.

ÓSCAR FUENTE

DIRECTOR Y FUNDADOR DE IEBS BUSINESS SCHOOL

Óscar Fuente, es el fundador de IEBS Business School, la escuela de negocios de la innovación y los emprendedores. Licenciado en Marketing y Gestión Comercial y Postgrado en Marketing Directo y Comercio Electrónico por ESIC-ICEMD ha desarrollado su carrera profesional en el área del marketing y management comercial en empresas como Harrods, Equifax Inc, Universidad de Barcelona y Grupo Planeta. Ha participado como inversor y/o Business Angel en startups de éxito como Glovo, Coverfy, Chicfy, Wazypark o Hannun, entre otras. También ejerce como Mentor en la aceleradora Seedorocket.

Por qué no existe desempleo en ciberseguridad

La relación entre las arquitecturas Zero Trust y la morfología de la redes, aunque pueda parecer evidente, esconde algunos detalles que no son triviales de encontrar en la literatura de ciberseguridad.

Así lo corroboran informes como el de Empleos Emergentes España de Linkedin, en el que el especialista en Ciberseguridad ocupa el puesto número cinco. Además, el mismo estudio indica que el número de expertos en el ámbito en el país ha aumentado un 60,01% respecto al año anterior y que las habilidades relacionadas con la ciberseguridad son de las más demandadas por las empresas, seguida de la automatización de procesos y marketing. La tecnología digital es el punto común de la lista de profesiones de este estudio, ya que los profesionales que más proliferan son aquellos que a través de la tecnología conectan a personas y ayudan a tomar las decisiones más inteligentes.

En este sentido, y como era de esperar, la aceleración de la transformación digital ha impulsado el sector de la Informática y telecomunicaciones,

La demanda de profesionales especializados en ciberseguridad ha aumentado por 30 los últimos diez años y su tasa de desempleo en España es cero

Según cifras de la Oficina Europea de Estadística, una persona tarda de media 5,4 meses en darse cuenta de que ha sufrido un hackeo

siendo una de las categorías con más vacantes gracias a una mayor resistencia a la crisis, según el informe Estado del Mercado Laboral en España de Infojobs. Es una profesión con gran demanda y se espera que ésta se vea altamente incrementada en un futuro. Se trata de un perfil fundamental para las empresas nativas digitales, pero es aún más crítico para aquellas organizaciones en proceso de transformación digital, en las que las vulnerabilidades informáticas puedan ocasionar problemas en la entrega de los productos o incluso pérdida de información privada y estratégica de sus clientes.

Según el balance anual publicado por el Instituto Nacional de Ciberseguridad (INCIBE), durante 2020 se gestionaron nada menos que 133.155 incidentes de ciberseguridad. Esto supone un aumento del 24% respecto a los 107.397 que se registraron el año anterior. Sin embargo, lo más alarmante es que, según cifras de la Oficina Europea de Estadística, una persona tarda de media 5,4 meses en darse cuenta de que ha sufrido un hackeo.

Uno de los ataques más sonados es el que sufrió el Servicio Público de Empleo Estatal (SEPE)

> Dentro de la ciberseguridad hay múltiples salidas profesionales, desde informática forense hasta hacking ético, gestores de incidentes, cibercrimen o desarrollo seguro

el pasado 9 de marzo por el virus Ryuk, un virus que entra en el sistema cuando un empleado abre un correo electrónico infectado. Este ataque puso en jaque al funcionamiento del sistema informático del organismo del Gobierno y de los datos que contenía. También el virus Netwalker amenazó a los hospitales españoles en marzo del año pasado. Se trata de un ransomware, un ciberataque que bloquea los sistemas informáticos de la víctima y pide un rescate a cambio de la clave para liberarlos.

Estas cifras de ataques suponen una gran amenaza para las compañías a la hora de asegurar sus sistemas. Especialmente a causa del incremento del uso de los dispositivos personales para trabajar y acceder a datos sumado al escaso conocimiento en herramientas de ciberseguridad por parte de los empleados. Este panorama ha hecho que la demanda de profesionales especializados en ciberseguridad haya aumentado por 30 los últimos diez años y que su tasa de desempleo en España sea cero.

El resumen es que hay pocos profesionales y están muy solicitados, siendo una de las necesidades reales del mercado laboral. De hecho, dentro de este ámbito hay múltiples salidas profesionales, desde informática forense hasta hacking ético, gestores de incidentes, cibercrimen o desarrollo seguro. El mundo de la ciberseguridad es especialmente innovador. Por eso, para triunfar en él, es fundamental formarse con entidades reconocidas y profesionales en activo constantemente para estar al día en una profesión cuyo objetivo es anticiparse a los ciberdelincuentes.

Enlaces de interés...

- Abierto el registro de Academia Hacker de INCIBE
- Las empresas se enfrentan al avance del phishing y a la falta de talento en seguridad
- La fuerza laboral de ciberseguridad ha crecido un 25% a nivel mundial