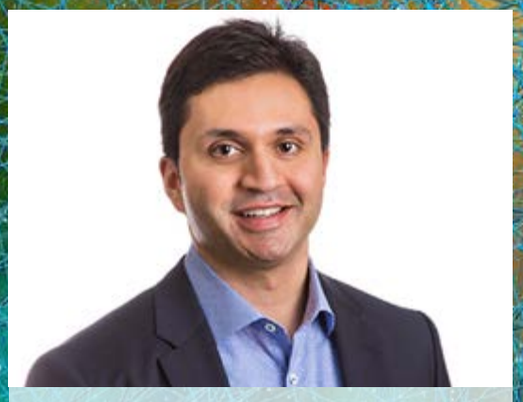
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Febrero 2021 - nº 38

NDR, la detección y respuesta llegan a la red

‘El IoT es el principal dolor de cabeza en el sector sanitario’ (Josep Bardallo)



“El reto de la seguridad cloud es equilibrar negocio y protección de datos” (Sanjay Beri)

‘Hay una voluntad real de que haya más diversidad’ (Eduvigis Ortiz)

Kaspersky Optimum y Expert, Seguridad B2B

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

NDR, ¿estás preparado?

Las redes son cada vez más complejas y distribuidas y por eso la visibilidad, antes importante, ahora es imperativa para poder detectar y detener las amenazas antes de que generen una brecha de seguridad. Aquí es donde entra en juego la detección o respuesta de red, o NDR (Network Detection and Response), una categoría de producto que tiene su origen en la detección de intrusiones en la red, la búsqueda de amenazas basada en la red y la investigación de incidentes. Se dice, además, que dentro de cinco años será una tecnología ampliamente adoptada.

En #ITDSFebrero hemos entrevistado a Josep Bardallo, CISO de Recoletas Grupo Hospitalario, quien asegura que, aparte de tener una buena base técnica, un buen CISO tiene que tener capacidades de hablar el lenguaje de negocio y que nunca se tienen en cuenta todas las contingencias. También hemos hablado con Sanjay Beri, CEO de Netskope, una empresa que, fundada en 2012 nació con la mirada puesta en lo que años después se ha convertido en revolución: SASE (Secure Access Service Edge). Eduvigis Ortiz es una persona que decide ser feliz cada día y que además de Strategic Alliances Leader de SAS es la presidenta de Women4Cyber Spain, una organización que busca promover la diversidad en el mercado de ciberseguridad. También hemos hablado con Jorge Arrufat, Head of Security en BBVA Next Technologies, para quien la base de una arquitectura de seguridad es la coherencia.

La actualidad llega marcada por la Qualys Security Conference (QSC) EMEA 2021, en la que su CEO, Philippe Courtot, aboga por una plataforma cloud abierta capaz de integrar más soluciones, recibir más telemetría, eliminar los falsos positivos y, por lo tanto, permitir la automatización. También nos hacemos eco de un debate entre Craig Jones, Director de cibercrimen de la Interpol, y Amy Hogan-Burney, Directora general de la Unidad de Crímenes Digitales de Microsoft, en torno a la importancia de las alianzas público-privadas paran combatir el cibercrimen; y de un estudio realizado por Trend Micro centrado en los desafíos asociados a la integración de la seguridad en los procesos de negocio.

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

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

En Portada

NDR, la detección y respuesta llegan a la red

itds

Sumario

Actualidad

Open Cloud Platform,
la base de un nuevo modelo de seguridad

¿Entiende la alta dirección el papel de la ciberseguridad en el negocio?

Alianza contra el cibercrimen

Kaspersky Optimum y Kaspersky Experto

Kaspersky Optimum y Kaspersky Expert:
dos familias, dos necesidades, la misma seguridad
kaspersky

Entrevistas

'El IoT es el principal dolor de cabeza en el sector sanitario'

Josep Bardallo, CISO Recoletas Red Hospitalaria

"El reto de la seguridad cloud es cómo equilibrar el avance del negocio y la protección de mis datos"

Sanjay Beri, Netskope

Hay una voluntad real de que haya más diversidad'

Eduvigis Ortiz, Presidenta de W4C Spain

'EDR y Threat Hunting son metas a las que hay que llegar, pero hay muchas cosas antes que eso'

Jorge Arrufat, BBVA Next Technologies

No solo IT

El Nacimiento de Zero Trust: CIS Community Defense Model y Mitre ATT&CK

El estado digital global: del mal uso político de la evolución digital al estado digital global

Índice de anunciantes

ESET	IT Webinars
Bitdefender	IT User
Stormshield	IT Reseller
Realsec	CdR Almacenamiento
Secure&IT	CdR Impresión
Trend Micro	

Qualys Security Conference

Open Cloud Platform, la base de un nuevo modelo de seguridad

Con una plataforma de nube abierta, las organizaciones pueden reemplazar su pila de soluciones puntuales heredadas con un conjunto de aplicaciones y servicios de cumplimiento y seguridad integrados de forma nativa y basados en la nube.

"Todos sabemos que hemos perdido la poca visibilidad que teníamos", decía Philippe Courtot, presidente y CEO de Qualys, durante la Qualys Security Conference (QSC) EMEA 2021, celebrada hace unos días en un ponencia en la que discutió por qué, en un mundo donde los dispositivos conectados están explotando, la visibilidad en todos los dispositivos (conocidos y desconocidos) y entornos es esencial.

La visibilidad a la que se refería Courtot no sólo es saber qué dispositivos hay conectados a la red, sino poder evaluar su seguridad de manera automatizada. Proponía el CEO de Qualys retirar las soluciones de seguridad tradicionales y

"Estábamos empezando a entender cómo la seguridad puede jugar un papel importante en la transformación digital, cuando tuvimos un cambio radical completo y completamente nuevo en TI"

Sumedh Thakar,
Chief Product Officer, Qualys

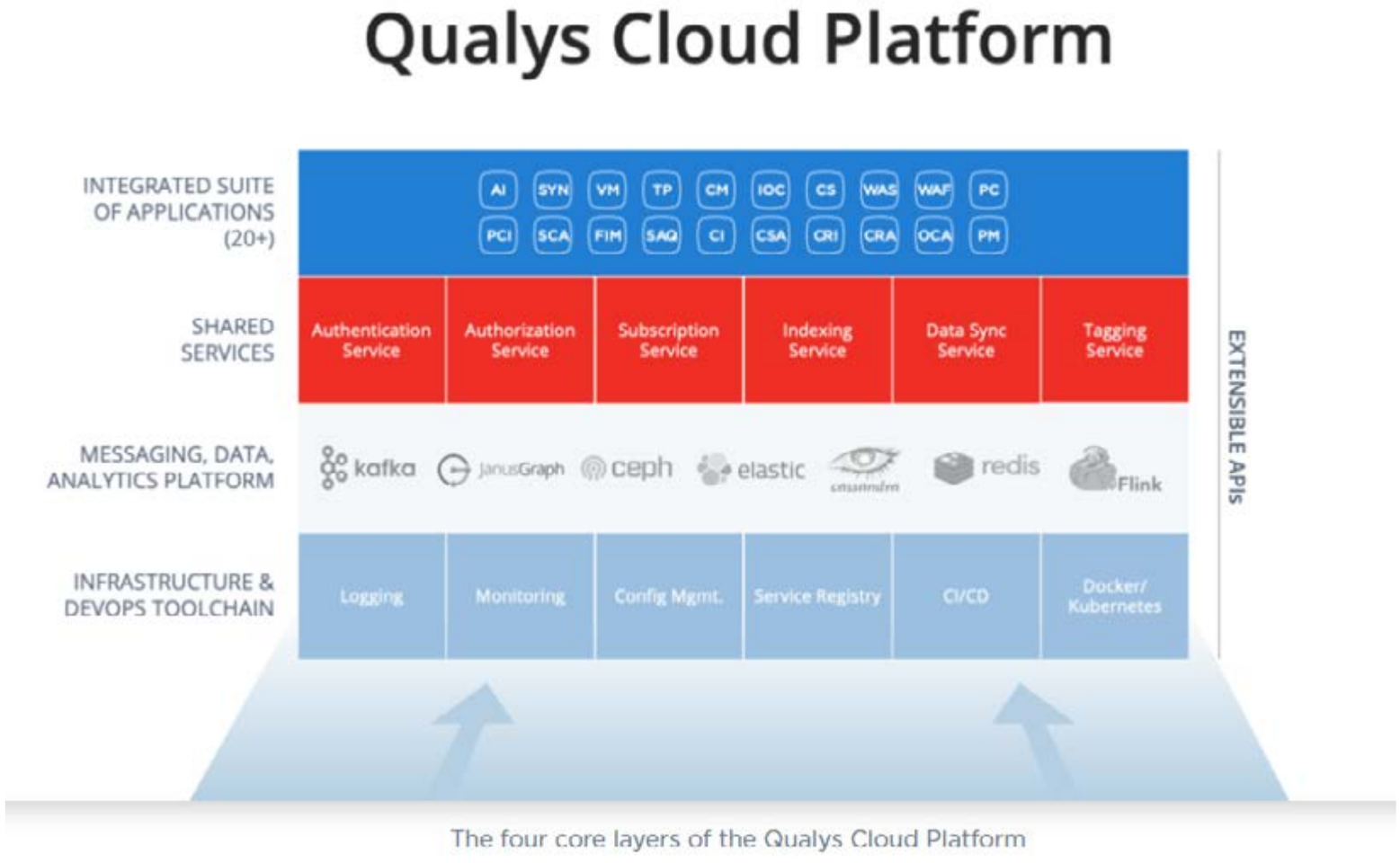
reconstruirlas teniendo en cuenta que deben poder integrarse, que deben poder escalar y trabajar en tiempo real; "idealmente deben construirse de forma nativa en la misma plataforma basada en cloud y asegurarse de que los datos que recopilan y procesan también sean accesibles para que pueda comunicarse esencialmente con otras plataformas y traer toda esa inteligencia que ha adquirido". Al final, a lo que nos lleva este camino es a una plataforma de nube abierta "que no sólo va a proporcionar mejor seguridad, sino reducir los costes" porque no se tienen diferentes aplicaciones que deben ser administradas, instaladas e implementadas, aseguraba Philippe Courtot

La respuesta

"El problema de la seguridad ha sido y sigue siendo un problema de falsos positivos". Eliminarlos, aseguraba, no sólo lleva a pensar en la automatización, sino a contar con un inventario global de

I QUALYS CLOUD PLATFORM

CLICAR PARA VER EL VÍDEO



The four core layers of the Qualys Cloud Platform

Qualys Cloud Platform ha indexado 8 billones de puntos de datos, mueve 15 mil millones de mensajes Kafka por día, procesa 3 billones de eventos de seguridad por año y realiza 6 mil millones de escaneos de IP al año

activos de TI siempre actualizado, que es la única forma de tener la escala, la velocidad, la precisión, la visibilidad y el contexto necesarios para proteger las infraestructuras de TI dinámicas e híbridas de la actualidad.

Decía también CEO de Qualys que nuestras empresas necesitan adoptar el cloud “para mejorar su modelo de negocio y ser más competitivas”, pero que “debemos tener mucho cuidado de no caer en la misma trampa que hemos estado siguiendo antes. Necesitamos construir una plataforma capaz de integrar más soluciones, recibir más telemetría, eliminar los falsos positivos y, por lo tanto, permitir la automatización”.

Seguridad basada en riesgo

Durante su discurso habló Philippe Courtot de la seguridad basada en riesgos “que hemos estado buscando tantos años”. Empezaba diciendo que hay que ser “absolutamente cuidadosos” con las soluciones que otorgan una puntación, un scoring de riesgo, porque el riesgo cambia continuamente y está asociado con el riesgo del negocio, “y hacer estas dos cosas juntas cuando no tienes visibilidad es absolutamente imposible”.

La piedra angular de un nuevo modelo de seguridad basado en una plataforma de nube abierta debe ser un inventario de activos completo y siempre actualizado que proporcione visibilidad completa en todo el entorno híbrido de una

Mejoras en Qualys Cloud Platform

Thakar destacó una serie de mejoras que Qualys ha realizado en la plataforma el año pasado que van más allá de la adición de funcionalidades incrementales. “Es una mejora continua de la plataforma”, dijo. “No estamos hablando de pequeñas características aquí y allá. Estamos hablando de visibilidad integral y acciones de respuesta integrales”.

- **VMDR** combina el inventario de activos, la gestión de vulnerabilidades, la priorización de amenazas y la remediación. “Reconstruimos toda la solución de VM reuniendo todos estos flujos de trabajo en un solo lugar” dijo. “Puede pasar de descubrir un activo a descubrir vulnerabilidades, priorizarlas y corregirlas en cuestión de minutos”
- **Multi-Vector EDR** aprovecha Qualys Cloud Agent para ir más allá de las soluciones EDR al proporcionar prevención, detección y respuesta integrales a lo largo de todo el ciclo de vida del ataque. Proporciona descubrimiento en tiempo real de puntos finales; priorización de actividades sospechosas; y capacidades de respuesta de varios niveles.
- **Patch Management** permite a las organizaciones implementar parches extrayéndolos directamente de las CDN de los proveedores, por lo que no usa VPN, y mapea los parches con CVE, lo que ayuda a optimizar y acelerar la corrección de todos los activos.
- **Seguridad SaaS y Cumplimiento,** actualmente en versión beta, permite a las organizaciones evaluar la seguridad y el cumplimiento de las aplicaciones en Office

365 de Microsoft y G Suite de Google, y pronto se agregarán Salesforce.com y Zoom. Comprueba que todas las configuraciones estén realizadas correctamente, que los usuarios adecuados tengan el acceso correcto, que nadie esté participando en actividades sospechosas o maliciosas, que las aplicaciones tengan los permisos adecuados para compartir datos, y más, según Thakar.

- **CloudView,** que le permite inventariar y evaluar continuamente la seguridad y el cumplimiento de sus cargas de trabajo en la nube pública, ahora está obteniendo capacidades de remediación y respuesta. Esas nuevas capacidades están en beta.
- **Container Runtime Security** agrega capacidades de defensa en tiempo de ejecución y aplicación automatizada a Qualys Container Security. Proporciona supervisión, detección y bloqueo basados en políticas del comportamiento de los contenedores en tiempo de ejecución, y elimina la necesidad de una gestión engorrosa de contenedores privilegiados y secundarios.
- **Enterprise Mobile Security,** ahora en versión beta, proporciona un inventario en tiempo real de dispositivos móviles, su sistema operativo y las vulnerabilidades de sus aplicaciones, y ofrece capacidades de remediación y respuesta. “Estos dispositivos móviles se están comunicando con las API que alojan los datos más importantes, por lo que debe garantizar que estén seguros y de que se rastreen en tiempo real”, dijo Thakar.
- **Security Analytics and Response,** actualmente en versión alfa, proporciona detección de amenazas más allá del punto final al ingerir datos de registro de herramientas de terceros y correlacionarlos y enriquecerlos con datos de Qualys. “Dado que Qualys Cloud Platform ya recopila y correlaciona una gran cantidad de datos, ahora podemos extraer datos de registro de terceros de, por ejemplo, firewalls de Palo Alto Networks y de sistemas de correo electrónico como Proofpoint, para incorporar un contexto adicional de qué actividad puede estar sucediendo y para permitir algunos casos de uso muy interesantes”, dijo Thakar.
- **La contención de red,** también en alfa, proporciona una respuesta sin agentes en la red con un sensor pasivo en línea o fuera de banda.

"Un verdadero enfoque de seguridad basado en el riesgo requiere que comprendamos todo lo que cambia en nuestro entorno informático, y debemos superponerlo al contexto empresarial"

Philippe Courtot, CEO, Qualys

organización; tener la capacidad de identificar en tiempo real todos los dispositivos que se conectan a la red, aprobados y no aprobados, además de proporcionarles un control de acceso granular.

También es fundamental garantizar que la plataforma ofrezca API abiertas y seguras para que los datos que recopila y procesa sean accesibles para otras plataformas en la nube y viceversa. Las tareas de seguridad y cumplimiento deben automatizarse y organizarse, y los datos deben recopilarse y analizarse masivamente en tiempo real. De esa manera, las organizaciones pueden acelerar su tiempo para remediar, mitigar y responder.

La plataforma abierta también debe ofrecer un verdadero enfoque de seguridad basado en riesgos, lo que significa equilibrar continuamente los riesgos tecnológicos con el contexto empresarial. Esto implica tener algoritmos que capturen el riesgo con precisión, y no solo proporcionar una puntuación de riesgo aislada y estática.

"Un verdadero enfoque de seguridad basado en el riesgo requiere que comprendamos todo lo que cambia en nuestro entorno informático, y debemos superponerlo al contexto empresarial", dijo Courtot.

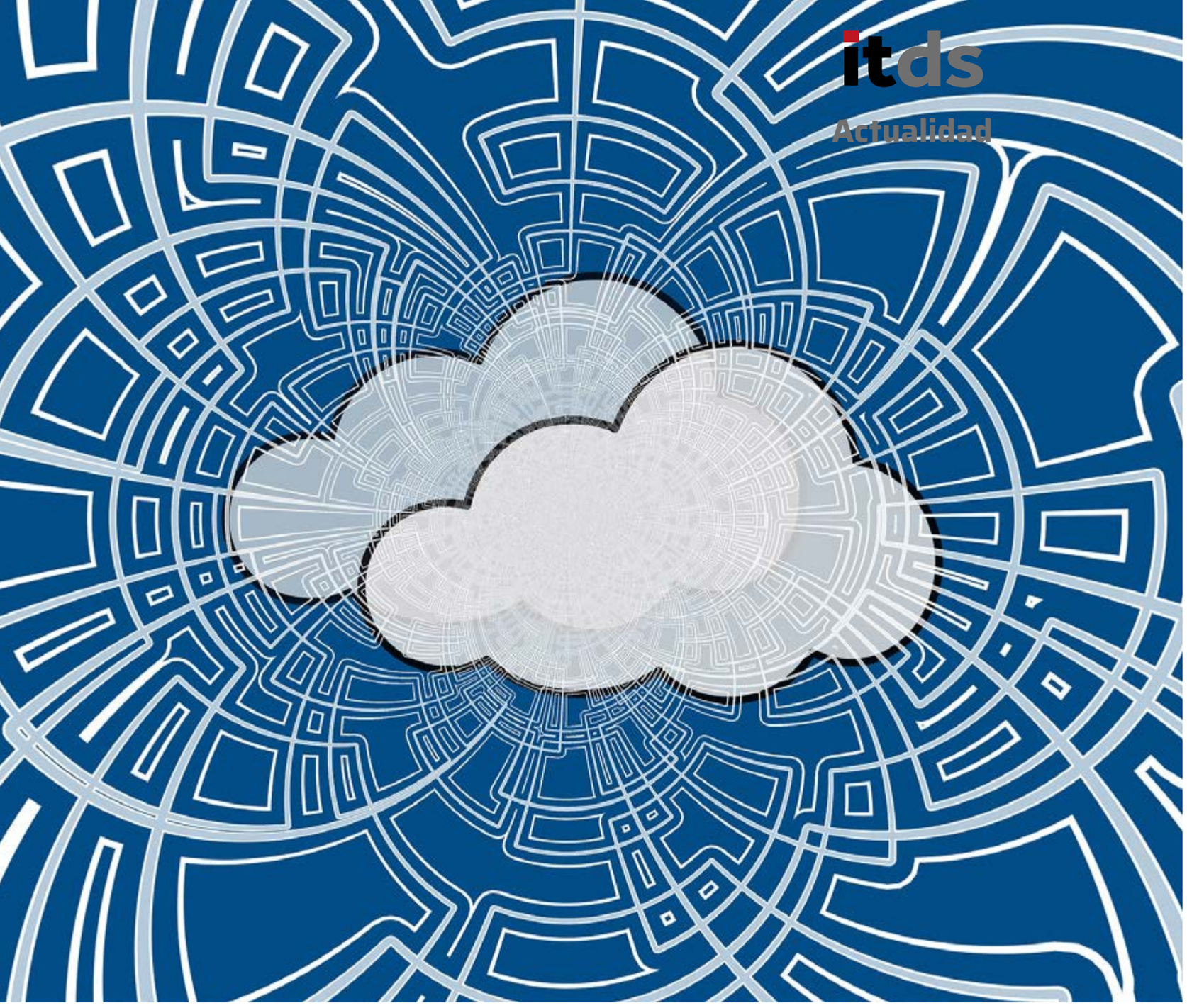
Como resumen decía el directivo que, para hacer frente a los nuevos desafíos de seguridad, no podemos hacer lo que estamos haciendo hoy; "tenemos que movernos a plataformas de nube abierta que interoperen entre sí", Qualys ya lo ha hecho integrando su plataforma cloud con una Zero Cloud Platform totalmente transparente y con seguridad incorporada, "y por supuesto hay mucho más que debemos hacer".

La Evolución de Qualys Cloud Platform

Durante su discurso Sumedh Thakar, Presidente y Chief Product Officer de la compañía, aseguró que el trabajo en remoto generó desafíos inesperados en las empresas. No sólo sobrecargó las VPN, sino que la distribución de parches se volvió difícil y, "a medida que los empleados se conectan a redes domésticas inseguras, la protección de sus dispositivos y datos se vuelve más difícil".

"Estábamos empezando a entender cómo la seguridad puede jugar un papel importante en la transformación digital, cuando tuvimos un cambio radical completo y completamente nuevo en TI", dijo Thakar, añadiendo que el problema más profundo no fue la crisis imprevista, sino el uso, aún predominante, de arquitecturas de seguridad tradicionales diseñadas para proteger redes y activos locales, en lugar de defender entornos de TI dinámicos e híbridos.

Al igual que el CEO, el CPO de Qualys dijo que las organizaciones no pueden confiar en pilas de



Es fundamental garantizar que la plataforma ofrezca API abiertas y seguras para que los datos que recopila y procesa sean accesibles para otras plataformas en la nube y viceversa

seguridad compuestas por herramientas puntuales heterogéneas que no interoperan, no se pueden escalar y están unidas, lo que las hace difíciles y costosas de implementar y administrar, dijo. No pueden depender de varios agentes con funcionalidad limitada que recopilan datos fragmentados que se envían a varias consolas. Esto obliga a los profesionales de la seguridad a correlacionar manualmente los datos, lo que les impide responder rápidamente a las amenazas.

Plataforma unificada

"No es que haya pasado nada nuevo", aseguraba Sumedh Thakar, "es que las soluciones que usamos no fueron lo suficientemente prospectivas como para crear una forma de manejar cualquier situación nueva". La respuesta de la compañía es su Cloud Platform, una plataforma unificada con un backend en la nube centralizado, un solo agente, un conjunto complementario de sensores y un conjunto integrado de aplicaciones de seguridad y cumplimiento de forma nativa.

Esta plataforma tiene tres grandes pilares:

- Un inventario de activos de TI global y siempre actualizado. La plataforma descubre todos los activos administrados y no administrados (hardware y software) y categoriza, normaliza, enriquece y organiza los datos de inventario, para una visibilidad completa de los activos en todas partes.
- Capacidades de prevención y reparación, incluida la capacidad de detectar continuamente vulnerabilidades y configuraciones incorrectas en

Una plataforma de nube abierta no sólo va a proporcionar mejor seguridad, sino reducir los costes porque no se tienen diferentes aplicaciones que deben ser administradas, instaladas e implementadas

todos los activos, y solucionar estos problemas rápidamente.

■ Capacidades de detección y respuesta, incluida la protección antimalware, detección de infracciones y acciones de respuesta como la cuarentena de activos.

Explicaba también Sumedh Thakar las cuatro grandes capas de esta plataforma cloud:

■ Un conjunto de más de 20 aplicaciones de seguridad y cumplimiento integradas de forma nativa

■ Un conjunto de servicios compartidos para tareas como autenticación, autorización, suscripciones, indexación, sincronización de datos y etiquetado.

■ Motores de mensajería, datos y análisis, incluidos Kafka, JanusGraph, Ceph, Elastic, Cassandra, Redis y Flink

■ Una infraestructura y una cadena de herramientas de DevOps que incluye registro, monitorización, administración de configuración, registro de servicios, CI / CD y Docker y Kubernetes.

En la actualidad, Qualys Cloud Platform ha indexado 8 billones de puntos de datos, mueve 15 mil millones de mensajes Kafka por día, procesa 3 billones de eventos de seguridad por año y realiza 6 mil millones de escaneos de IP al año, todo con una precisión Six Sigma del 99,9996%.

Enlaces de interés...

- Qualys Cloud Platform
- Qualys avanza hacia el endpoint
- Armor integrará en su plataforma de seguridad cloud la app Qualys CloudView

Compartir en RRSS

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

¿Entiende la alta dirección el papel de la ciberseguridad en el negocio?

Recientemente se han compartido los resultados de un estudio, patrocinado por Trend Micro y realizado por Enterprise Strategy Group, centrado en los desafíos asociados a la integración de la seguridad en los procesos de negocio.

El estudio detectó que cuanto más comprometidos y formados están los miembros de la junta con la función de ciberseguridad, más profundizan en los problemas y es más probable que den el salto de los problemas técnicos a los comerciales.

La gran mayoría (82%) de los encuestados afirmó que el ciberriesgo, o riesgo cibernético, ha aumentado en los últimos dos años, principalmente

El 51% de las organizaciones dice que su junta directiva participa en algún tipo de formación continua en ciberseguridad

gracias a un aumento de las amenazas, una superficie de ataque corporativa en expansión y el hecho de que los procesos comerciales dependen más que nunca de la tecnología.

Sin embargo, a pesar de la rápida adopción de los procesos de transformación digital en el último año, la seguridad todavía se considera principalmente (41%) o completamente (21%) un área tecnológica.

Los profesionales de la ciberseguridad a menudo lamentan que sus organizaciones no quieran una “buena seguridad” sino una seguridad que sea “suficiente”. En otras palabras, los directivos solo están dispuestos a financiar personas, procesos y tecnologías de ciberseguridad que ayuden a la organización a cumplir con las regulaciones y brindar protección básica. Desafortunadamente, los datos del estudio indican que esta actitud minimalista sigue siendo persistente en varias áreas. Por ejemplo, el 41% de las organizaciones califica el compromiso de sus ejecutivos de nivel C con la ciberseguridad como adecuado o justo, el 43% califica la intención de su organización de incorporar la ciberseguridad en los procesos comerciales y las iniciativas de TI como adecuada o justa. Aún más revelador, los gerentes no técnicos que tienen responsabilidades de ciberseguridad son calificados como adecuados, regulares o malos por el 69% de las organizaciones.

De hecho, el 44% de los encuestados indicó que su junta directiva tiene una participación limitada en muchas operaciones críticas de ciberseguridad. Esta falta de participación significa que muchas juntas directivas solo están preparadas para financiar lo mínimo necesario para cumplir con los requisitos de cumplimiento y protección.

Un programa de ciberseguridad empresarial debe incluir múltiples áreas con enfoque e inversión sesgados hacia áreas que apoyan las operaciones comerciales. Cuando se les preguntó qué áreas del programa son las más maduras, el 40% de los encuestados identificaron la seguridad de la información (es decir, proteger la confidencialidad, integridad y disponibilidad de datos sensibles), el 36% dijo operaciones de seguridad (es decir, prevención, detección y respuesta de amenazas, etc.) y el 34% señaló la seguridad en la nube (es decir, la seguridad de las aplicaciones, los datos y las cargas de trabajo basadas en la nube). Alternativamente, las áreas menos maduras fueron la gestión de riesgos de terceros, la seguridad de endpoints y el ciclo de vida de desarrollo seguro / de ingeniería (SDLC).

Dada la proliferación de aplicaciones nativas de la nube y trabajadores remotos, sería seguro asumir que las organizaciones están invirtiendo en estas áreas, pero los datos indican que no es

Enlaces de interés...

- El 47% de las empresas españolas carece de soluciones para proteger los datos
- El 64% de los CISO planea invertir en software de detección de amenazas móviles
- Un 44% de las empresas españolas carece de una protección alta de su información en remoto

así, ya que las inversiones se centran en categorías más maduras como operaciones de TI (16%), seguridad en la nube (15%), seguridad de la información (14%) y operaciones de seguridad (14%). Los CISO y los gerentes comerciales deben hacer más para alinear las inversiones con las necesidades de seguridad agudas que impactan el negocio a corto y largo plazo.

Dice también el informe que el 23% de las organizaciones priorizan la alineación de la seguridad con las iniciativas empresariales clave, una cifra un tanto baja que lleva a la compañía de seguridad a realizar tres recomendaciones:

La mayoría (85%) de las organizaciones dice que su junta está más comprometida con la ciberseguridad hoy que hace dos años

- **Agregar un Business Information Security Officer (BISO) para mejorar la alineación de la seguridad empresarial.**
- **Crear un programa medible que ayude a los CISO a comunicarse mejor con sus juntas directivas.**
- **Cambiar las estructuras para que los CISO informen directamente a su CEO.**

Para Ed Cabrera, director de ciberseguridad de Trend Micro solo se podrán "crear una cultura de ciberseguridad si los directores ejecutivos y directores corporativos predican con el ejemplo. Esto anima a todos los empleados a creer que tienen un papel en la protección de la organización".

Compartir en RRSS

ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTION DE LOS RIESGOS

Con el 7 de julio incluimos también el Elemento Humano

Bitdefender®

WWW.BITDEFENDER.ES

Alianza contra el cibercrimen

Craig Jones, Director de cibercrimen de la Interpol, y Amy Hogan-Burney, Directora general de la Unidad de Crímenes Digitales de Microsoft, han sido los protagonistas de un encuentro virtual de las Microsoft EMEA Security Series centrada, en esta ocasión, en la importancia de las alianzas público-privadas para combatir el cibercrimen.

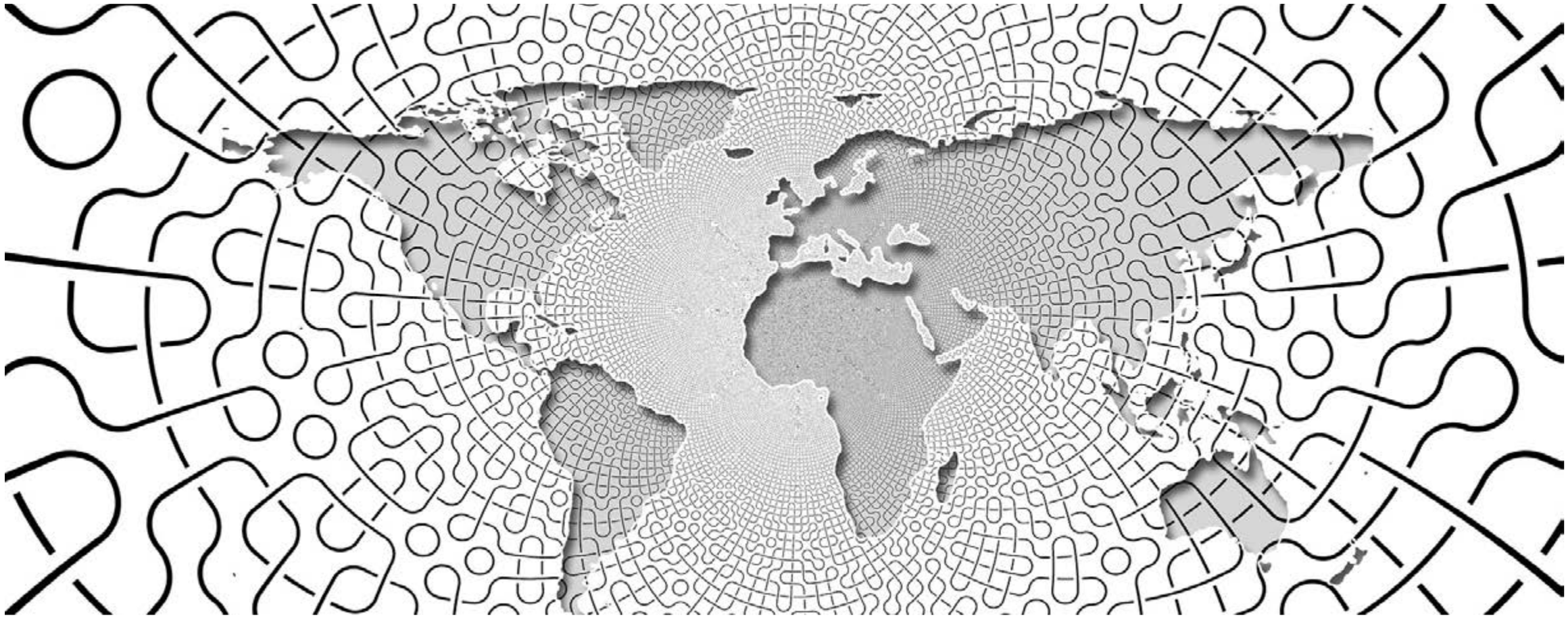
La reunión arrancó hablando de cómo ha evolucionado el panorama de ciberamenazas desde el inicio de la pandemia.

Aseguraba Amy Hogan-Burney que la tipología de los ataques no se alteró de manera significativa, sino que el trabajo en remoto acercó los objetivos a los ciberdelincuentes. Lo más interesante, decía la ejecutiva de Microsoft, es que "el teletrabajo será más permanente de lo que pensábamos al principio", y el hecho de tener a la fuerza laboral dispersa hace que las empresas tengan muchas más cosas a proteger de unos ciberdelincuentes que "son hábiles, implacables y están constantemente buscando formas de adaptar sus técnicas".

Además, los ciberdelincuentes han estado en condiciones de aprovechar el carácter evolutivo del desastre del COVID-19 para que ciertas técnicas comunes como el phishing sean mucho más poderosas. Mencionaba de manera específica la directiva esta amenazas tanto para conseguir credenciales como para lanzar ataques BEC (Business Email Compromise) que permiten interceptar pagos.

Craig Jones, observó que los ataques como phishing, que atraen a los consumidores a hacer clic en enlaces de retorno maliciosos, tienen muchas más probabilidades de triunfar cuando se utilizan

Factores para una alianza público-privada sostenible y eficaz



El cibercrimen se ha convertido en una gran amenaza para la prosperidad global. Con el objetivo de reducir su impacto mediante una cooperación público-privada, se creó la iniciativa Partnership Against Cybercrime en el marco del Foro Davos 2020 que incluye alrededor de 50 representantes de proveedores de plataformas y servicios, organizaciones financieras multinacionales, agencias gubernamentales, organizaciones internacionales y alianzas líderes sin fines de lucro.

Una de las primeras actividades del grupo de trabajo fue establecer los cuatro factores que permiten una cooperación sostenible y eficaz:

1. Si bien el objetivo final de la cooperación sirve a un bien mayor, **cualquier colaboración debe tener en cuenta los respectivos intereses y misiones de los participantes.**

2. El segundo factor es la confianza. Garantizar la transparencia, promover la equidad y la justicia, hacer del intercambio voluntario la opción predeterminada y favorecer la toma de decisiones conjunta son algunas de las formas de generar confianza a largo plazo.

3. El **tercer factor es la alineación estratégica.** Los participantes deben ponerse de acuerdo sobre los objetivos estratégicos. Todos los participantes deben comprender las necesidades, los objetivos y los valores respectivos de los demás e identificar continuamente un terreno mutuo.

4. El cuarto factor es la estructura. La cooperación eficaz a largo plazo requiere reglas de negocio, procesos y gobernanza transparentes y repetibles.

En este panorama, la necesidad de que los organismos encargados de hacer cumplir la ley trabajen a través de las fronteras y con múltiples entidades privadas ha crecido significativamente. Honan-Burney aseguraba que “los delincuentes no se preocupan por las fronteras geográficas, no les importa dónde están sus víctimas”, ni siquiera dónde está su infraestructura. Hasta cierto punto, aseguraba la directiva de Microsoft, “tenemos que

Amy-Hogan-Burney_-Microsoft

señuelos relevantes como COVID. Aseguró durante su intervención que “el factor humano está en todo esto”.

Comentando que se ha convertido en habitual por parte de los ciberdelincuentes aprovechar situaciones geopolíticas en sus ataques, ambos portavoces revelaron que, si el año pasado el topic era el COVID, lo que están explotando ahora son las vacunas. Según Craig Jones los delincuentes están comenzando a usar vacunas y certificados falsificados para engañar a los usuarios, y señaló que las personas que viven en áreas más pobres serán específicamente susceptibles a tales tácticas. “Quienes no tengan acceso a la vacuna la querrán conseguir implique lo que implique”, dijo.

Craig Jones, Interpol

hacer exactamente lo mismo", y que no importe que yo esté sentada en Estados Unidos, el ciberdelincuente en Nigeria y las víctimas en otro país, "tenemos que hacer el trabajo juntos".

Jones estuvo de acuerdo y destacó que la investigación del ciberdelito generalmente exige que las empresas encargadas de hacer cumplir las regulaciones obtengan acceso a la información de varias empresas diferentes. "Es posible que tenga una sola empresa que solo vea una pequeña parte de ella y tenemos que comenzar a agregar eso", describió.

A diferencia de otras áreas delictivas, el sector privado a menudo tiene un acceso superior a la información técnica y la capacidad de identificar, rastrear y analizar las infraestructuras y los servicios de los ciberdelincuentes. Esto le da al sector privado la capacidad no solo para descubrir actividades delictivas, sino también para emprender acciones disruptivas específicas al desmantelar la infraestructura de los delincuentes. Sin embargo, estas capacidades tienen límites y solo los gobiernos tienen la autoridad legal para enjuiciar a los ciberdelincuentes e imponer sanciones. Por lo tanto, ni el sector público ni el privado tienen la capacidad suficiente para reducir el impacto global del ciberdelito por sí mismos.

A diferencia de otras áreas delictivas, el sector privado a menudo tiene un acceso superior a la información técnica y la capacidad de identificar, rastrear y analizar las infraestructuras y los servicios de los ciberdelincuentes

Enlaces de interés...

- Acuerdo contra el cibercrimen
- Interpol

Los ataques como phishing, que atraen a los consumidores a hacer clic en enlaces de retorno maliciosos, tienen muchas más probabilidades de triunfar cuando se utilizan señuelos relevantes como COVID

Dadas las limitaciones de cada sector, la única forma de lograr el objetivo de reducir el ciberdelito global es a través de la cooperación público-privada.

Honan-Burney aseguró durante su intervención que la coordinación que ahora involucra a empresas como Microsoft y la aplicación de las regulaciones está mejorando, ya que existe un reconocimiento cada vez mayor del valor de llevar a los ciberdelincuentes ante la justicia para enriquecer la seguridad digital sobre la expresión prolongada.

Argumentaba Honan-Burney en un artículo publicado a finales del año pasado que una respuesta eficaz al delito cibernético requiere explorar muchos cursos de acción posibles y tener en cuenta los intereses tanto del sector público como del privado. Diseñar e implementar tales respuestas requiere creatividad en la conceptualización e implementación de acciones colaborativas. “Necesitamos interrumpir rápidamente las infraestructuras y los servicios de los ciberdelincuentes de manera que aumente el costo para los actores delictivos, en un esfuerzo coordinado. Y, siempre que sea posible, debemos atribuir y enjuiciar el delito cibernético para aumentar el riesgo de los actores criminales y ofrecer justicia a las víctimas. En última instancia, esto frena al adversario en su camino; la agilidad es a menudo un lujo que disfrutan”, dice el artículo.

Compartir en RRSS

STORMSHIELD

Primer cortafuegos en obtener ambas certificaciones del CCN.

Producto Cualificado y Producto Aprobado

Stormshield, filial participada al 100 % de Airbus CyberSecurity, propone soluciones de seguridad completas e innovadoras para proteger las redes (Stormshield Network Security), los puestos de trabajo (Stormshield Endpoint Security) y los datos (Stormshield Data Security). www.stormshield.com/es/

‘El IoT es el principal dolor de cabeza en el sector sanitario’

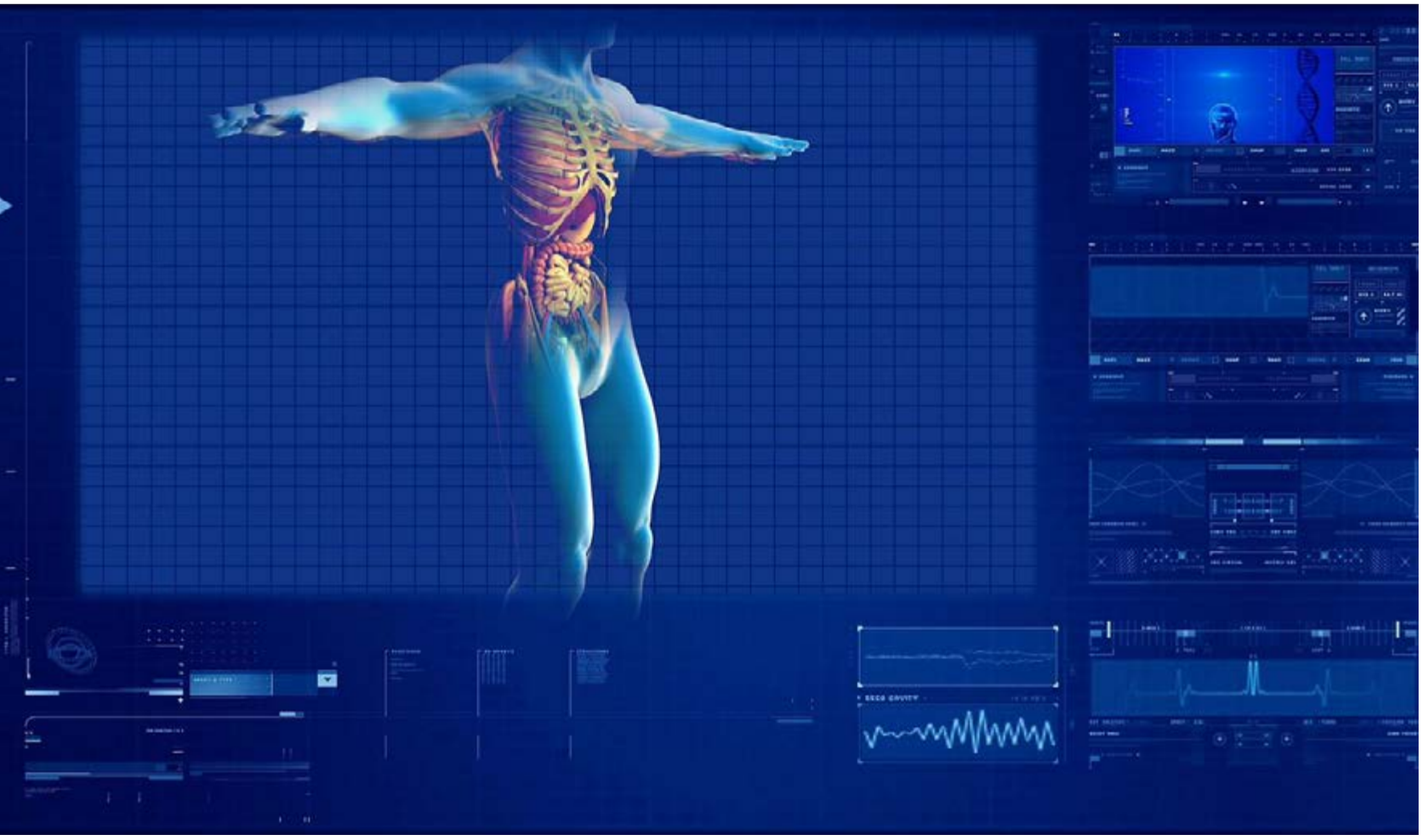
(Josep Bardallo, CISO Recoletas Red Hospitalaria)

Texto: Rosalía Arroyo

Con más de 20 años de experiencia, Josep Bardallo inició su carrera en la compañía de seguros Winterthur-AXA, de la que salió como responsable operativo y de seguridad para co-fundar algunas empresas de servicios TI y seguridad, como Virtualsys o Nilo TI, y dar clases en algunas universidades. También ha realizado tareas de consultoría y desarrollo de negocio, y ha sido el CTO de PasswordBank, una empresa con oficinas en Silicon Valley y Barcelona que acabó en manos de Symantec.

Actualmente es el CIO, CISO y DPO de Recoletas Red Hospitalaria, un importante grupo hospitalario a nivel nacional y líder en Castilla y León que cuenta con 7 hospitales, 11 centros médicos, 5 institutos y 4 centros de diagnóstico repartidos por varias provincias españolas. También es Security Consulting Manager en A2Security, actúa como CISO virtual en empresas como AEDAS, Copernicus o Via Celere y enseña sobre Seguridad en el Master de la Universidad de Sevilla.

Arrancamos la entrevista preguntando por las cualidades que debe tener un buen CISO, y las tiene claras: “Aparte de tener una buena base técnica,



"Recoletas Red Hospitalaria tiene 1.800 trabajadores, pero que hay tres veces más equipos conectados en red"

un buen CISO tiene que tener capacidades de hablar el lenguaje de negocio, saber expresar los riesgos de seguridad a la alta dirección", asegura Josep Bardallo, añadiendo que aunque hace unos años no era tan relevante, hoy sí que se necesita tener conocimiento de las regulaciones y normativas porque "incluso aunque no sean específicas de seguridad, casi todas las auditorías implican una parte de ciberseguridad", dice el responsable de TI y CISO de Recoletas Grupo Hospitalario.

No acaban aquí las capacidades de un buen CISO. Añade el directivo el tener paciencia "y una visión a medio-largo plazo, que es una de las tareas más complicadas de conseguir".

¿Crees que la seguridad se ha convertido finalmente en una prioridad para la empresa española? "No". La respuesta no puede ser más concisa. Añade que solo se ha convertido en prioridad para las empresas que están auditadas, reguladas, o están en Bolsa; "en estos casos sí que hay una prioridad porque están constantemente auditadas y las empresas se han puesto las pilas". Reconoce, eso sí, que no falta mucho para que la ciberseguridad se convierta en una prioridad para todas las empresas.

Impacto de COVID 19

La pandemia que arrancó a finales de 2019 en Asia y se extendió rápidamente impactó de lleno en la vida y los negocios de todo el mundo. En apenas unas semanas y ante una movilidad reducida, un trabajo en remoto casi obligatorio y una adopción del cloud acelerada, los planes de contingencia se sacaron de los cajones para que muchos responsables de TI, entre ellos Josep Bardallo, se dieran cuenta de que "nunca tienes en cuenta todas las contingencias". Como han repetido varios expertos entrevistados en estas páginas el factor humano no se había tenido en cuenta de manera global en esos planes de contingencia.

"Me encontré con médicos que querían trabajar desde casa. Nunca había pensado tener que hacer una contingencia de este tipo, sino que se cayeran los sistemas, las comunicaciones… Surgieron

"Si contrato algún servicio tiene que haber tenido experiencia en el sector sanitario y sus problemáticas"

nuevos casos que no teníamos previsto, y hubo que adaptarse rápidamente a la nueva situación, a que el usuario trabaje, aunque esté en casa y con un ordenador suyo. Pero siempre tiene que haber un mínimo de seguridad".

Respecto a los CEOs, en opinión de Josep Bardallo, han aprendido la importancia de la agilidad y los planes de contingencia, "a los que no les daban tanta importancia"; han visto cómo era cierto lo que se les estaba diciendo desde hace tiempo: tenemos que ser ágiles, tener resiliencia, y muchos proveedores y bien cuidados. De forma que los responsables empresariales se han dado cuenta de que merece la pena gastar dinero en los planes de contingencia.

Cloud y Servicios Gestionados

Sobre la adopción del cloud, tiene claro el responsable de ciberseguridad de Recoletas Red Hospitalaria que el cloud es un hecho, que todo el mundo, quiera o no quiera, utiliza una media de más de cien aplicaciones; "si eres un CISO y no lo das por hecho es que lo estás haciendo mal". ¿Cómo se aborda desde el punto de vista de seguridad? Yo creo que se debe abordar como si fuera otro datacenter más en el que tienes que asumir la seguridad y la responsabilidad; "yo no creo en esto de la responsabilidad compartida. La responsabilidad es tuya y otra cosas es que subcontrates o delegues algunas cosas, pero tú sigues teniendo la responsabilidad y debes tener una visión y control de todo esto", dice Bardallo.

Haciendo referencia al Shadow IT, menciona el directivo la importancia de contar con tecnologías que te permitan descubrir los servicios y aplicaciones cloud que tiene contratada una empresa.

Sobre los servicios de seguridad gestionada, Bardallo los ve como imprescindibles en los entornos que requieren una seguridad 24x7, y necesarios en el resto, entre otras cosas porque las diferentes tecnología son cada vez más complejas. A la hora de escoger proveedor Josep Bardallo se fija en los niveles de servicio y referencias que puede aportar;

"Me encontré con médicos que querían trabajar desde casa. Nunca había pensado tener que hacer una contingencia de este tipo"

“estamos en el entorno sanitario, un entorno muy diferente al resto de sectores, y si contrato algún servicio tiene que haber tenido experiencia de ese tipo de sectores y sus problemáticas”, dice el directivo.

Uno de los factores que diferencia al sector sanitario es que hay mucho IoT asociado. Este IoT es, según Bardallo, “el principal dolor de cabeza en el sector sanitario”; en este entorno la palabra clave, como en el cloud, es la visibilidad, utilizar tecnologías que te permiten descubrirlo y aplicar diferentes medidas, incluida las más básicas como la segmentación de la red.

Si tenemos en cuenta la cantidad de máquinas médicas que hay conectadas, ¿tiene Josep Bardallo que proteger más máquinas que personas? Nos cuenta que el Recoletas Red Hospitalaria tiene 1.800 trabajadores, pero que hay tres veces más equipos conectados en red que van desde los ordenadores, a impresoras, máquinas de laboratorio, de rayos X… teniendo en cuenta que en lo que se refiere a dispositivos móviles sólo están conectados los que se utilizan internamente para atender a los pacientes, y no los dispositivos móviles de todos los empleados.

Tecnologías y previsiones

Todo lo que se necesite para poder ver, que aporte visibilidad es, para Josep Bardallo, una herramienta imprescindible hoy en día. Considera fundamental la protección de los datos, así como la del endpoint mediante soluciones EDR; también la protección del correo electrónico es clave en tanto en cuanto es por donde más se mueven los datos. Por último, “todo lo que tiene que ver con contingencia. Todas estos puntos son imprescindibles para mí”.

"La ciberseguridad aún no es prioridad para la empresa española"

Cuando le preguntamos sobre las soluciones o tecnología que le gustaría implementar si tuviera un cheque el blanco, menciona el CISO de Recoletas Red Hospitalaria que hay dos que tienen mucho futuro: el análisis con Inteligencia Artificial de los logs, "porque tenemos muchas tecnologías que nos recogen información de todo lo que ocurre, pero todo eso tienes que analizarlo", y análisis del comportamiento (UEBA) porque te permite detectar más amenazas.

"Nos van a dar más presupuestos", dice Bardallo cuando le preguntamos si espera algún cambio significativo en 2021 en torno a la seguridad. En lo que tiene que ver con la seguridad, dice que se irán consolidando las tecnología que buscan aumentar el control sobre la nube.

Reconociendo que el dato médico es más caro, confirma el directivo que ha habido un crecimiento de los ataques contra el sector sanitario y que durante la pandemia "hubo incremento importante de intentos de campañas de phishing".

Precisamente datos de un reciente informe aseguran que el sistema sanitario se ha convertido en la diana de los ciberataques y si bien se ha mejorado la seguridad y protección de los datos, los ataques maliciosos son cada vez más frecuentes y complejos, sobre todo desde que se desató la pandemia. El estudio, de Check Point Research alerta de un aumento del 45% en los ataques dirigidos contra empresas relacionadas con la salud y la Medicina a nivel mundial"; España, que ha visto cómo sus cifras se duplicaban, es el tercer país con mayor grado de infección, sólo por detrás de Canadá (250%) y Alemania (220%).

Enlaces de interés...

- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)
- 'En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar' (Jesús Alonso Murillo, Ferrovial Servicios)
- 'Los CISO somos ciberresilientes desde hace mucho tiempo' (Javier Sánchez Salas - HAYA Real Estate)

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.

‘El reto de la seguridad cloud es cómo equilibrar el avance del negocio y la protección de mis datos’

(Sajay Beri)

“La visión de la compañía desde sus inicios es lo que ahora se llama SASE”. Con esta frase arranca una entrevista a Sanjay Beri, CEO de Netskope. La compañía, que fundara el propio Beri en 2012, acumula 740 millones de dólares en varias rondas de financiación, y se posicionó rápidamente como un referente en el mundo de los CASB (Cloud Access Security Broker), un término que terminó quedándose corto para el enorme reto que supone la migración al cloud.

Rosalía Arroyo

Las tecnologías CASB generaron una gran revolución en un mercado que consolidó rápidamente y casi dejaron huérfano a Netskope, que vio desaparecer a Adallom en manos de Microsoft, a Skyhigh Networks en las de McAfee, Palerra en las de Oracle, o Elastica y Perspecsys en las de BlueCoat, posteriormente adquirida por Symantec. Con un Shadow IT disparado y una postura más amigable frente al cloud, las empresas buscaban visibilidad, control y, en definitiva, seguridad en la nube. Y mientras que CASB se convirtió en una herramienta suficiente para mantener las políticas de seguridad y proteger las aplicación en la nube, el concepto Secure Access Service Edge (SASE) vino a proporcionar todas las capacidades de CASB, así como soluciones de seguridad adicionales y capacidades de confianza cero que se extienden más allá de la nube, llegando al usuario remoto y a la sucursal. Definido por Gartner en 2019 este modelo está revolucionando el sector, generando ‘SASE Believers’, e

APIs, el gran lenguaje de Internet

También hablamos con Sanjay Beri de las APIs, que él considera el nuevo lenguaje de Internet. Inicialmente, explica, el lenguaje eran los puertos y las direcciones IP; posteriormente fue el lenguaje de las aplicaciones, cuando surgieron empresas como Palo Alto en contraposición a tras como Juniper. Más de diez años después, el lenguaje ha vuelto a cambiar, "ya no son las aplicaciones, son las APIs", todo lo que sucede en Internet cuando se accede a un sitio web, a Office o a Salesforce... el lenguaje subyacente de esas aplicaciones, son las APIs, lo que significa que "los equipos de seguridad tradicionales, como los proxys o los firewalls, ya no pueden comprender lo que la gente está haciendo".

Cuando se entiende el lenguaje de las APIs se comprende lo que está haciendo el usuario y se comprenden los riesgos. "Esa es la razón por la que Sequoia ha financiado a las mayores empresas de seguridad del mundo", incluida Netskope, que cerró a primeros de 2020 una inversión de 340 millones de dólares.

impulsando la adopción de seguridad en la nube.

Defiende Sanjay Beri que la visión de la compañía "siempre fue mucho más amplia que un CASB" y fue la de querer "convertirse en un proveedor de seguridad cloud con una propuesta diferencial que no sólo tenga en cuenta en Saas, el IaaS y la navegación web, sino las aplicaciones legacy y avances como el Edge o la 5G".

De forma que, ¿es el gran momento para Netskope? "Sí. Estamos en el lado correcto de la historia", asegura el directivo, añadiendo que el mundo se está moviendo hacia una nueva forma de trabajar y que los clientes buscan "una empresa que esté innovando para poder, ellos a su vez, seguir innovando en su forma de trabajar". Una empresa que no es otra que Netskope, que durante los últimos años ha trabajado para crear NewEdge, la nube privada de seguridad más grande y de mayor rendimiento del mundo que potencia los servicios de seguridad online de Netskope Security Cloud y está a 15 milisegundos de cualquier persona del mundo. En la actualidad, NewEdge funciona con centros de datos en

"Necesitas permitir que los empleados usen el SaaS, la nube pública, que trabajen de forma remota, pero al mismo tiempo necesitas seguridad"

40 regiones -el año pasado se abrió uno en Madrid, y cada mes se agregan nuevos centros de datos.

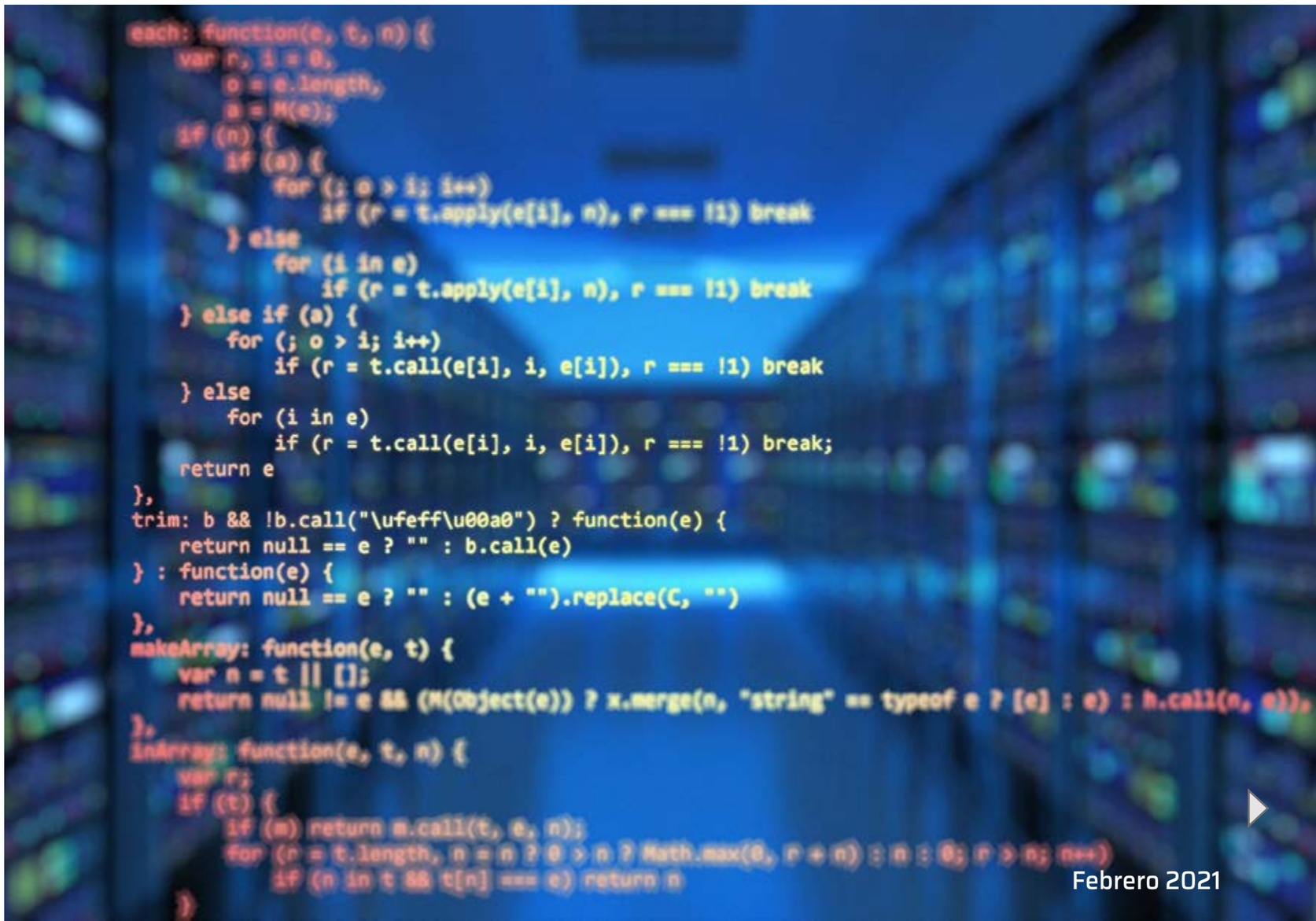
Impacto de la experiencia de Usuario

Hablar de NewEdge es hablar de la experiencia de usuario en la nube. Y eso le preguntamos al CEO de Netskope: ¿Cuál es el impacto de la experiencia de usuario en la nube? “La realidad es que debes diseñar tu nube de la manera correcta”, explica Beri. Dice que una de las cosas más importantes para la compañía es “cómo ofrecer seguridad sin ninguna penalización en el rendimiento”, así que la compañía invirtió una gran cantidad de dinero y talento para el desarrollo de NewEdge, una red compuesta por docenas de centros de datos repartidos y conectados por todo el mundo que llevan a más de un cliente a decir “compré seguridad y estoy obteniendo rendimiento”, asegura Sanjay Beri.

La clave, añade Beri, es ofrecer rendimiento al tiempo que se ofrece seguridad cercana a los usuarios; “cada centro de datos tiene una funcionalidad de seguridad completa. Está descifrando el tráfico cifrado, está aplicando políticas de pérdida de datos, previene contra el malware, está detectando comportamientos anómalos. No sólo se trata de tener una red rápida, sino de poder ofrecer servicios de seguridad con este tipo de rendimiento”.

Hay que tener en cuenta, explica el CEO de Netskope, que la mayoría de los proveedores de seguridad han optado básicamente por tomar a sus clientes y moverlos a la nube pública, “y la nube pública es ideal para aplicaciones, pero es horrible como

El concepto Secure Access Service Edge (SASE) vino a proporcionar todas las capacidades de CASB, así como soluciones de seguridad adicionales y capacidades de confianza cero que se extienden más allá de la nube, llegando al usuario remoto y a la sucursal.



NETSKOPE NEWEDGE

CLICAR PARA VER EL VÍDEO

NewEdge, la nube privada de seguridad de Netskope está a 15 milisegundos de cualquier persona del mundo

red", dice Beri, añadiendo que "debido a eso, están obteniendo un rendimiento diez veces peor. Los clientes lo ven muy rápidamente y piden algo diseñado como una red en la nube". Menciona aquí el directivo a Joe DePalo, responsable del diseño, la construcción y las operaciones de las generaciones actuales y futuras de la infraestructura y plataforma de Netskope, y sobre el que Beri dice que es "uno de los mejores diseñadores de redes en la nube del mundo", y asegura que la compañía ha invertido más de ciento cincuenta millones de dólares para construir esta red para que pueda funcionar de esta manera. "Hay muy pocas empresas que tengan la gente, el capital y el beneficio de diseñarlo desde cero", asegura Beri.

Reto de la seguridad cloud

Todo el mundo está atacando a todo el mundo, dice Beri cuando le preguntamos cuál es el gran reto de la seguridad cloud. Lo que todos buscan, dice, son los datos, y por eso es primordial saber dónde están sus datos y protegerlos sin obstaculizar el negocio; "necesitas permitir que los empleados usen el SaaS, la nube pública, que trabajen de forma remota, pero al mismo tiempo necesitas seguridad. El problema, el reto de la seguridad cloud, es cómo equilibrar el balance del negocio y la protección de mis datos".

Recuerda el directivo que cuando las soluciones de Netskope entran en acción se detectan cosas como que las personas publican datos confidenciales en un blog o se las descargan en un blog; "descubrimos este tipo de cosas y luego permitimos, de manera automatizada, establecer reglas y gobernanza para que no permita que estas cosas sucedan y, como resultado, sepan dónde están sus datos".

Qué esperar de 2021

No es un secreto que en 2020 se aceleró la transformación digital, y eso va a seguir en 2021. Sobre lo que ocurrirá este año dice Beri que hay 150.000

"La nube pública es ideal para aplicaciones, pero es horrible como red"

millones de dólares en capitalización de mercado para las empresas de seguridad de redes, y que las empresas gastan cerca de 30.000 millones de dólares al año en la compra de seguridad para redes de datos. Al mismo tiempo, el 98% de esas inversiones siguen realizándose en una caja, "pero te das cuenta que la gente trabaja en forma remota, que el idioma de Internet ha cambiado", y lo que va a suceder es que "el gasto se trasladará a un modelo de seguridad basado en la nube que permitirá la nueva forma de trabajar". Como resultado, continúa diciendo el CEO de Netskope, "seguirás viendo palabras como SASE, nube o Edge".

Añade Beri que el 77% de las personas que utilizan NewEdge trabajan de forma remota, "y por eso creo que la otra gran tendencia es que la gente necesita tener una gran cobertura mundial para sus soluciones". it

Enlaces de interés...

- "Para ser realmente un Service Edge tienes que tener un Edge" (Samuel Bonete, Netskope)
- Internet is Broken
- W Arquitectura SASE

Compartir en RRSS

Secure&IT by LKS

www.secureit.es

CIBERSEGURIDAD EN LA DESESCALADA DE LA COVID-19

& Promoción especial

Auditorías y seguridad gestionada

& Privacidad vs. COVID-19

¿Qué medidas de contención pueden implementar las empresas?

& Adecuación a la normativa e-commerce

¿Cómo adaptar una web para vender de forma online?

+ INFO

‘Hay una voluntad real de que haya más diversidad’

(Eduvigis Ortiz, Presidenta de W4C Spain)

Texto: Rosalía Arroyo • Fotos: Ania Lewandowska

Eduvigis Ortiz es… “una persona que decide ser feliz cada día, que decide aportar su granito de arena cada día, una persona que decide sumar”, así se define esta profesional con 29 años de experiencia en el sector TI, sobre todo en el área de consultoría, que ocupa el cargo de Strategic Alliances Leader de SAS, y a quien le queda energía y pasión para presidir Women4Cyber Spain, el capítulo español de la Fundación Europea sin ánimo de lucro Women4Cyber que busca promover programas de formación en ciberseguridad para atraer más talento femenino y potenciar la presencia de mujeres en el mercado de la ciberseguridad.

"En ciberseguridad todos cabemos. Se necesitan todas las miradas"

Su compromiso con una sociedad con igualdad de oportunidades le ha llevado a ser miembro del Patronato de la Red de Mujeres Profesionales de Madrid durante siete años; lidera el capítulo de Madrid del MeetUp for Women in Machine Learning and Data Science (WiMLDS) y se desempeña como mentora en el Programa Pulsar de la Fundación Everis y también en el Programa Mujeres e Ingeniería de la Real Academia de Ingeniería (RAI) en España. También es jueza en el programa Technovation.

"Llegó, sumó y se fue en paz", es lo que desea que rece su epitafio dentro de muchos años; agradece el privilegio de haber trabajado siempre en lo que le ha gustado, de tener una familia maravillosa y haber podido rodearse de gente buena y solidaria. Es una mujer de acción que asegura: "a mí me gusta que las cosas sucedan".

Estudiante de Ingeniería Industrial no entendía una minoría que no era reflejo de la sociedad real; "de 45 alumnos éramos 8 mujeres", una minoría que se fue repitiendo en los sucesivos trabajos de Eduvigis Ortiz, ya fuera en producción o control de calidad como ingeniera industrial o en el sector tecnológico, entorno en donde además hay "muchísimas más oportunidades".

Antes de la creación oficial de Women4Cyber Spain, en España triunfaba el Women In Cybersecurity of Spain, más conocido como WICS, que también contaba con Eduvigis Ortiz en su cúpula directiva. Fue a finales de 2015, en su paso por Capgemini, cuando Eduvigis se siente atraída por la ciberseguridad "porque veía que era un pilar de la vida digital". En aquellos tiempos, asegura esta experta, de lo que se hablaba sobre todo era del cloud, pero lo que iba a llegar después, irremediablemente, era la securización del cloud; su posición en la consultora le permite investigar y, más adelante, buscar trabajo en ciberseguridad "que era lo que me gustaba". Los primeros pasos los daría en la unidad de ciberseguridad de Prosegur, donde su trabajo para realizar el esquema de alianzas de la unidad le llevó a hacer "un máster acelerado en ciberseguridad gracias a estar viendo a proveedores, evaluando soluciones… fue una etapa muy intensa, muy exigente y muy bonita porque aprendí

"Me siento una privilegiada porque tengo la oportunidad de trabajar con los dos pilares de la vida digital, que son los datos y la ciberseguridad"

EDUVIGIS ORTIZ EN #14ENISESPIRIT

CLICAR PARA VER EL VÍDEO

muchísimo" que le permitió, además, "cogerle más cariño todavía si cabe a la ciberseguridad, porque soy una apasionada".

Tras pasar por la experiencia de intentar montar su propia empresa, es fichada por Novared, una empresa chilena centrada en ciberseguridad con 25 años de experiencia que abría oficina en España, y con la que estuvo más de un año hasta que una llamada de SAS abre una nueva oportunidad en el mundo de la analítica de seguridad y en la que Eduvigis Ortiz se siente una privilegiada porque "tengo la oportunidad de trabajar con los dos pilares de la vida digital, que son los datos y la ciberseguridad".

Dos mujeres y un destino

El destino unió a Eduvigis Ortiz y Karen Gainer, actual Global Head of Cybersecurity Defense en Siemens. Dos mujeres con las mismas inquietudes en torno al posicionamiento de la mujer en el mercado de las TI y la ciberseguridad. Así es como se gestó la creación de Women in Cybersecurity Spain (WICS), a la que pronto se incorporaron Julia Perea, Idoia Mateo, Rosa Díaz y otras grandes expertas de la comunidad de ciberseguridad en España, una comunidad que Ortiz asegura que es muy generosa y a la que le gusta compartir.

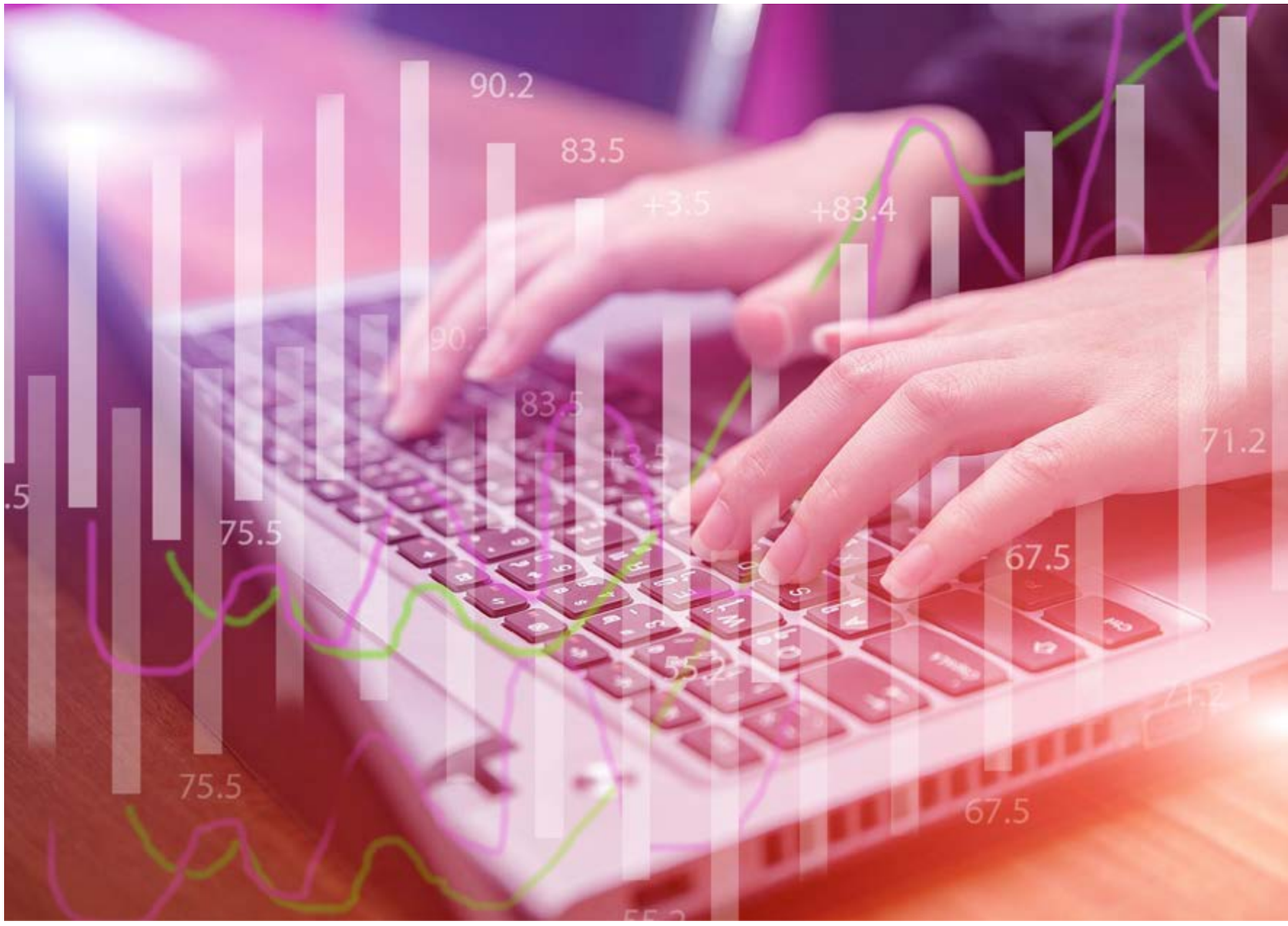
La posibilidad de abrir capítulos nacionales de la fundación Women4Cyber atrajo la atención de estas luchadoras que se plantearon inicialmente mantener en paralelo ambas asociaciones, aunque posteriormente se dieron cuenta que "no somos tantas mujeres en España" y era mejor tener una sola asociación que, si depende de Europa, "nos da más fuerza". En poco tiempo la página de LinkedIn de la asociación suma ya más de mil miembros, frente a los 200 que tenía en octubre del año pasado

"Estamos teniendo un apoyo de la comunidad increíble", asegura Eduvigis Ortiz. El plan estratégico

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
SPAIN CHAPTER

Líneas de Actuación de W4C Spain

1. Crear comunidad promoviendo las mejores prácticas y visibilizando los referentes femeninos del sector
2. Promover programas de formación a todos los niveles en ciberseguridad y tecnología para atraer más talento femenino
3. Potenciar la presencia de mujeres en el mercado laboral de la ciberseguridad a través de distintos programas
4. Incrementar la presencia de mujeres en la Investigación e Innovación (I + I) en ciberseguridad y en el campo de las tecnologías emergentes
5. Apoyar y dar forma a políticas a nivel nacional y de la UE que estén en consonancia con los mensajes de Women4Cyber
6. Establecer y coordinar alianzas nacionales e internacionales que apoyen la misión de Women4Cyber



de la asociación está basado en líneas de trabajo que se realizan con empresas, administración pública y entornos educativos. Ya se han firmado alianzas con el ISMs Forum o con la Universidad Católica de Ávila y se trabaja para fomentar que haya más mujeres formándose en ciberseguridad y crear, en general, “un verdadero espacio inclusivo, colaborativo e integrado de toda la sociedad con un objetivo común: un mundo más diverso, más inclusivo y más justo”.

Una de las grandes líneas de trabajo de la asociación es la de la visibilidad y los referentes, necesarios para que desde la edad temprana las niñas vean normalizado la presencia de la mujer en entornos de TI y ciberseguridad, “y que sea una opción

Enlaces de interés...

- Women for Cybersecurity Spain firma su primer acuerdo de colaboración
- Nace oficialmente Women4Cyber Spain

"Se trabaja para fomentar que haya más mujeres formándose en ciberseguridad y crear, en general, un verdadero espacio inclusivo, colaborativo e integrado"

para ellas", asegura Eduvigis Ortiz añadiendo que en ciberseguridad "todos cabemos. Se necesitan todas las miradas". Menciona no sólo la captación de talento a edades jóvenes, sino perfiles que quieran reciclarse, que quieran "cambiar de tercio", porque el de la ciberseguridad es un sector "con muchísimas oportunidades, con paro cero y que tiene mucho interés".

¿Crees que hay un verdadero interés por las empresas del sector por dar valor a la mujer? "Yo creo que sí", responde Eduvigis Ortiz. A pesar de que hay quien sólo busca hacerse la foto, asegura esta experta que "hay gente que lo cree y que está poniendo medidas para tener más mujeres incorporadas, aunque es cierto que tenemos un problema de cantera". Sobre esto último asegura que hay que hacer el camino, se tiene que trabajar con las niñas, con las adolescentes, con la gente que se quiere reciclar. Eso sí, insiste en que "hay una voluntad real de que esto cambie, de que haya más diversidad". it

Compartir en RRSS

Todo lo que necesita para asegurar su nube.

Simplifique su seguridad en la nube con Trend Micro Cloud One™, la plataforma de servicios de seguridad para desarrolladores líder en el mundo.

Cloud One™ Cloud Security simplificada

La infraestructura global evoluciona con el tiempo pero Trend Micro va por delante optimizando la protección. Creado con datos reales por el artista **Andy Gilmore**

Descubra Cloud One en este video:

Conozca más en www.trendmicro.es

TREND MICRO™

‘EDR y Threat Hunting son metas a las que hay que llegar, pero hay muchas cosas antes que eso’

(Jorge Arrufat, BBVA Next Technologies)

En esta era muticloud ya no vale instalar la solución y darle a un botón, dice Jorge Arrufat, Head of Security en BBVA Next Technologies. Asegura también que lo que ha cambiado es la forma de operar, que no hay un Zero Trust para todos, que las arquitecturas cloud y los datos, así como la seguridad de ambos, serán foco de inversión este año y que el análisis de comportamiento será crucial en un futuro.

Hace más de tres años BBVA pisaba el acelerador en su proceso de transformación digital con el lanzamiento de BBVA Next Technologies, una compañía con más de 1.200 expertos en tecnología, presencia en España y México, y fruto de la unión de

dos empresas ya existentes con anterioridad en el Grupo: BEEVA, especializada en cloud computing y big data, e I4S, dedicada a la ciberseguridad.

Como nos cuenta Jorge Arrufat, Head of Security en BBVA Next Technologies, la compañía nació con la misión de apoyar al Grupo BBVA en toda la transformación digital, siempre enfocados en plataformas Next Gen.

"Trabajamos con un enfoque de crear stacks de seguridad que protejan todas estas tecnologías nextgen dentro del banco, siempre con modelos de DevSecOps, intentando integrar estrategias o filosofías de Zero Trust y acompañando al banco en modelos de negocio que puedan surgir y que requieran, por ejemplo, de estrategias passwordless que habiliten autenticación limitando sus mecanismos tradicionales de contraseñas", dice Arrufat, explicando que las estrategias nextgen a las que hace referencia son aquellas que se contraponen al legacy y apoyadas en el cloud.

La experiencia adquirida en BBVA, y lo que se intenta trasladar a los clientes externos es que "aquí no hay café para todos; no todas las nubes, ni todas las soluciones, valen para todo el mundo", dice el directivo. La experiencia, explica, es que en un entorno tradicional la configuración de una solución integrada apenas varía, pero cuando hablamos del cloud, sea una nube privada o pública, "ya no vale instalar la solución y darle a un botón". En estos casos, asegura el responsable de seguridad de BBVA Next Technologies, hay que tener en cuenta que cada negociado es distinto, con unas problemáticas distintas y unos servicios que explotan en estas nubes y que tienen que ser protegidos de diferentes maneras; "lo bueno, desde mi punto de vista, es que los proveedores cloud ya proporcionan muchas tecnologías de seguridad embebidas".

"El doble factor de autenticación robustece mucho la seguridad y minimiza considerablemente los riesgos que nos puedan venir de fuera cara a comprometer la identidad de clientes y empleados"

En todo caso, reflexiona Jorge Arrufat que no se trata de contratar los cuatro servicios cloud que necesitas y ya está, sino que "hay que saber construir o diseñar esa arquitectura para que la seguridad tenga coherencia". Añade que el peligro de la nube

es la pérdida de control; ya que la escalabilidad de los entornos cloud es muy alta y crece muchísimo, “es muy importante que nazca todo con una coherencia”. “Cuando nosotros hablamos de crear un stack tecnológico de seguridad, precisamente lo que intentamos es centralizar y homogeneizar esa seguridad en todos aquellos despliegues o arquitecturas que vayamos a construir en la nube, ya sea protección de identidad, protección del tráfico de red, etc.”, asegura Arrufat.

Al igual que hace unos años, hoy en día se deben tener conocimientos tecnológicos, “lo que cambia es la forma de operar”. Dice Arrufat que ya no sirven los modelos tradicionales de operación de la gestión de inteligencia de amenazas o vulnerabilidades, y que a pesar de que el perímetro se haya difuminado, hay que ser capaces de procesar toda la información, una información que ya no sólo está en el CPD, sino en los usuarios y en sus casas, en dispositivos IoT, “ya hay que saber centralizar eso y explotarlo porque la cantidad de

datos es mucho mayor y se puede extraer información muy útil".

A la hora de explotar la información menciona el directivo que si bien el machine learning facilita el trabajar con toda la información, "el talento también es básico y necesitas contar con gente" que tenga el conocimiento para operar "porque la tecnología por sí no lo resuelve todo".

La tecnología está para ayudarnos y tenemos que saber utilizarla para automatizar porque el método tradicional de operación ya no vale. Dice también el responsable de ciberseguridad de BBVA Next Technologies que tenemos que utilizar la tecnología para poder centralizar, pero que eso no significa que vaya a poder sustituir a las personas. "El talento es clave aquí y a los especialistas tienes que dejarles dedicar su tiempo en trabajar en ese negociado y no en tareas que deberían habilitarnos estas nuevas tecnologías, como puede ser que les dé la información de una forma más coherente, más normalizada. En España, además, hay un talento increíble", asegura Arrufat.

"Aquí no hay café para todos; no todas las nubes, ni todas las soluciones, valen para todo el mundo"

BBVA Next Technologies. Clientes y demandas

El grueso del negocio de BBVA Technologies está en el propio banco. Ese know-how se exporta y se trabaja con clientes externos "que también nos ayudan un poco a ver distintos retos y aprender de ellos". En cuanto a la tipología, "se trabaja sobre todo con clientes que ya están en fases avanzadas de esa transformación digital, que ya trabajan con plataformas nextgen o plataformas cloud. Les ayudamos a la hora de diseñar y construir la parte de automatización y mejorar las arquitecturas existentes evaluando la seguridad y construyendo aquella piezas que permitan robustecer toda la plataforma".

Se trabaja también con startups que, aunque no sean muy maduras, no necesiten tener una altísima complejidad tecnológica, pero ya nacen en un mundo nuevo. También hay un grupo de clientes que se encuentran en el proceso de transformación digital y con los que trabajamos sobre todo en plataformas

"El talento es básico y necesitas contar con gente porque la tecnología por sí no lo resuelve todo"

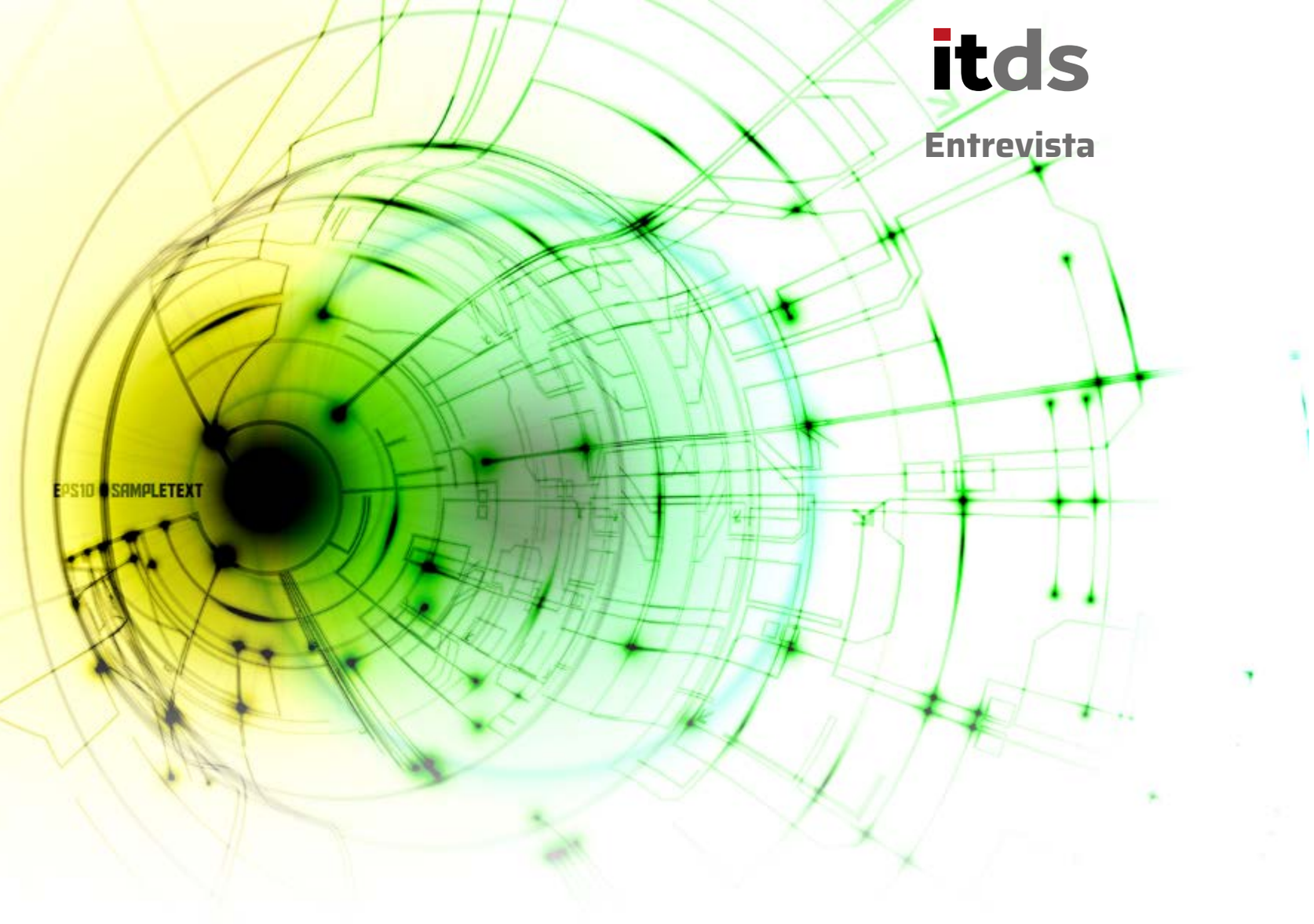
de datos y automatización con machine learning, inteligencia artificial, etc.

Si hablamos de seguridad, cuando la empresa está más avanzada se le ayuda "a construir esa coherencia de seguridad con stacks personalizados, en las configuraciones que son distintas dependiendo de si es nube privada o híbrida". Además, desde el área de innovación de seguridad se ayuda en la protección de los modelos de machine learning. "Al final siempre vamos con el pack. No se trata de construir una plataforma y la seguridad la dejamos de lado porque tiene que estar desde el principio y hay que darle una coherencia", asegura el directivo.

¿Qué es lo que os demandan los clientes? Algunos llegan con criterios de seguridad propios, explica Arrufat añadiendo que algunas empresas, por regulaciones y normativas saben que se tienen que proteger algunas cosas, que un dato tiene que estar anonimizado o cifrado. "También nos piden temas relacionados con DevSecOps como filosofía y los flujos de trabajo que lo habiliten; integración continua, testing, gestión de vulnerabilidades, etc.", añade el directivo, dejando para el final la demanda de arquitecturas Zero Trust, que Arrufat ve "como una filosofía que ayuda a ver el end to end del problema que tenemos y cómo atajarlo".

Asegura el Head of Security en BBVA Next Technologies que Zero Trust es muy amplio, que habla de identidades, de la protección del endpoint, de la seguridad en redes… de cómo no confiar en nada partiendo de que todo puede ser una amenaza o un riesgo; "no existe un Zero Trust para todos porque dependerá muchísimo del negocio, de las tecnologías de redes que tengas, dónde estás, a qué te dedicas, dónde están tus usuarios, tus clientes o tus sistemas… Pero la filosofía es la que nos ayuda a definir un modelo de seguridad bastante sólido".

Sobre cuán avanzadas están las empresas españolas en lo que a adopción de tecnologías de seguridad se refiere, menciona Arrufat que EDR y Threat Hunting "son metas a las que hay que llegar", pero que no todas las empresas están en disposición de poder implantarlo "porque hay muchas cosas antes que eso". Explica que antes de tener Threat Hunting debes tener una estrategia de Threat Intelligence y que se está avanzando mucho en la seguridad de los endpoints, potenciado por el teletrabajo o el BYOD, pero que por encima de todo esto, hay algo que no es tecnológico, sino cultural, y que es la concienciación; "la concienciación es la primera capa, en este caso invisible, de la seguridad".



Seguridad en 2021

La pandemia sanitaria, por cierto, ha potenciado la concienciación de la ciberseguridad. La situación, reconoce Arrufat ha cambiado mucho en los últimos años, igual que las amenazas. La pandemia, además, ha tenido cierto impacto en las inversiones tecnológicas de 2021; arquitecturas cloud y datos, así como la seguridad que ambas conllevan serán foco este año, según el responsable de seguridad de BBVA Next Technologies.

Como tecnologías que Jorge Arrufat cree que serán imprescindibles en los próximos años menciona el directivo varias. “Todo lo que sea la identidad y comportamiento, no sólo del usuario, completa muy bien el ciclo de Threat Intelligence, y en conjunto nos da una visión muy sólida de hacia dónde debería ir la seguridad, donde yo invertiría mucho”, asegura el directivo, mencionando además las tecnologías biométricas como opción de doble factor de autenticación porque “robustece mucho la seguridad y minimiza considerablemente los riesgos que nos puedan venir de fuera cara a comprometer la identidad de clientes y empleados”.

Enlaces de interés...

- ‘El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad’ (Elena García, Indra)
- ‘En seguridad la heterogeneidad es compleja de gestionar, y sobre todo de financiar’ (Jesús Alonso Murillo, Ferrovial Servicios)
- ‘Los CISO somos ciberresilientes desde hace mucho tiempo’ (Javier Sánchez Salas - HAYA Real Estate)

Compartir en RRSS

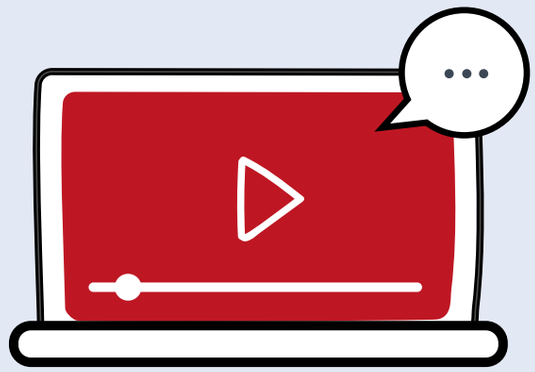
Aplicaciones,
¿cómo desarrollo y entrego mi mejor software?

Porque las aplicaciones son hoy -más que nunca- la cara del negocio y estamos en la era del DevSecOps... ¿cómo creo mi mejor software y lo pongo a disposición de mis usuarios? Únete a esta sesión online y conoce las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlas en producción. ¡Reserva ahora tu sitio!

REGISTRO

Ya vivo en la nube, ¿y ahora qué?
Mejores prácticas para desenvolverse en entornos híbridos

Los entornos de TI multicloud e híbridos se están convirtiendo en el modelo hacia el que se dirigen las arquitecturas de TI actuales. Gestionar estas infraestructuras cloud, controlar sus costes, desarrollar nuevos servicios nativos en cloud, asegurar la disponibilidad del negocio basado en la nube, garantizar el cumplimiento normativo y proteger los activos que residen en la cloud, son cuestiones que todo responsable de TI debe tener bajo control. ¡Regístrate ahora!



#ITWEBINARS

Kaspersky Optimum y Kaspersky Expert:

dos familias, dos necesidades, la misma seguridad

kaspersky

Kaspersky Optimum y Kaspersky Expert:

dos familias, dos necesidades, la misma seguridad

El malware como servicio, o los kits de herramientas para la creación de amenazas, al alcance de cualquiera, han hecho que lanzar un ciberataque sea relativamente fácil y económico, convirtiendo a cualquier empresa en un posible objetivo para los ciberdelincuentes, no sólo en sí misma, sino como parte de una cadena de suministro que le permita llegar al pez grande. Las familias de soluciones Optimum y Expert en las que Kaspersky ha reorganizado su oferta se adaptan a los niveles de madurez y recursos en ciberseguridad de las organizaciones.

Si hasta ahora una solución de protección endpoint tradicional era suficiente para mantener las empresas a salvo, en el momento en que todas, incluidas las más pequeñas, se convierten en objetivo de los ciberdelincuentes, se necesita una estrategia más seria y herramientas algo más avanzadas. El reto reside en que muchas empresas medianas carecen del conocimiento e inteligencia sobre las amenazas y sus recursos son limitados. La respuesta de Kaspersky ha sido ampliar sus soluciones corporativas con un nuevo enfoque estratégico para adaptarse a las necesidades tanto técnicas como presupuestarias de las empresa.

Para Alfonso Ramírez, director de Kaspersky Iberia, 2020 ha sido un año complicado, y *"apasionante para la ciberseguridad"*. En apenas unos meses

KASPERSKY INTEGRATED ENDPOINT SECURITY

CLICAR PARA VER EL VÍDEO

El portfolio Expert está dirigido a empresas que cuentan con un nivel alto de madurez en seguridad TI o incluso con un equipo dedicado a la seguridad de la información.

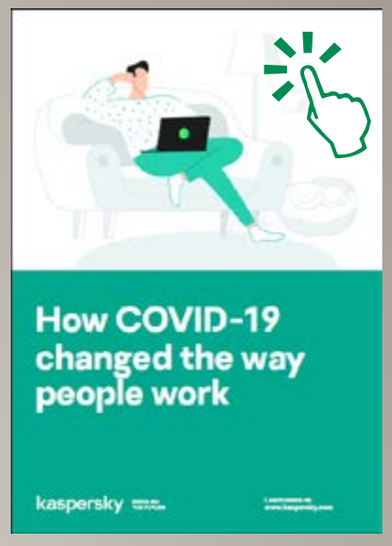
ha cambiado la manera de trabajar, se ha visto el esfuerzo de las empresas por mantener la continuidad de sus negocios, *"pero cometieron el mismo error: no priorizaron la seguridad"*. Asegura el directivo que en la primera oleada de la pandemia no se vio algo realmente transgresor en lo que se refiere a los ataques, pero los ciberdelincuentes se han preparado para esta segunda oleada, *"y las amenazas son las mismas seas una empresa grande u otra más pequeña"*. La estrategia de Kaspersky ha sido ampliar sus soluciones corporativas para adaptarse a las necesidades tanto técnicas como presupuestarias de las empresas. El resultado son dos entornos de desarrollo: Expert y Optimum con los que Kaspersky busca alinear la conceptualización y desarrollo de los productos y servicios de seguridad empresarial con las necesidades concretas de las empresas, en función de su madurez y recursos en seguridad de TI.

La realidad es que el panorama de la tecnología y la ciberseguridad está cambiando rápidamente y, se ha vuelto más complejo. Durante 2019, el 91% de las organizaciones de todo el mundo se vio afectado por ciberataques, y uno de cada diez se enfrentó a un ataque dirigido. Y mientras el 40% de las empresas y compañías medianas carecen del conocimiento e inteligencia sobre las amenazas a las que se enfrenta su organización, el coste de una brecha de datos en una pyme europea asciende a unos 89.000 dólares, según datos de Kaspersky.

Con el fin de ayudar a las empresas a luchar contra las ciberamenazas complejas y en constante evolución, y adaptarse a sus necesidades espe-

¿CÓMO HA CAMBIADO COVID-19 LA MANERA DE TRABAJAR DE LA GENTE?

La pandemia de coronavirus ha provocado cambios repentinos y radicales en todo el mundo. Este informe analiza cómo las personas afrontan el día a día fuera de la oficina, las formas en que sus relaciones familiares están cambiando, las dificultades que pueden tener mientras trabajan de forma remota y la importancia de permanecer seguros online cuando realizan sus funciones desde casa todos los días.



cíficas desde el punto de vista tanto técnico como presupuestario, Kaspersky desarrolla un nuevo enfoque estratégico basado en tres pilares: las expectativas del mercado –lo que demandan las empresas en cuanto a tecnología; el nivel de madurez de las estrategias de seguridad de la información de cada organización; así como sus recursos técnicos, financieros y de personal.

Bajo esta premisa, la compañía ha reorganizado sus soluciones en dos nuevas familias: Optimum, enfocada a clientes con un nivel bajo o medio de madurez y presupuestos limitados en seguridad de TI, y Expert, dirigida a aquellas compañías con conocimientos y recursos de ciberseguridad más avanzados y mayor capacidad de inversión en infraestructura.

Familia Optimum

Dentro del entorno Optimum se engloban Kaspersky Endpoint Security for Business, la protección tradicional endpoint de la compañía, Kaspersky Endpoint Detection and Response (EDR Optimum) y Kaspersky Sandbox. Estas dos últimas soluciones son las principales novedades lanzadas este año dentro del portfolio de seguridad empresarial de la compañía.

Añadir capacidades EDR, o de detección avanzada y respuesta, a la protección endpoint, se ha convertido en algo habitual en las grandes empresas. Kaspersky lanzó su primer EDR en 2017 y con Optimum lo que hace es democratizar esta tecnología.

Kaspersky EDR Optimum proporciona capacidades básicas de EDR a organizaciones con recursos y experiencia en ciberseguridad limitados, incluyendo una mejor visibilidad de los endpoints, análisis simplificado de causa raíz y opciones de respuesta automatizadas. El producto, más ligero y fácil de usar, aporta un mayor nivel de automatización, lo que lo convierte en la mejor opción para aquellas compañías que no están preparadas para construir su propio SOC o para incorporar capacidades de respuesta a incidencias a sus equipos. Kaspersky EDR Optimum añade visibilidad a las amenazas detectadas por Kaspersky Endpoint Solutions for Business, además de los antecedentes de toda la actividad maliciosa, estableciendo la ruta de propagación del incidente detectado y el análisis de su causa.

Para remediar la amenaza, Kaspersky EDR Optimum introduce un amplio conjunto de capacidades de respuesta, como puede ser el aislar un

Kaspersky Managed Detection and Response (MDR) es un servicio gestionado de detección y respuesta ante incidencias, con funciones de y servicios de alerta temprana

endpoint con malware potencial, o poner en cuarentena un archivo sospechoso.

En cuanto a Kaspersky Sandbox, se trata de una herramienta avanzada para analizar objetos sospechosos en un ambiente aislado, lo que permite bloquear automáticamente amenazas avanzadas, desconocidas y complejas sin la necesidad de recursos adicionales. El veredicto de Kaspersky Sandbox puede enriquecerse aún más con el análisis del archivo realizado por Kaspersky EDR Optimum. Además, con su emulación dinámica de amenazas, Kaspersky Sandbox puede incluso detonar malware diseñado para eludir la protección de endpoints y evadir la detección de sandbox, y realizar un análisis de comportamiento más profundo, algo que no debe realizarse a nivel de endpoint porque afectaría la productividad. El resultado es que es capaz de detectar las amenazas avanzadas y evasivas más peligrosas.

Familia Expert

El portfolio Expert está dirigido a empresas que cuentan con un nivel alto de madurez en seguridad TI o incluso con un equipo dedicado a la seguridad de la información. Bajo este entorno la compañía engloba soluciones de gama más alta como la plataforma Kaspersky AntiTargeted Attack, y Kaspersky EDR Expert.

Con la plataforma Kaspersky AntiTargeted Attack, Kaspersky proporciona un enfoque integrado para los ataques dirigidos y la detección de amenazas. La solución ofrece un enfoque estratégico para la detec-

ción e investigación de ataques complejos en su fase inicial a nivel de red. Se complementa con tecnologías y soluciones de prevención multicapa, así como con un amplio portfolio de servicios de inteligencia de seguridad para la respuesta y predicción.

Por su parte, Kaspersky EDR Expert se dirige a aquellas empresas que cuentan con recursos internos y desean recibir capacidades avanzadas de EDR, incluyendo remediación de amenazas, análisis retrospectivo, capacidades de investigación profunda y caza proactiva de amenazas. La solución proporciona una sólida defensa de los endpoints y la red frente a amenazas complejas. Además, puede trabajar junto con plataformas EPP de terceros.

Nuevo servicio Kaspersky Managed Detection and Response

El portfolio de soluciones de seguridad empresarial se complementa con diferentes servicios. Entre las principales novedades destaca Kaspersky Managed Detection and Response (MDR), otra de las novedades lanzadas este año por la compañía. Se trata de un nuevo servicio gestionado que proporciona servicios de alerta temprana y de respuesta a aquellas organizaciones que no dispongan de un equipo dedicado de ciberseguridad.

Cuenta, asimismo, con los niveles Optimum y Expert para adaptarse a las necesidades de las organizaciones según su nivel de madurez en seguridad informática. Kaspersky MDR Optimum aumenta instantáneamente la capacidad de ciberseguridad sin necesidad de invertir en personal adicional y proporciona resistencia a los ataques evasivos a través de su rápido despliegue. Kaspersky MDR Expert incluye todas las características de Optimum, además de proporcionar una amplia funcionalidad y flexibilidad para los equipos de seguridad informática maduros, permitiéndoles que la solución de Kaspersky se encargue del triaje y la investigación de los incidentes mientras dedican sus recursos a actuar frente a lo que vaya ocurriendo.

Enlaces de interés...

- Kaspersky Integrated Endpoint Security
- Una defensa sencilla contra ataques complejos

EDR Optimum ofrece capacidades EDR esenciales a una audiencia más amplia, a empresas que no están preparadas para construir su propio SOC o contratar a un equipo de respuesta a incidentes

PEDRO GARCÍA-VILLACAÑAS

HEAD OF PRESALES, IBERIA, KASPERSKY

La tecnología EDR protege las redes corporativas frente a ataques dirigidos

El panorama de las ciberamenazas dirigidas a empresas ha experimentado cambios dramáticos en los últimos años, debido a nuevas amenazas previamente desconocidas, ataques sin archivo (file-less), ransomware o criptomineros.

Febrero 2021

Compartir en RRSS

Ninguna empresa es demasiado pequeña para ser atacada, pero a menudo, las compañías no saben a qué amenazas están expuestas, y sus recursos y conocimientos de ciberseguridad suelen ser muy limitados, lo que les dificulta hacer frente a amenazas complejas.

Proteger solo el endpoint no es suficiente

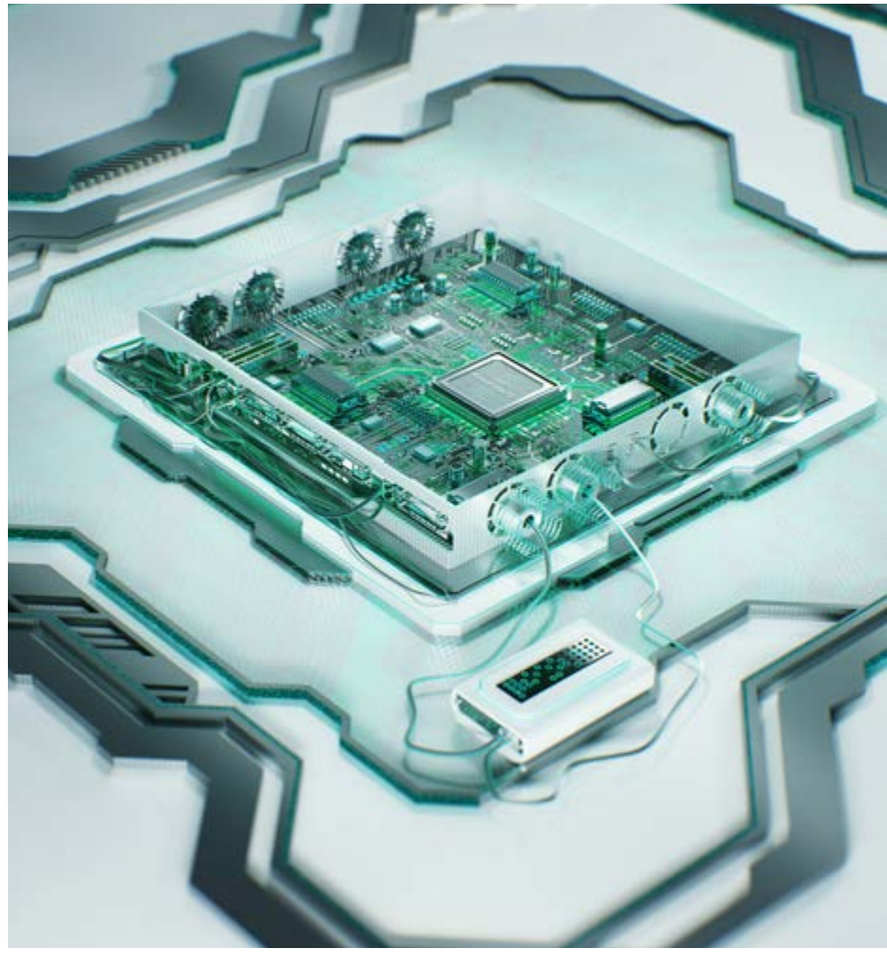
Un software de seguridad corporativo debe proporcionar una protección completa para todas las estaciones de trabajo y servidores, pero también debe ser fácil de usar. Por su parte, los ciberdelincuentes han sido capaces de burlar fácilmente la detección basada en firmas y los análisis de binarios, así como modificar los hashes y cifrar cadenas de caracteres. Además, utilizan cada vez más programas maliciosos que se ejecutan en memoria y que no dejan rastros en el disco duro, con lo que pueden pasar desapercibidos para las soluciones de seguridad tradicionales. Por todo ello, no basta con bloquear *"sólo"* las amenazas en el endpoint. Las empresas necesitan herramientas que les permitan detectar y responder a las amenazas más recientes y sofisticadas.

EDR como complemento para una protección proactiva

La tecnología EDR (Endpoint Detection and Response) responde a la necesidad de vigilancia en tiempo real, con foco en el análisis y la respuesta a incidentes en el endpoint. EDR proporciona una visibilidad completa de la actividad de cada endpoint en la infraestructura gestionada desde una única consola central, junto con valiosas fuentes de inteligencia que los profesionales de la seguridad TI pueden utilizar para mejorar la investigación y respuesta. EDR está diseñado para detectar de forma proactiva las amenazas nuevas y desconocidas y las infecciones no identificadas que se infiltran en las organizaciones a través de las estaciones de trabajo y los servidores.

Además, puede utilizarse para detectar malware desconocido en ataques de día cero y APT utilizando tecnologías de detección avanzadas como las reglas YARA, sandboxing, escaneo de indicadores de compromiso o análisis retrospectivo con correlación de eventos basado en el aprendizaje automático dinámico.

La solución de protección para el endpoint (EPP) y el EDR deben trabajar conjuntamente para garantizar una protección fiable y eficaz contra las amenazas sofisticadas. Por ejemplo, una solución EDR notifica el descubrimiento de cualquier archivo sospechoso que se identifique y que no pueda clasificarse definitivamente como malicioso, y lo envía al sandbox. Esta herramienta detona el archivo sospechoso en un entorno aislado y analiza su actividad en busca de posibles amenazas. Esto permite



Un software de seguridad corporativo debe proporcionar una protección completa para todas las estaciones de trabajo y servidores, pero también debe ser fácil de usar

EDR en modo de servicio de seguridad gestionado supone una importante oportunidad, especialmente para las empresas con nivel de madurez bajo-medio en ciberseguridad

determinar si hay indicios de una posible intrusión o de actividades no autorizadas de empleados o socios.

Las firmas, reglas y restricciones solían ser suficientes para contrarrestar esos ataques. Sin embargo, estas medidas a menudo ya no son suficientes en una época de ataques selectivos y de múltiples niveles. Más de una cuarta parte (28%) de las empresas que han implementado una solución EDR han sido capaces de detectar ciberataques en tan sólo unas horas o casi inmediatamente después de que ocurriera un incidente.

El futuro: Detección y respuesta automática

De cara al futuro, la implantación de EDR dependerá en gran medida de los proveedores y de su capacidad para automatizar el análisis, la valoración y la respuesta, así como para reproducirlo sin intervención humana. EDR en modo de servicio de seguridad gestionado supone una importante oportunidad, especialmente para las empresas con nivel de madurez bajo-medio en ciberseguridad, que suelen carecer de especialistas en esta área.

La seguridad de los endpoint se puede subcontratar a proveedores de servicios especialistas en seguridad, lo que permite al departamento TI interno centrar sus recursos en las competencias básicas sin comprometer la seguridad de la empresa. Por supuesto, esto también mejora la ciberseguridad de la empresa. Cuanto mejor sea la protección, los especialistas dispondrán de más tiempo y recursos para para hacer frente a los ataques.

it User
TECH & BUSINESS

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

Junto a modelos como Zero trust o tecnologías como Threat Hunting, el NDR (Network Detection and Response) es una de las claras tendencias de los últimos años, incluída la lista de lo debemos tener muy presente este 2021.

NDR, la detección y respuesta llegan a la red

Las redes son cada vez más complejas y distribuidas y por eso la visibilidad, antes importante, ahora es imperativa para poder detectar y detener las amenazas antes de que generen una brecha de seguridad. Aquí es donde entra en juego la detección o respuesta de red, o NDR (Network Detection and Response), una categoría de producto que tiene su origen en la detección de intrusiones en la red, la búsqueda de amenazas basada en la red y la investigación de incidentes.

Network Detection and Response permite a las organizaciones monitorizar el tráfico de red en busca de actores maliciosos y comportamiento sospechoso, y reaccionar y responder a la detección de amenazas. La clave está en la capacidad de respuesta. Igual que las herramientas de seguridad endpoint evolucionaron hacia los EDR, las herramientas tradicionales de la monitorización de la red evolucionan hacia los NDR.

Según Gartner, las herramientas de NDR están ayudando a las empresas a detectar mejor el tráfico de red sospechoso en comparación con las herramientas más tradicionales. Gran parte de la tecnología que hay detrás de la mayoría de las plataformas NDR se puede rastrear hasta el análisis del tráfico de red y hasta las plataformas de IA para operaciones de TI (AIOps). Estas herramientas se centran en el rendimiento de la red mediante la recopilación de datos que se analizan para identificar problemas de rendimiento de red difíciles de encontrar, como sobreutilización, fallos intermitentes de hardware o

NDR vs NTA (Network Traffic Analysis)

Explican los expertos que gran parte de la confusión que rodea a NDR tiene que ver con su relación con el análisis de tráfico de red (NTA). Gartner definió el Análisis de tráfico de red (NTA) como una categoría de producto de seguridad que utiliza las comunicaciones de red como la fuente de datos principal para la detección e investigación de amenazas dentro de una red. No se habla aquí de respuesta.

NDR se basa en la supervisión y el análisis en tiempo real que NTA proporciona con capacidades de respuesta integradas. Las soluciones NDR más completas integran la tecnología de orquestación, automatización y respuesta de seguridad (SOAR) para optimizar y automatizar las opciones de respuesta. Es decir, los productos NDR usan NTA pero agregan metadatos históricos para investigaciones y búsqueda de amenazas y respuesta automatizada.

"Las soluciones basadas en análisis de red y respuesta a incidentes vienen a proporcionar una herramienta capaz de analizar el tráfico que se propaga en nuestra red, sea cual sea el entorno en el que este desplegada"

Alex López, Iberia Sales, Gigamon

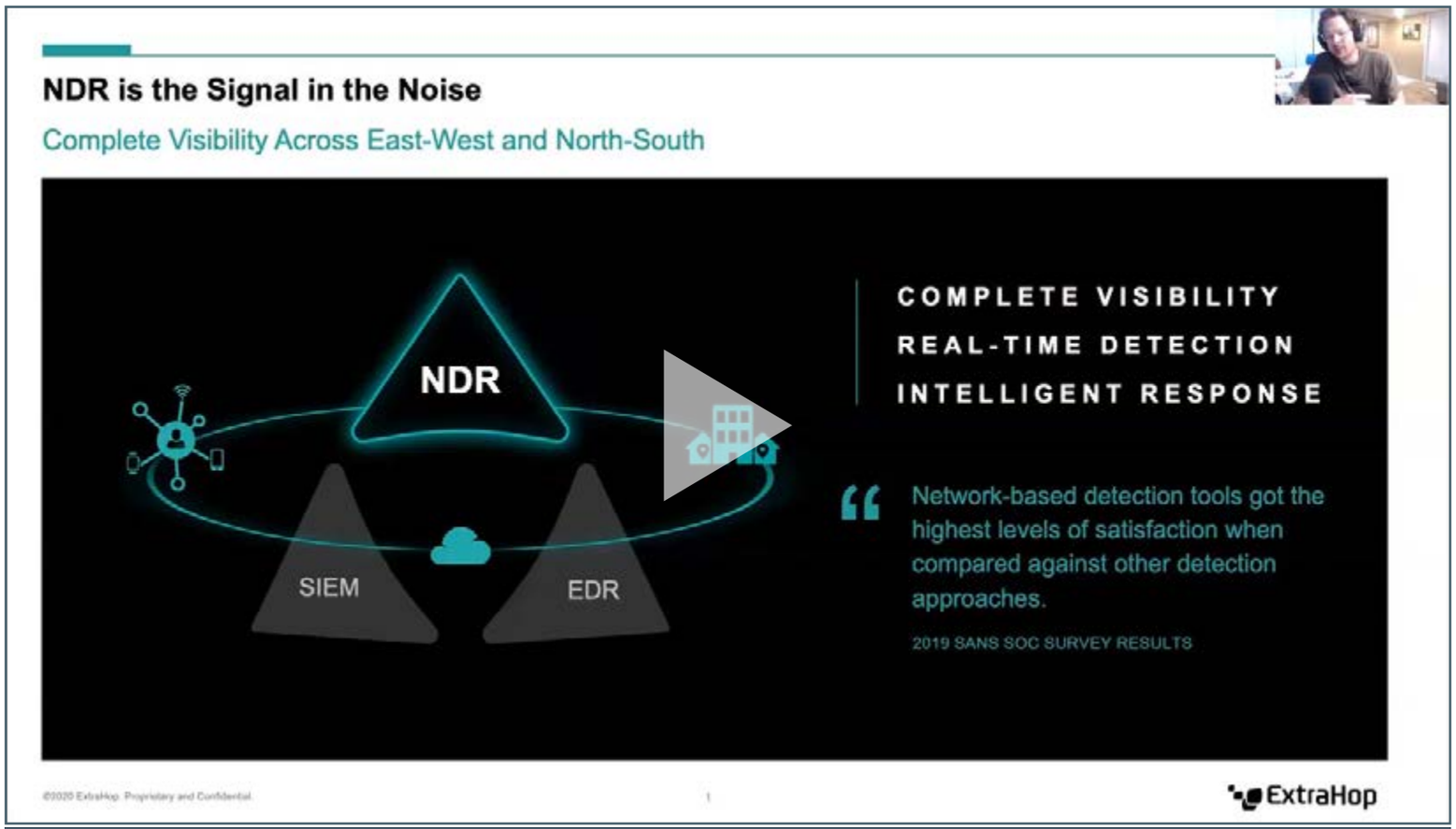
software y configuraciones incorrectas de TI. Una plataforma NDR recopila y establece una línea base de todo el comportamiento de la red, pero en lugar de centrarse en el análisis del rendimiento de la red, el enfoque cambia hacia el análisis de seguridad de la red para identificar comportamientos de tráfico sospechosos.

Añadir que cuando se trata de gestionar las ciberamenazas, el enfoque tradicional se ha centrado en la prevención, pero hoy en día, con un panorama de ataques cada vez más complejos y dirigidos, hay que dar un paso más, ir hacia la detección y la respuesta.

¿Qué viene a solucionar un NDR?

A medida que el malware evoluciona para evadir la detección de las soluciones antivirus tradicionales, los sistemas de prevención de intrusiones, los firewalls y otras soluciones de seguridad de red, se necesita un nuevo tipo de solución de seguridad denominada detección avanzada de amenazas, o Advanced Threat Detection, asegura Christian Buhrow, Sales Director DACH & IBERIA de ExtraHop. Añade que para descubrir estos ataques, este tipo de soluciones avanzadas a menudo incluyen capacidades como sandboxing, análisis de comportamiento, monitorización automatizada y otros mecanismos de detección. “Después del mundo del ‘protect’ se necesita una segunda capa, que es la del ‘detect’ para poder responder”, dice. Los NDR estarían dentro de esta nueva categoría de soluciones.

Explica Alex López, Iberia Sales de Gigamon, que en redes cada vez más deslocalizadas, sin un perímetro definido, y en despliegues cada vez más híbridos on-site & cloud, cada vez es más complejo tener una visión unificada de la exposición de la empresa a las amenazas de seguridad. De forma



NDR IS THE SIGNAL IN THE NOISE — **CLICAR PARA VER EL VÍDEO**

que las soluciones basadas en análisis de red y respuesta a incidentes “vienen a proporcionar una herramienta capaz de analizar el tráfico que se propaga en nuestra red, sea cual sea el entorno en el que esté desplegada”. Añade además que más allá de la tecnología, con la escasez de recursos especializados que hay para administrar la gran cantidad de soluciones de seguridad disponibles en el mercado, “este tipo de soluciones son una oportunidad adicional para simplificar el stack de seguridad cuando se consumen en modo servicio, sin requerir de recursos humanos indisponibles”.

Dice Francisco Verdugo, Senior Partner Solution Engineer de VMware Iberia, que un NDR resuelve ante todo “el problema de ‘visibilidad’ a nivel de red y la automatización de las respuestas ante los eventos o incidentes de seguridad, bien de forma directa o bien a través de un tercero”. VMware juega en el mercado de NDR gracias a la compra el año pasado de Lastline, cuya tecnología se ha añadido a su propuesta NSX; conocida por su investigación anti-malware y su detección y respuesta de red impulsada por inteligencia artificial (AI), el producto principal de Lastline es una sandbox capaz de observar cada instrucción que ejecuta un malware para ver cómo funciona y después bloquear diferentes iteraciones de malware.

¿Por qué deberían las empresas adoptar una solución de NDR?

Todas las empresas que desean visibilidad en entornos locales, remotos y en la nube dentro de una única solución deben considerar NDR. ¿Ya cuenta con un SIEM (gestión de eventos e información de seguridad) y un EDR? Pues lo que recomienda Gartner es añadir el NDR para crear una Triada de visibilidad del SOC capaz de proporcionar un enfoque proactivo para reducir las posibilidades de que un ciberdelincuente permanezca en la su red el tiempo suficiente para obtener lo que busca.

Al igual que su equivalente en el mundo de los endpoints (EDR) un NDR se antoja como una tecnología imprescindible en el mundo de la

Una triada mágica para el SOC de nueva generación

Los equipos encargados de mantener a raya a los ciberatacantes luchan cada día por ganar visibilidad. Con ese fin, Gartner introdujo el concepto SOC Visibility Triad, un trío compuesto por información de seguridad y gestión de eventos (SIEM), detección y respuesta de puntos finales (EDR) y detección y respuesta de red (NDR). Todo ello aderezado con analítica de conducta de entidades y usuarios (UEBA).

El objetivo de esta triada es reducir significativamente la posibilidad de que un atacante pueda evadir todas las defensas de ciberseguridad de una organización. Cada parte de la tríada proporciona capacidades complementarias que ayudan a fortalecer el todo, lo que da como resultado una arquitectura de seguridad que puede detectar más amenazas que las soluciones individuales por sí solas.

Ver amenazas en la red ha ganado importancia a medida que la infraestructura ha evolucionado mucho más allá de los puntos finales dentro de un perímetro bien definido para incluir una combinación diversa de implementaciones de Bring Your Own Device (BYOD), Internet de las cosas (IoT) y la nube pública.

¿Por qué NDR es más eficaz en conjunto con las soluciones SIEM y EDR? El análisis forense de redes es uno de los análisis de seguridad más difíciles de completar debido a la gran cantidad de datos que los analistas deben analizar, todo mientras se evitan numerosos falsos positivos y dificultades con la investigación de paquetes. EDR y SIEM ayudan a refinar NDR en situaciones en las que la visibilidad de la red es una preocupación, como en el caso de las conexiones de red cifradas de un extremo a otro. Las amenazas rara vez se observan solo desde la red; es necesario conectar las piezas.

"Es fundamental saber lo que pasa en la red, detectar las amenazas conocidas y desconocidas así como responder en tiempo y forma"

Francisco Verdugo, Senior Partner Solution Engineer de VMware Iberia

seguridad actual, explica Francisco Verdugo; “Es fundamental saber lo que pasa en la red, detectar las amenazas conocidas y desconocidas, así como responder en tiempo y forma”, asegura el directivo de VMware.

Para Christian Buhrow la necesidad de adoptar una solución de detección o respuesta de red viene determinada porque te da una enorme visibilidad de lo que ocurre dentro de la red; “las empresas saben quién está hablando, pero no qué están hablando, y esta es la parte de visibilidad que les falta hoy en día a las empresas”.

Para Alex López, los NDR son una muy buena alternativa en el campo de seguridad “cuando se tiene una red dispersa con numerosos puntos de entrada de ataques tanto físicos como virtuales, o cuando se busca una solución en modo servicio gestionado para el control de tráfico de red. La capacidad de retención de datos de la plataforma combinada con las nuevas técnicas de ML/IA

THE ADVENT OF NETWORK DETECTION AND RESPONSE IN SECURITY OPERATIONS

CLICAR PARA VER EL VÍDEO

aplicadas en seguridad dan una muy buena respuesta a la protección de los activos de IT".

La capacidad de análisis y visibilidad que ofrece un NDR es extremadamente atractiva porque las amenazas emergentes están diseñadas para evadir las herramientas de seguridad que se utilizan tradicionalmente para identificar comportamientos sospechosos que indican un compromiso o una violación de la infraestructura. Como hemos comentado, estas herramientas van desde un firewall a un EDR, a sistemas de IPS y SIEM que centralizan la visibilidad de la seguridad. Los ciberdelincuentes buscan la manera de eludir tanto el EDR como el sistema de registro, y si consiguen entrar tienen mucha flexibilidad porque ya que la mayoría de las herramientas de seguridad se enfocan en amenazas externas en lugar de internas.

Dicen los expertos que no es probable que los atacantes tengan idea de que un NDR está observando sus actividades, ya que este tipo de análisis y monitorización de seguridad de red es completamente pasivo, por lo que es probable que no busquen eludirlo. Además, el hecho de que NDR monitorice todo el tráfico, hace que sea más probable que los dispositivos internos comprometidos se detecten poco después de que cambie el comportamiento del tráfico de la red.

NDR, un imprescindible en el mundo IoT

NDR parece condenada a convertirse en la solución ideal si se trabaja en un entorno con dispositivos de Internet de las cosas (IoT) y tecnología operativa (OT) o sistemas de control industrial (ICS), donde es complicado, y a veces imposible, instalar agentes para la detección basada en puntos finales. Por ejemplo, las organizaciones con sistemas de control de supervisión y adquisición de datos (SCADA) pueden usar NDR para monitorizar e inspeccionar el flujo de tráfico entre dispositivos y alertar sobre protocolos que rara vez se ven.

El IoT se extiende, imparable; está en camino de hacer que nuestros hogares, edificios comerciales, lugares de trabajo y sistemas de transporte o sanitarios sean mucho más inteligentes y autónomos de lo que son hoy, y aunque son encomiables los esfuerzos de la industria e incluso de los reguladores para incentivar la seguridad del Internet de las Cosas, se avanza de forma lenta.

No se puede esperar mucho de los fabricantes de dispositivos IoT. Las prisas por llegar al mercado llevan a dejar de lado la seguridad por diseño y eso hace que sea habitual que estos dispositivos

NDR vs XDR

La pasión por la siglas a veces lleva el mercado al límite. Lo que parece claro es que la DR de Detección y Respuesta, gana cada vez más adeptos.

Extended Detection and Response (XDR) es una tecnología de seguridad que proporciona mayor visibilidad, análisis y respuesta en redes y nubes, además de aplicaciones y puntos finales, explican desde VMware, que además añade que XDR es una progresión más sofisticada y avanzada de seguridad de detección y respuesta de endpoints (EDR). Donde EDR contiene y elimina amenazas en terminales y cargas de trabajo, XDR extiende esas capacidades más allá del terminal a múltiples puntos de control de seguridad (incluyendo correo electrónico, redes, servidor y nube) para detectar amenazas más rápidamente utilizando datos recopilados en todos los dominios.

¿Cuáles son las similitudes y diferencias entre NDR y XDR? Dice ExtraHop que NDR y XDR comparten el mismo objetivo: ayudar a los clientes a detectar amenazas y responder a ellas. La diferencia fundamental radica en la fuente de datos, el enfoque analítico y los requisitos necesarios para beneficiarse de esas diferentes fuentes de datos.

aterricen con contraseñas predeterminadas que no se pueden cambiar o configuraciones que transmiten contraseñas en texto sin cifrar. Hoy en día, millones de dispositivos de IoT son vulnerables desde el primer momento. E incluso los dispositivos que son relativamente seguros y listos para usar, con el tiempo, probablemente no se actualizarán a medida que se descubran nuevas vulnerabilidades.

Del lado de las empresas, se lucha con una superficie de amenazas cada vez mayor, una gran escasez de profesionales y en muchas ocasiones con presupuestos reducidos.

Para Sri Sundaralingam, vicepresidente de soluciones cloud y seguridad de ExtraHop, "lo único que es muy posible hacer hoy es monitorizar los paquetes de red que emanan de los dispositivos de IoT". Explica que NDR implica la aplicación de aprendizaje automático, análisis de datos avanzados y detección basada en reglas para el seguimiento de paquetes, y que la tecnología de ExtraHop está diseñada para escrutar y analizar continuamente los paquetes que circulan dentro de la red de una organización, desde todos los rincones de la red. Explica el directivo que se pueden "extraer metadatos enriquecidos del tráfico de red que estamos monitorizando. Podemos ejecutar nuestro aprendizaje automático y modelos de comportamiento en los paquetes para buscar anomalías o comportamientos sospechosos. Ayudamos a los analistas de seguridad a comprender el radio de explosión y a tomar medidas correctivas para ayudar a contenerlo".

"Entre un SIEM, un EDR y un NDR, cubres 360 grados de tu infraestructura y tienes una visibilidad completa"

Christian Buhrow,
Sales Director DACH + IBERIA, ExtraHop

Factores a tener en cuenta para adoptar una adecuada solución de NDR

Tiene claro Alex López que en aquellas soluciones que el cliente va a operar por sí mismo “es fundamental tener en cuenta la superficie sobre la que se va a tener visibilidad, que debe ir más allá de la red física y entrar en el tráfico este-oeste de la red virtual; la metodología de reconocimiento de ataques, que debe ir más allá de las firmas y reglas y entrar en técnicas más novedosas basadas en IA/ML; y las posibilidades de integración con terceros productos para automatizar la respuesta a incidentes”.

Sin olvidarse de tener en cuenta el precio competitivo, añade el Iberia Sales de Gigamon que en las propuestas basadas en servicios gestionados, se deben negociar bien los SLAs que se van a ofrecer basados en los KPIs antes descritos, y que otro parámetro fundamental tiene que ver con “la tecnología de captura de tráfico, ya que las soluciones basadas en SPAN/Mirror pierden visibilidad de tráfico, mientras que las basadas en TAP/NPB nos darán una visión más real de las potenciales amenazas en la red”.

Además de tener en cuenta las redes que se pretenden monitorizar, como son todas aquellas en las que haya cargas críticas a nivel de negocio (tanto on-premise como en cloud)., dice Francisco Verdugo que se debe tener en cuenta “la facilidad de integración con otros elementos de seguridad (como SOARs o SIEMs). Por último, debe ir acompañado de otras tecnologías como IDPS, Sandboxing, NTA

La capacidad de análisis y visibilidad que ofrece un NDR es extremadamente atractiva

o inteligencia de amenazas globales en tiempo real”.

Christian Buhrow prefiere centrarse en la cooperación entre el departamento de seguridad y el de redes “porque tienes que encontrar los puntos de tu red donde sacar el tráfico”. Explica el directivo de ExtraHop que NDR funciona con una copia del tráfico y es muy importante encontrar los puntos donde se tiene un tráfico interesante, “y eso requiere una coordinación entre seguridad y el departamento de sistemas y redes que no en todas las empresas existe”.

A la hora de seleccionar una solución NDR para el negocio también deben tenerse en cuenta los datos a analizar; a este respecto se recomienda buscar soluciones capaces de analizar todo el paquete y no sólo las alertas porque proporciona mucha más profundidad y permite que se identifiquen amenazas más relevantes. Por otra parte, también se recomienda consolidar, por lo que los NDR deberían

"NDR parece condenada a convertirse en la solución ideal si se trabaja en un entorno con dispositivos de Internet de las cosas (IoT) y tecnología operativa (OT) o sistemas de control industrial (ICS)"

reemplazar soluciones existentes para análisis forense de redes, búsqueda de amenazas, etc.

Retos y Oportunidades

Dice el Senior Partner Solution Engineer de VMware Iberia que, en general, "las oportunidades de mercado más lógicas para este tipo de tecnología están relacionadas con banca, seguros y otras grandes industrias", mientras que los principales retos a los que se enfrentamos los fabricantes de esta tecnología son: Dar a conocer la potencia que tiene esta nueva generación de soluciones de seguridad en red y cambiar la percepción de los clientes demostrándoles que son necesarias y más eficaces que otras soluciones tradicionales.

Para Alex López la gran ventana de oportunidad que se presenta en el mercado para las soluciones de detección y respuesta de red está relacionada con la migración de servicios a la cloud, bien pública y/o privada, que está haciendo que las soluciones ya desplegadas por los clientes para su entornos on premise dejen de tener efectividad; "la gran amenaza, para los clientes en este caso, va a ser contratar soluciones de nicho para cada uno de sus entornos, que van a acabar siendo poco prácticas al no mostrar toda la huella de amenazas de una manera unificada, requiriendo además unos recursos humanos muchas veces inexistentes".

"Esta tecnología es totalmente independiente de verticales de mercado", asegura Christian Buhrow añadiendo que la experiencia de ExtraHop es que son las empresas más maduras las que suelen utilizar este tipo de soluciones y que aquellas que ofrecen servicios de SOC gestionado (MSSPs)

“deberían ser los primeros en utilizar una solución NDR. Pero todavía les falta entenderlo”. Como reto índice también el directivo de ExtraHop que estas soluciones no son baratas, pero que “en cinco años ninguna empresa importante va a vivir sin un NDR porque cada vez hay más ataques que sólo se pueden evitar a nivel de red”.

Sin una herramienta NDR la posibilidad de que se produzcan compromisos e infracciones no detectados es un riesgo continuo. El caso de negocio para una plataforma NDR es simple: la evolución de los métodos de ataque justifica el uso de plataformas de detección de ciberseguridad que no pueden ser ignoradas por actores nefastos.

Enlaces de interés...

- Best Network Detection and Response (NDR) Solutions
- La Evolución de NDR

Compartir en RRSS

it Reseller
TECH&CONSULTING

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

SANTIAGO MORAL RUBIO

EXPERTO EN CIBERSEGURIDAD

Actualmente es el VP de Innovación y Ciberseguridad de OpenSpring y codirector y uno de los fundadores del Instituto DCNC Sciences de la Universidad Rey Juan Carlos, así como Presidente de la Asociación HITEC en España y miembro de su sede norteamericana. Moral Rubio, quien ocupó el cargo de CISO del Grupo BBVA entre 2000 y 2018, también ha participado en la creación del Grupo de Ciberseguridad del Laboratorio de Informática e Inteligencia Artificial (CSAIL) del MIT.

Compartir en RRSS

it Digital Security

Tribuna Experto

El Nacimiento de Zero Trust: CIS Community Defense Model y Mitre ATT&CK

Es riesgo con adversario como eje del modelo Zero Trust

Actualmente es el VP de Innovación y Ciberseguridad de OpenSpring y codirector y uno de los fundadores del Instituto DCNC Sciences de la Universidad Rey Juan Carlos, así como Presidente de la Asociación HITEC en España y miembro de su sede norteamericana. Moral Rubio, quien ocupó el cargo de CISO del Grupo BBVA entre 2000 y 2018, también ha participado en la creación del Grupo de Ciberseguridad del Laboratorio de Informática e Inteligencia Artificial (CSAIL) del MIT.

En la edición de Securmática de 2007 presenté un modelo de análisis de riesgos basado en el riesgo intencional. Junto con los amigos con los que entonces enredaba en esto de la Cyber lo bautizamos con el nombre de Casandra. Queda para otro artículo hablar de la estrecha relación de los CISOs con el Síndrome de Casandra o Síndrome de Martha Mitchell.

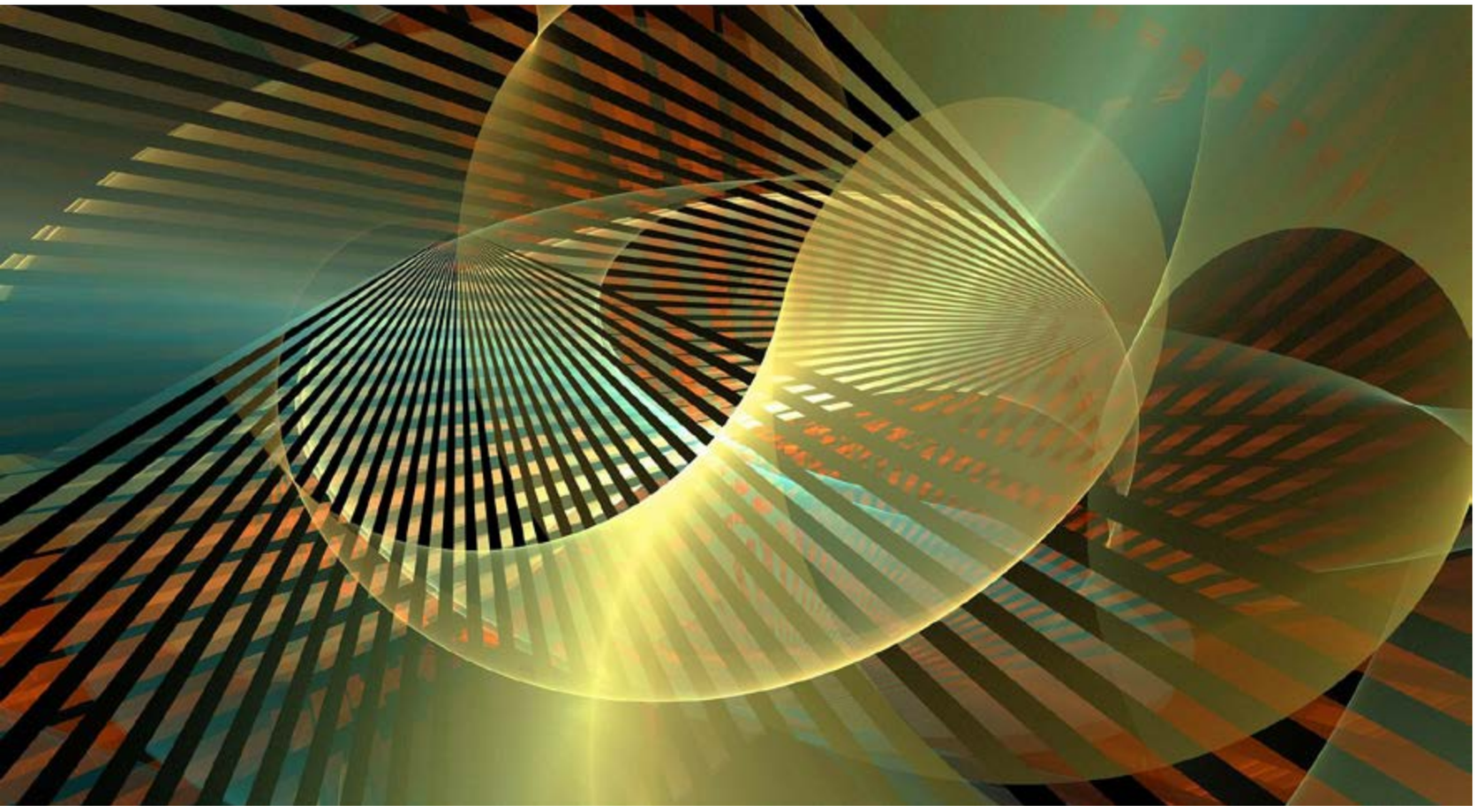
La principal diferencia entre un incidente oportunista y uno intencional es la premeditación. Implica paciencia por parte del delincuente. Implica estar a la espera durante el tiempo que sea necesario de que se den las circunstancias oportunas para perpetrar el delito.

Es lo que sucede cuando un atacante consigue saltarse las medidas de seguridad del perímetro, llegar a un servidor o un PC y desde allí estra observando durante semanas hasta que se dan las circunstancias oportunas para el ataque: El día que se publica un nuevo Exploit. Sabe que va a tener días o semanas para ejecutar el ataque. Desde el punto de entrada que consiguió tiempo antes, puede observar toda la red y llegar a donde le apetezca. Los sistemas tardaran tiempo en parchearse y las tecnologías de seguridad casi seguro que también. Es su momento. Su paciencia se ve recompensada.

> Los Controles CIS son uno de los conjuntos priorizados de elementos de protección que están entre los más reconocidos en la industria de la Ciberseguridad

El modelo que comenzamos a utilizar en 2007 estaba basado en la idea de que la premeditación y la alevosía son las bases sobre las que opera habitualmente la delincuencia organizada. La tecnológica también.

Si estábamos en lo cierto, había una consecuencia muy interesante a la hora de elaborar planes de seguridad. La forma de operar de los atacantes sigue patrones repetitivos. No todas las formas posibles de ataque las utilizan. Sólo las técnicas de ataque que estén bajo el paraguas de la premeditación y la alevosía van a ser utilizadas por



La principal diferencia entre un incidente oportunista y uno intencional es la premeditación

los atacantes. ¿Nos estábamos defendiendo de muchas más cosas de las que realmente eran necesarias? Y si la respuesta es positiva ¿Cuáles nos sobraban?

Es decir, las técnicas de ataque más utilizadas en los últimos meses son las más probables de ser utilizadas en los siguientes ataques. Por alguna razón "desconocida" en los ataques también hay modas. Según las hipótesis de Modelo Casandra se debe a que son las estrategias con las que la delincuencia tecnológica organizada optimiza en cada momento la rentabilidad de sus inversiones.

Desde este punto de vista, todo mecanismo de defensa que vaya a estar "eliminado" algunos días cada pocas semanas, es un elemento que favorece la premeditación de los atacantes en la ejecución de sus delitos.

Los modelos Zero Trust buscan el diseño de arquitecturas que no estén basadas en el principio de que algunos días al mes somos vulnerables.

Nos quedaría poder catalogar cada mecanismo de protección según un ratio de cuántos días de media al año va a estar "fuera de juego". Podríamos intentar medir este ratio de los distintos antivirus, EDR, cortafuegos, … y por qué no de los sistemas operativos, plataformas de nube, plataformas ofimáticas,…

Los únicos que conozco que se han atrevido a hacer algo parecido han sido l@s chi@s del CIS. Luego volveremos sobre esta auto-medición de efectividad de sus 20 controles.

Y en agosto de 2020 nació Casandra.

Casi me caigo de la silla cuando a primeros de septiembre leí el documento que había elaborado el CIS en agosto llamado "Community Defense Model". Una organización de la talla de CIS había hecho el enorme trabajo de estudiar de manera pormenorizada los ataques de los dos últimos años. Habían llegado a la conclusión de que una inmensa mayoría de los ataques se clusterizaban en cinco grupos de incidentes.

- Ataques a través de aplicaciones Web.
- Insiders y abuso de privilegios
- Malware
- Ransomware
- Ataques dirigidos (Targeted Intrusions)

Lo sorprendente es que estos meta-incidentes lo son por que comparten las técnicas de ataque.

Las técnicas de ataque más utilizadas en los últimos meses son las más probables de ser utilizadas en los siguientes ataques

Desde el año 2013 CIS colabora con Verizon en la elaboración del DBIR, que es la base de datos anual que publica Verizon con las estadísticas de los ataques del año.

En este último año, CIS ha trabajado con los incidentes de la base de datos de Verizon y LOS HA MAPEADO CONTRA MITRE ATT&CK!!!!

ESPECTACULAR!!!

Es decir, han juntado las poderosas estadísticas de incidentes de Verizon con el detalle minucioso de Mitre ATT&CK.

El resultado son cinco matrices Mitre ATT&CK donde se marcan las técnicas de ataque que de manera repetitiva son utilizadas en cada uno de los cinco meta-incidentes. Es el trabajo de Ciberseguridad que más me ha sorprendido en los últimos años.

Por primera vez contamos en la industria de Cyber con una herramienta que aúna el detalle estadístico de los incidentes que realmente están sucediendo, con la minuciosidad de la descripción de cómo están sucediendo eso incidentes: Casandra ha nacido.

Al menos un tercio de la inversiones y del esfuerzo que hacemos para defendernos no sirve para nada

Hemos llegado al punto mollar del artículo. Si podemos saber cuáles son los Sub-controles CIS y las Técnicas Mitre ATT&CK más útiles en la defensa de la mayor parte de los incidentes, también sabemos por exclusión cuáles (y cuantos) son los controles que no sirven para para ninguno de los ataques.

Sorprendentemente (para algunos) el número de los controles de defensa que jamás aparecen como útiles en ninguno de estos cinco tipos de meta-incidentes son muy altos.

En caso de Mitre ATT&CK, de las 325 Sub-Técnicas descritas, sólo 211 aparecen en las estadísticas de Verizon. El 35,1% no parecen ser utilizadas en los casos estudiados.

La cifra sube cuando el propio CIS ha analizado la utilidad de sus 171 Sub-controles. Sólo 91 aparecen en algún momento como elementos útiles para defenderse de las técnicas de ataque estudiadas. 80 Sub-controles CIS, el 46,8%, no

CIS (Center for Internet Security) es una organización sin ánimo de lucro fundada por SANS Institute hace 20 años

aparecen en el modelo que ha nacido de las estadísticas obtenidas de los incidentes reales identificados por Verizon.

En la página 12 del informe CIS Community Defense Model hay una conclusión que es lapidaria: “Vale la pena considerar la eliminación de los Controles”. Se refiere a aquellos que verifiquen que realmente no son útiles para defender ninguna de las técnicas de ataque utilizadas en los dos últimos años y que tampoco estén destinados a aportar orden e higiene en los entornos de Cyber.

CIS (Center for Internet Security) es una organización sin ánimo de lucro fundada por SANS Institute hace 20 años.

Los Controles CIS son uno de los conjuntos priorizados de elementos de protección que están entre los más reconocidos en la industria de la Ciberseguridad. Periódicamente son reevaluados por voluntarios expertos de Cyber de todos los sectores públicos y privados.

Posiblemente ser una institución sin ánimo de lucro le permita ser la primera en aportar datos contrastados de que una parte no menor de los controles de protección que nos autoimponemos tiene escasa o nula utilidad.

Quedamos expectantes de los cambios que puedan aparecer en la versión 8 de los Controles CIS.

Enlaces de interés...

- Mitre Attack
- Casandra. Metodología de Análisis y Gestión de Riesgos
- CIS (Center for Internet Security)

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos it User

Almacenamiento it

Con la colaboración de: FUJIFILM Value from Innovation Western Digital.

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

Con más de 20 años en el sector de la CiberSeguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

El estado digital global:

del mal uso político de la evolución digital al estado digital global

A finales del siglo XX, la evolución digital dio a la un luz un fenómeno inesperado fruto de la necesidad de estudiantes universitarios de mejorar su comunicación personal: la creación de plataformas de redes sociales en la cual todos los participantes eran iguales y podían fácilmente intercambiar cualquier información, uno a uno, uno a varios o incluso, en un principio, uno a todos los participantes en la red social.

Febrero 2021

Compartir en RRSS

Facebook, inicialmente despreciada por los tecnólogos, fue una de las primeras redes y la que luego obtuvo la posición dominante al sobrepasar el ámbito universitario y conseguir millones y luego miles de millones de participantes; tuvo una enorme influencia en la evolución digital en el siglo XXI al dar nacimiento a la primera red social digital global en la que ciudadanos digitales operaban en prácticamente todos los idiomas escritos que existen en el planeta.

Apareció Twitter, otra plataforma con una idea absurda: permitir a los ciudadanos digitales difundir en 140 caracteres cualquier información que el ciudadano digital considerase de interés con la inmediatez de las plataformas digitas globales.

Google consolidó su liderazgo en los buscadores de Internet llegando a crear un nuevo verbo, que en español es “goglear”, y como resultado empezó a crear la mayor acumulación de datos sobre los usos y costumbres de los ciudadanos que se le ha permitido a una empresa privada.

El iPhone, fruto del genio de Steve Jobs, desde una antigua empresa de ordenadores personales casi quebrada, Apple, consiguió, a través de una nueva concepción del teléfono móvil, hacer el acceso a internet global, incluyendo regiones donde nunca se llegarán a tener redes físicas de cable.

Estas cuatro ideas han permitido el nacimiento de los Ciudadanos Digitales Globales, en los cinco continentes, en países ricos y pobres, gobernados por una tendencia política o la opuesta, independientes de la religión que profesen, la raza (aunque yo creo que hay una sola raza que es la humana), el sexo, la edad o cualquier diferencia que se la haya podido ocurrir a mentes calenturientas del pasado.

Disculpadme por esta introducción, muy personal, un tanto ingenua y superficial, pero era necesaria para llegar al concepto que paso a exponer.

La versión 1.0 del Político Digital aparece en la segunda década del siglo XXI y fue francamente mala, pésima diría yo. Los políticos de la segunda década del siglo XXI, en vez de utilizar las plataformas de acceso a los primeros ciudadanos digitales para mejorar la participación y el intercambio de ideas, escuchar y reconocer las necesidades de la mayoría, de manera grosera las utilizaron para promover la división y el enfrentamiento utilizando mecanismos propios de cibercriminales (legiones de falsos usuarios, difusión de falsa noticias, criminalización de ideas…) con el único objetivo de obtener o mantenerse en el poder pasando por encima de sus propias endebles convicciones sin ningún atisbo de ética o vergüenza ajena.

Como todo lo malo, situaciones tan vergonzosas como esta traen consecuencias que pueden ser incluso consideradas buenas, y una de ellas fue que en la tercera década del siglo XXI los ciudadanos digitales globales maduraron y fueron desarrollando resiliencia frente a las burdas manipulaciones de los políticos digitales versión 1.0, fueron reconociendo estas manipulaciones y se alejaron de quienes pretendían seguir usándolas para sus abyectos fines.

Hasta aquí una visión particular de la realidad hasta 2021 y un sueño de evolución de la humanidad a través del avance de los ciudadanos digitales ante uno de los casos de utilización dañina de las nuevas tecnologías para fines delictivos, mafiosos de la corrupción que produce el poder en los humanos.

A partir de aquí, un sueño del futuro en clave de optimismo de como el Político Digital puede ser parte del desarrollo del Estado Digital Global del siglo XXII.

Político Digital 2.0 apareció a mediados de la tercera década del siglo XXI, no tuvo nada que ver son la versión anterior, porque nació de un proyecto colaborativo de ciudadanos digitales independientes que desarrollo la primera plataforma de Inteligencia Artificial capaz de realizar todas las actividades útiles de los políticos (no citare cuáles son esas actividades útiles porque sería una lista muy larga), eliminando aspectos que durante siglos han entorpecido el buen hacer de los políticos (citare solo unos pocos, ambición desmedida por el poder, corrupción personal, narcisismo… no vale la pena detallar más)

La plataforma de Inteligencia Artificial del Político Digital 2.0 utiliza masivamente la tecnología DMA (Decision Making Algorithms), que permite tomar la mejor decisión en situaciones simples y complejas para cumplir Indicadores de eficiencia y eficacia diversos y necesarios, pero también nuevos indicadores tan importantes para los nuevos ciudadanos digitales como, por ejemplo, la felicidad y el bienestar emocional.

Pero cómo se pueden determinar estos indicadores si no es a través de un sistema colaborativo o red social donde todos los participantes en este modelo dan su opinión libremente, sobre temas creados o creando nuevos de su interés, tantas veces como consideren y en cualquier momento del día o la noche. Este sistema colaborativo es el principal combustible de datos que llega a la plataforma de Inteligencia Artificial.

Este ejercicio intelectual que fue creciendo en complejidad y capacidad de abordar diferentes problemas únicamente con las aportaciones de ciudadanos digitales y algunas empresas privadas del área del Deep Learning y de la Inteligencia Artificial nunca fue apoyado por los estamentos políticos de ningún país del mundo, temerosos de que por fin la evolución tecnológica digital hiciera irrelevantes los modelos políticos arcaicos y que satisfacían con prebendas inaceptables a las clases políticas.

Cuando este modelo de Político Digital 2.0 intervino como candidato en juntas de comunidades de

La aparición y expansión de las redes sociales son el primer paso de la creación de lo que conocemos como Ciudadanos Digitales

A finales de la cuarta década del siglo XXI surgieron dos eventos que aceleraron el proceso hacia el Estado Digital Global que disfruta la Humanidad en el siglo XXII

vecinos y luego en las primeras elecciones en municipios pequeños para apoyar a los gestores humanos, fruto de la gratuidad de uso de esta nueva plataforma, los resultados desde el primer período resultaron tan satisfactorios que muchos de los gestores (políticos) humanos que usaron la plataforma como apoyo a su gestión manifestaron que el sistema podría funcionar autónomamente.

El estamento político intentó prohibir estos sistemas aduciendo un supuesto derecho de los políticos de decidir sobre la cosa pública, a pesar de que con el transcurso del tiempo se iba demostrando que la gestión de los recursos había mejorado sensiblemente con el uso de esta plataforma Político Digital 2.0, proporcionando índices de eficacia y eficiencia desconocidos hasta entonces, pero, además, daba índices de felicidad cada vez más altos.

Al igual que en todo aquello que va quedando obsoleto por la evolución digital, se produjo una reacción para evitar lo inevitable, pero fue inútil, ya que la gran mayoría de ciudadanos digitales aprobaron e impulsaron su utilización y gradualmente se generalizo su uso en pueblos y ciudades cada vez más grandes y complejas.

A finales de la cuarta década del siglo XXI surgieron dos eventos que aceleraron el proceso hacia el Estado Digital Global que disfruta la Humanidad en el siglo XXII.

El primero fue la evolución de la plataforma Político Digital 3.0, cuya principal novedad fue el desarrollo de la Federación de plataformas que permitía que diferentes plataformas pudieran intercambiar información relevantes para el ámbito de cada plataforma.

El segundo fue el nacimiento espontaneo de un movimiento autodenominado Ciudadanos Digitales por la Sociedad Digital que se expandió por todo

Político Digital 2.0 apareció a mediados de la tercera década del siglo XXI, no tuvo nada que ver son la versión anterior, porque nació de un proyecto colaborativo de ciudadanos digitales independientes

el mundo en unas pocas semanas para conseguir plataformas a nivel de todos los grupos humanos que se federaran en una gran plataforma global para gestionar todos los recursos del planeta para todos los ciudadanos digitales vivos del planeta de la manera fas eficiente y eficaz y con el indicador Felicidad como objetivo principal para todos los habitantes del planeta.

Fueron unos años muy convulsos, donde este movimiento fue muy perseguido por diversos estados gobernados aún por políticos de la vieja escuela que se resistían a entender que su tiempo había pasado, llegaron a causar guerras antes que dejar el poder que ostentaban; el nacimiento de cosas nuevas, al igual que el nacimiento de un nuevo ciudadano digital, siempre se produce con dolor.

Después de dos décadas donde la resistencia a la evolución digital fue intensa pero decreciente, donde cada vez que un estado más establecía por completo su federación de plataformas digitales, la unía a la federación global y se daba un paso más al establecimiento del Estado Digital Global, se producía una celebración digital que duraba tres meses, y eso hizo que la década de los 60 fuera prácticamente de celebración continua que por, una casualidad del destino, mantenía el recuerdo de la década de los 60 en el siglo XX, festiva del amor y la paz, que tanto impacto tuvo en la evolución humana.

Así fue que en 2068 se presentó la plataforma Estado Global Digital (vulgarmente conocida también como Político Digital 4.0), que es la que ha avanzado hasta el siglo XXII poniendo en marcha la primera civilización global de la humanidad, pero que, sin embargo, permite mantener y cultivar todas y cada una de las culturas, idiomas, costumbres con un respeto a individualidad de todos los seres humanos elevando el índice de felicidad a su máxima expresión.

No solo la evolución digital del poder ejecutivo ha ocurrido en este siglo XXI, también les han pasado a los poderes legislativo y judicial y todos los demás estamentos del estado moderno, democrático o no, trayendo un aire nuevo al servicio público, elementos tan dañinos como la ambición de perpetuación en el poder, la corrupción económica, el narcisismo del poder… en fin todo lo negativo que el poder llega a producir en el ser humano.

Claro que no todo ha sido debido únicamente a la evolución digital. Otros muchos avances tecnológicos han contribuido: energías renovables, economía circular, genética avanzada, nanotecnologías y algunos otros que no imaginamos en la actualidad.

Y colorín colorado, este cuento se ha acabado… o no, este cuanto no se ha acabado… realmente es solo el primer capítulo de una nueva etapa de la humanidad que no soy capaz de imaginar.

Enlaces de interés…

- Teoría de la separación de Poderes

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos itUser

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

Con la colaboración de: brother