it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Mayo 2021 - nº 41

Estados Nación, licencia para hackear

‘No conozco ninguna herramienta única que ayude a hacer una gestión de la parte cíber más sencilla’ (SEAT)

‘No estamos en el momento de que sólo contratando tecnología podamos estar protegidos’ (habitissimo)

IT Webinars. Descubriendo SASE y las últimas tecnologías de detección de amenazas

Agari: Queremos restaurar la confianza en la bandeja de entrada del correo electrónico

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

it Digital Security

Directora	**Rosalía Arroyo** rosalia.arroyo@itdmgroup.es
Colaboradores	Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez
Diseño revistas digitales	Contracorriente
Producción audiovisual	Favorit Comunicación, Alberto Varet
Fotografía	Ania Lewandowska

it Digital MEDIA GROUP

Director General Juan Ramón Melara	juanramon.melara@itdmgroup.es
Director de Contenidos Miguel Ángel Gómez	miguelangel.gomez@itdmgroup.es
Directora IT Televisión y Lead Gen Arancha Asenjo	arancha.asenjo@itdmgroup.es
Directora División Web Bárbara Madariaga	barbara.madariaga@itdmgroup.es
Director de Operaciones Ángel Porras	angel.porras@itdmgroup.es

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

Estados-Nación, licencia para hackear

Son varias las razones que llevan a un ciberdelincuente a actuar. Unos, la mayoría, lo hacen por dinero, otros para satisfacer su ego u obtener el reconocimiento de sus compañeros; unos lo hacen en grupo y otros prefieren realizar sus actividades en soledad; hay quienes llevan sus reivindicaciones sociales o políticas al mundo online y aunque sus acciones causen daño no se consideran malos actores. También hay quienes operan a la sombre de un estado; pueden formar parte del mismo, o ser contratados cual mercenarios, pero son peligrosos. Trabajan sin temor a represalias legales, operan de manera encubierta, y tienen una importante cantidad de recursos a su disposición.

Los ciberataques procedentes de los estados se han duplicado en los últimos tres años y no sólo hay que pensar en países como China, Corea del Norte o Irán para buscar a los culpables de una escalada de violencia en Internet que no sólo impacta contra organizaciones gubernamentales sino contra cualquier empresa relacionada con estas últimas.

Además de hablar de los ciberataques procedentes de los estados nación, este número de IT Digital Security recoge las respuestas a varias entrevistas, entre ellas a los CISOs de SEAT, habitissimo y Citrix, así como al director general de Logicalis Spain.

La actualidad viene marcada por la entrada en nuestro país de Agari, una compañía que quiere devolver la confianza en la bandeja del correo electrónico a través de varias tecnologías capaces de detectar el phishig, entre otros, y ofrecer una defensa activa. Pcysys ya estaba en España a través del mayorista Ireo, pero la compañía sube la apuesta con el nombramiento de un responsable encargado de potenciar la venta de Pentera, su solución de pentesting automatizado.

#ITDSMayo resumen también las conclusiones de un Webinar titulado 'Descubriendo SASE y las últimas tecnologías de detección de amenazas' en el que han participado responsables de Bitdefender, ExtraHop, Forcepoint y Rapi7.

Como siempre cierran este número varias tribunas de opinión centradas de Zero Trust, diversidad, resiliencia y en la escasez de chips.

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

Estados Nación, licencia para hackear

No solo IT

Trabajar desde los cimientos para construir un futuro diverso e inclusivo en la ciberseguridad

La ciber resiliencia y su papel en el diseño de una estrategia de ciberseguridad

Redes Zero Trust: El aislamiento y la bidireccionalidad

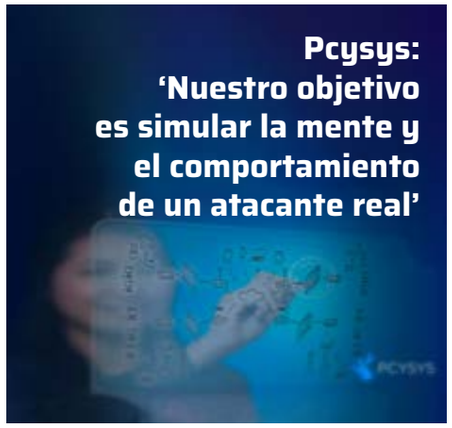
Escasez de chips y lucha por el podio entre Intel, Nvidia, Samsung, Apple, AMD, TSMC y Qualcomm

itds

Sumario

Actualidad

Agari: 'Queremos restaurar la confianza en la bandeja de entrada del correo electrónico'



Pcysys: 'Nuestro objetivo es simular la mente y el comportamiento de un atacante real'

Entrevistas

'No conozco ninguna herramienta única que realmente te ayude a hacer una gestión de la parte cíber más sencilla'

Alejandro Sánchez, CISO de SEAT

'No estamos en el momento de que sólo contratando tecnología podamos estar protegidos'

Judit Closa, habitissimo

'Los CISOs nos hemos dado cuenta de que la preparación al final del día compensa'

Fermín Serna, Citrix

'La confianza sigue siendo el gran agujero de la seguridad'

Alex Zaragoza, Logicalis

Índice de anunciantes

IT webinars

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro Vision One™

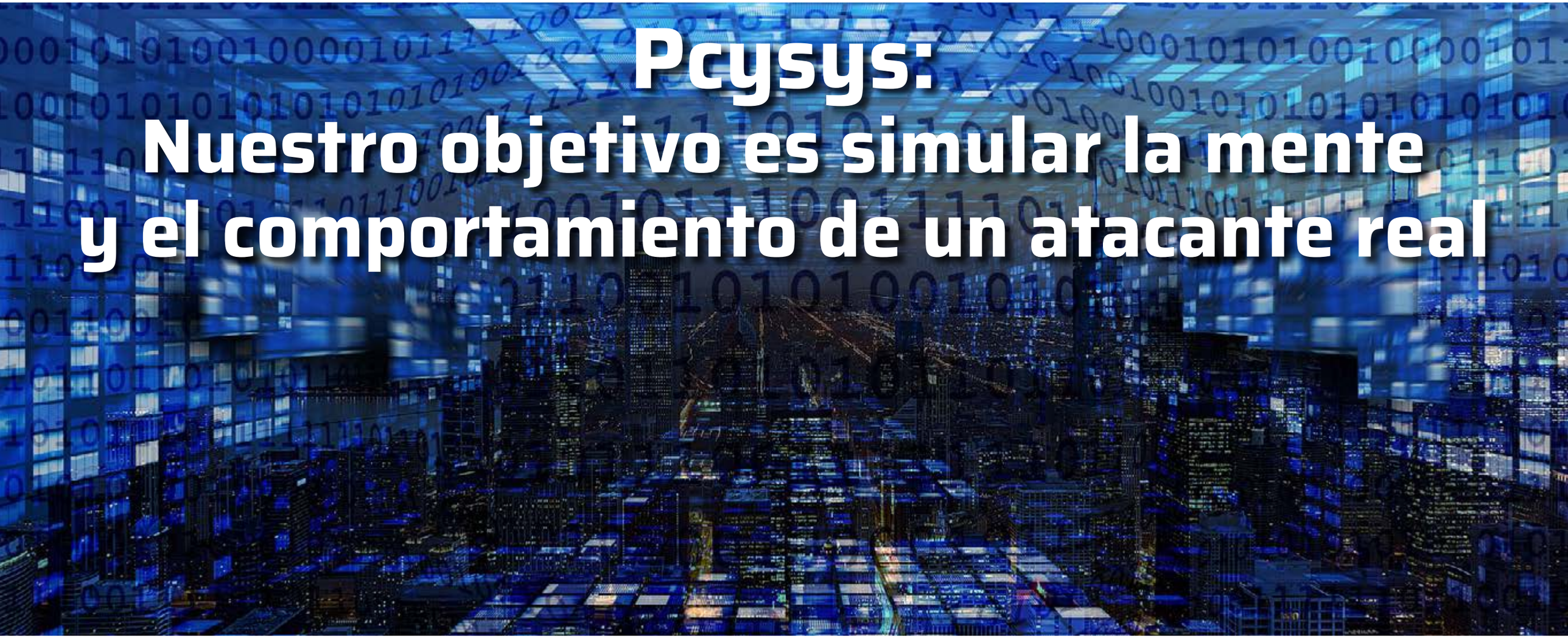
Mayor visibilidad para una respuesta más rápida

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

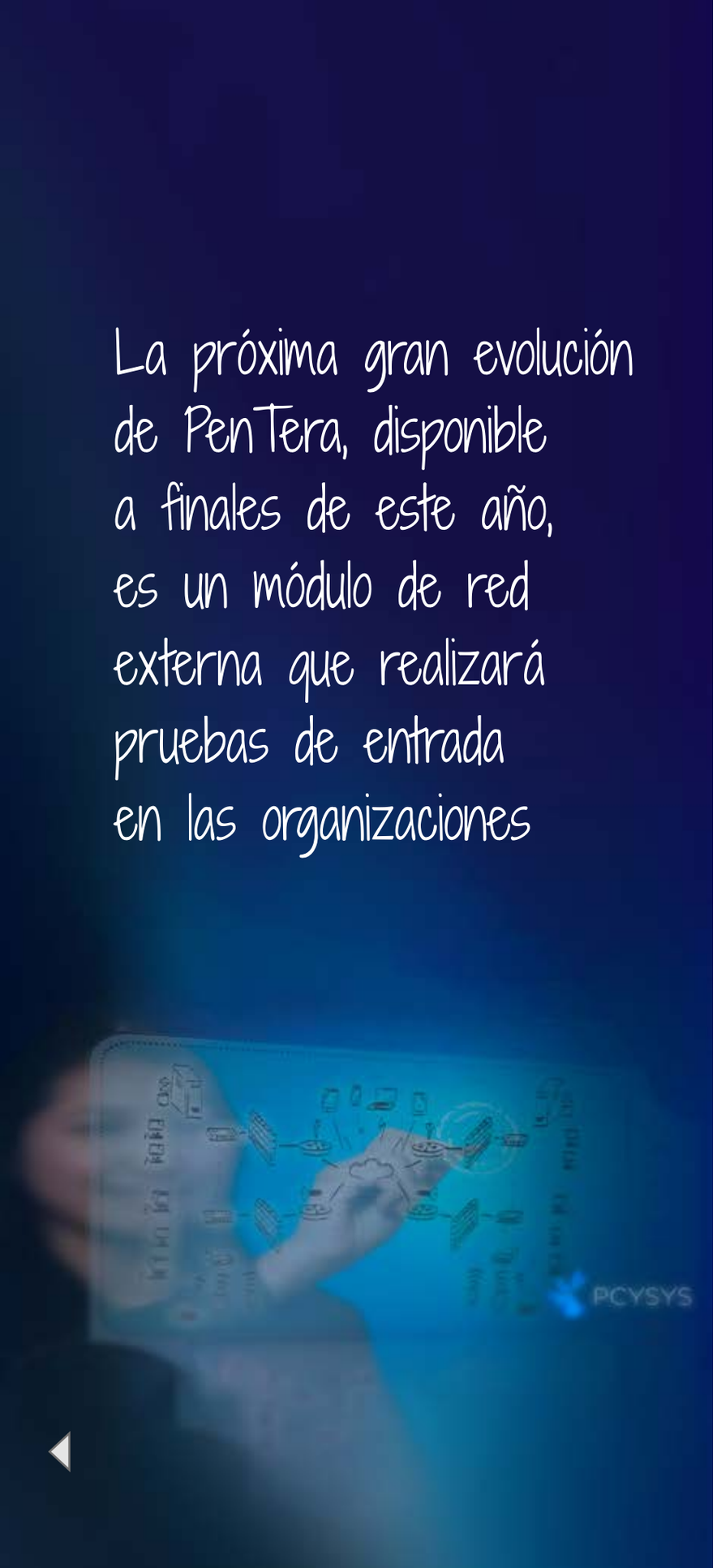
Más información en:
www.trendmicro.com

Pcysys, pronunciado ‘saisis’, del acrónimo Proactive Cyber Systems, es una compañía israelita fundada en 2015 que ha desarrollado PenTera, un sistema de automatización del pentesting para poder realizar una validación continua y consistente de la postura de ciberseguridad de las empresas. Nos lo cuenta Raúl Gordillo, responsable desde hace unos meses de esta compañía para la región de Iberia.

Pcysys: Nuestro objetivo es simular la mente y el comportamiento de un atacante real



Lo novedoso de Pcysys ha sido su capacidad para ofrecer un pentesting automatizado. El germen de la idea partió del propio fundador de la compañía, Arik Liberzon, quien dirigió un grupo de élite en la dirección de servicios informáticos de la Fuerza de Defensa de Israel responsable de las pruebas de penetración de redes de activos estratégicos y sistemas nacionales de misión crítica. Eran los tiempos en los que los ejercicios de red teaming y de hacking ético se hacían manualmente y por expertos, una figura que cada vez es más complicado fichar y retener debido a la escasez de profesionales en el sector. Y esto es lo que vio Liberzon, quien tras pasarse diez años realizando pruebas de penetración fundó Pcysys con el objetivo de automatizar todos esos ejercicios que se hacen manualmente, de crear un ciberdelincuente virtual capaz de



exponer las debilidades y posibles puntos de brecha de seguridad de una empresa, nos cuenta Raúl Gordillo.

"Donde una persona puede abarcar un ámbito limitado en un tiempo concreto, una máquina pueda abarcar mucho más de forma automática. Y ese es el concepto de cómo nace la compañía", dice el responsable de Pcysys en España y Portugal, añadiendo que el tiempo y el alcance son las dos grandes limitaciones de un buen testing manual, junto con el talento.

En un proyecto de pentesting tradicional los expertos analizan la empresa y buscan puertas de entrada, pero como no disponen de tiempo infinito, pueden estar centrándose en una parte de la red, o de la infraestructura, y dejando otras atrás. Además, "dependes del talento del profesional que haga el pentesting cada vez. ¿Quién garantiza que se está haciendo un buen trabajo sobre tus activos?", plantea Raúl Gordillo, añadiendo que hay que mantenerse muy al día de las últimas técnicas, tácticas y procedimientos de ataque que se estén lanzando al mercado.

Con un pentesting automático "es la máquina la que trabaja todo el tiempo en todas las partes de la red", mientras el departamento de i+d de la compañía trabaja en las últimas técnicas de ataques que van surgiendo en el mercado para añadirlas a la plataforma; "nosotros desarrollamos todos nuestros exploits éticos y hasta que no comprobamos que es 99,99% seguro para que no haga daño en la red del cliente, no lo introducimos

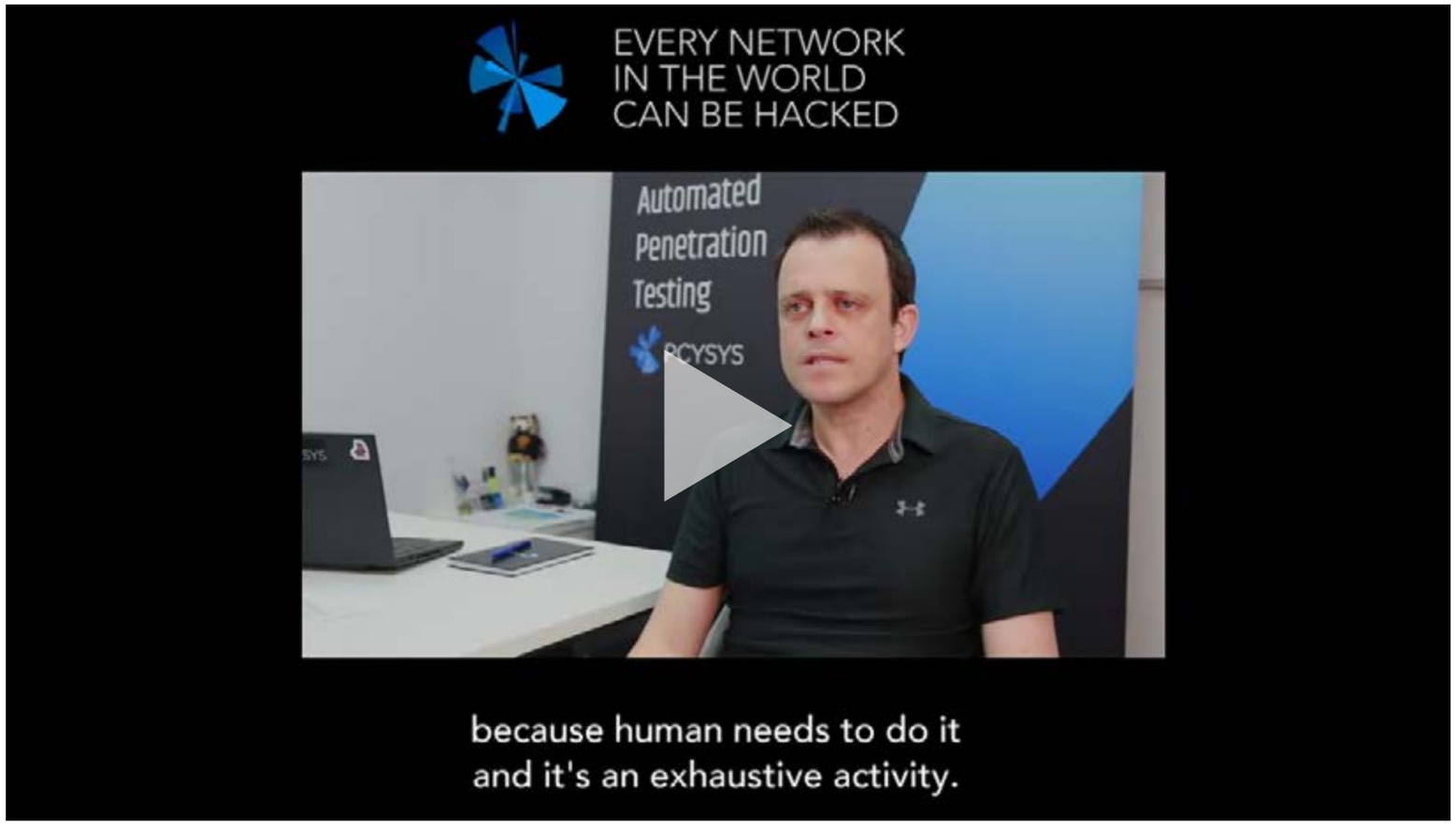
en la plataforma", lo que significa que la herramienta de pentesting automatizado siempre va a estar actualizada con las últimas vulnerabilidades, técnicas de ataque, etc.

Mercado en alza

"Las empresas se están dando cuenta de que su red es dinámica, que está cambiando constantemente, y la única forma de validar su postura de seguridad es realizando este tipo de ejercicios, pero de forma continua", responde Raúl Gordillo cuando le preguntamos qué es lo que está impulsando el mercado de soluciones de pentesting automatizado.

¿Significa eso que el pentesting manual está acabado? "No, porque la inteligencia humana también es necesaria", asegura Raúl Gordillo.

"Desarrollamos todos nuestros exploits éticos y hasta que no comprobamos que es 99,99% seguro para que no haga daño en la red del cliente, no lo introducimos en la plataforma"



4 RAZONES POR LAS QUE LAS PRUEBAS DE PENETRACIÓN DEBEN AUTOMATIZARSE

CLICAR PARA VER EL VÍDEO

La máquina puede realizar las tareas automáticas que no tienen un valor muy grande, pero que se van a realizar mucho más rápido, mientras la persona se puede dedicar a temas donde aporte su valor".

En todo caso PenTera se ofrece en un modelo de servicio que las empresas más enfocadas en pentesting manual pueden utilizar con sus clientes; "aseguramos que lo que esa empresa, con una persona o con un equipo, puede tardar a lo mejor diez días en un cliente, nosotros tardamos unas horas, o un día, y el resto del tiempo lo puede dedicar a valor añadido, o poder ir a más clientes".

Evolución

La compañía nace como una herramienta automática de pentesting de red interna. Se asume una amenaza interna o una brecha de seguridad que no se ha detectado y se analiza qué puede hacer esa persona que está dentro, hasta dónde puede llegar, qué información puede exfiltrar… La plataforma ha ido incrementando su capacidad con nuevas tipologías de ataques, nuevos sistemas operativos, nuevos protocolos, etc. La próxima gran evolución, disponible a finales de este año, es un módulo de red externa que realizará pruebas de entrada en las organizaciones.

La plataforma PenTera puede comprobar si el atacante ha saltado de la red IT a la red OT, "pero

"Las empresas se están dando cuenta de que su red es dinámica y la única forma de validar su postura de seguridad es realizando ejercicios de pentesting de manera continua"

Raúl Gordillo, Regional Sales Manager - Iberia, Pcysys

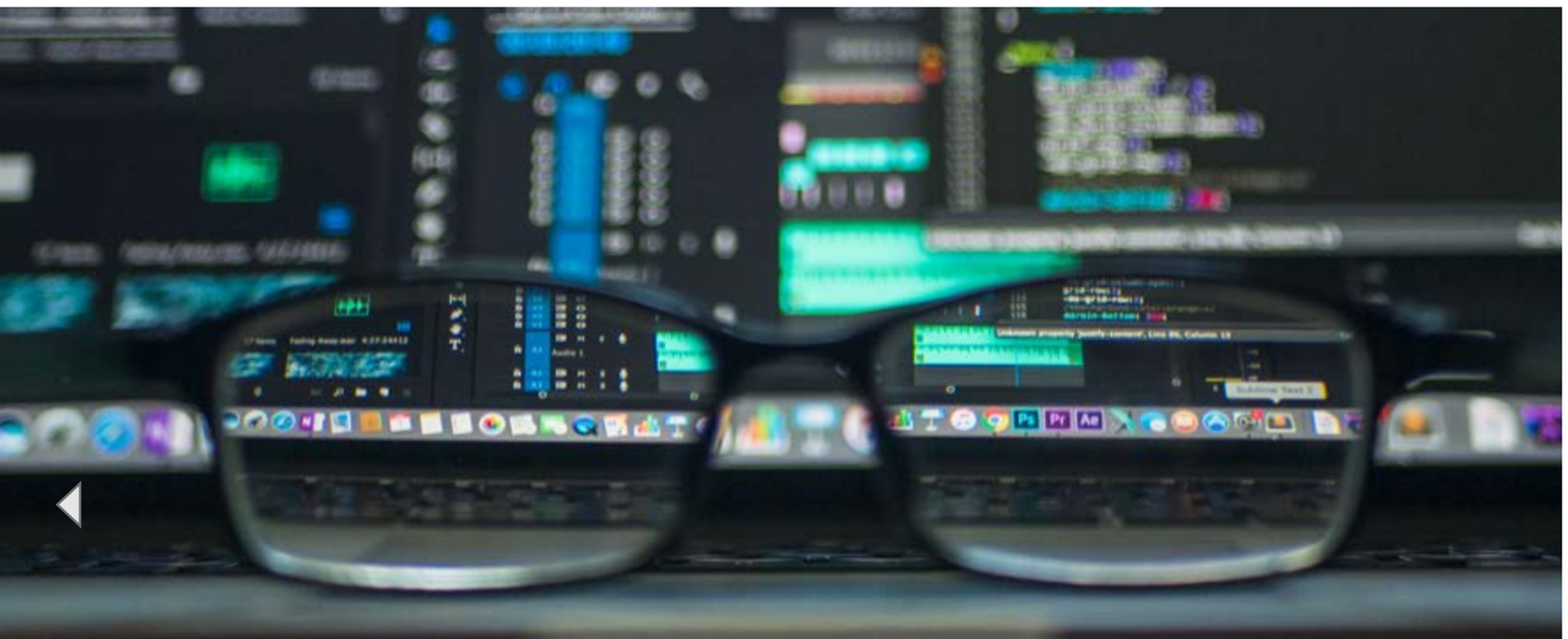
Enlaces de interés...

- Pcysys
- El mercado de 'testing' de seguridad crece por encima del 22%
- ¿Cuáles son las lecciones aprendidas del ataque a SolarWinds?

no tenemos desarrollados exploits para atacar redes OT, por ahora".

Sobre la tipología de un cliente de Pcysys dice Raúl Gordillo que el cliente objetivo tiene que tener cierto grado de madurez de seguridad y que el modelo de negocio es una suscripción anual o multianual basado en número de endpoints que permite al cliente hacer los ejercicios que quiera tantas veces como quiera.

Después de las pruebas de penetración, el sistema genera información y señala los riesgos y fallas de seguridad, para que las organizaciones puedan solucionarlos y mejorar sus defensas de ciberseguridad. La plataforma prioriza los riesgos y permite a las organizaciones concentrarse en sus vulnerabilidades más críticas, aliviando la responsabilidad de protegerse contra los miles de ataques no críticos. Según la empresa, su sistema de pruebas de penetración no tiene agentes y no es una simulación, sino una infracción real de la vida real.



Antes del nombramiento de Raúl Gordillo como responsable de Pcysys en Iberia, la compañía estaba presente en la región a través de Ireo. En los últimos meses se ha hecho un gran esfuerzo por incrementar el número de partners y certificarlos, explica Raúl Gordillo, añadiendo que "la estrategia es definir un modelo de partners no muy amplio y trabajar con ellos las oportunidades".

Compartir en RRSS

S21SEC

CIBERSEGURIDAD INDUSTRIAL

Servicios enfocados a una gestión eficiente de los riesgos de ciberseguridad industrial.

Conoce tus sistemas de automatización y control mejor que el enemigo.

Ahuyenta a potenciales atacantes de tus instalaciones industriales.

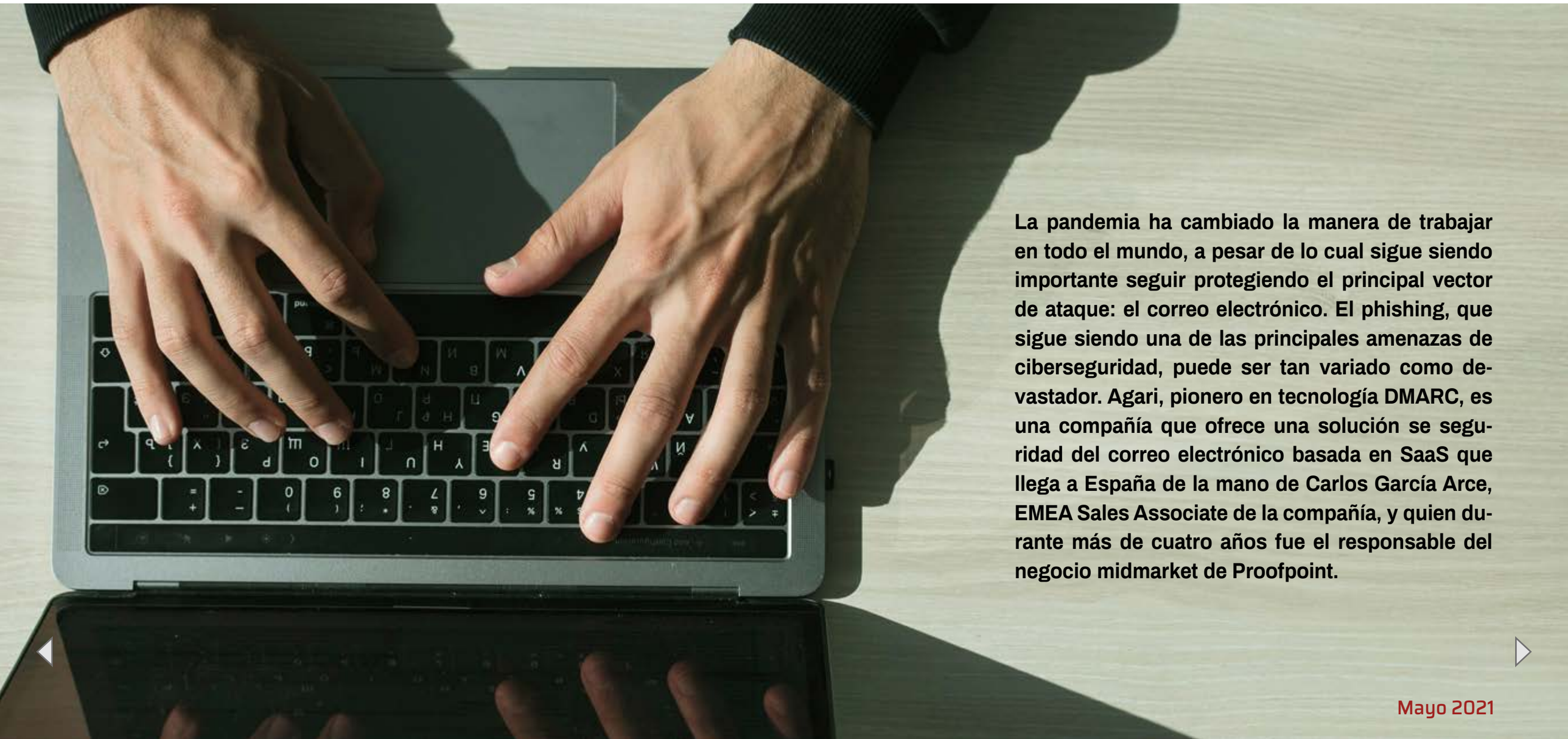
Vigila a tu enemigo en los procesos industriales.

Lucha contra el enemigo de tus instalaciones industriales.

Para más información puedes visitar www.s21sec.com/es/ciberseguridad-en-el-sector-industrial/ o escribir un correo a marketing@s21sec.com

Agari:

Queremos restaurar la confianza en la bandeja de entrada del correo electrónico



La pandemia ha cambiado la manera de trabajar en todo el mundo, a pesar de lo cual sigue siendo importante seguir protegiendo el principal vector de ataque: el correo electrónico. El phishing, que sigue siendo una de las principales amenazas de ciberseguridad, puede ser tan variado como devastador. Agari, pionero en tecnología DMARC, es una compañía que ofrece una solución se seguridad del correo electrónico basada en SaaS que llega a España de la mano de Carlos García Arce, EMEA Sales Associate de la compañía, y quien durante más de cuatro años fue el responsable del negocio midmarket de Proofpoint.

Agari fue fundada en 2009 por ex empleados de Cisco IronPort y cofundadores del estándar DMARC para la autenticación de correo electrónico. La compañía acumula algo más de 84 millones de dólares en varias rondas de financiación, la última en 2018 por valor de 40 millones y liderada por Goldman Sachs. Agari utiliza inteligencia artificial predictiva basada en los datos de cerca de 2 mil millones de correos electrónicos al año, para proteger a las organizaciones contra el phishing, las estafas de compromiso de correo electrónico empresarial (BEC) y otras amenazas avanzadas de correo electrónico.

"Lo que Agari está proponiendo es ver el correo bueno, el correo que está alrededor del usuario final teniendo en cuenta con quienes interactúa, bien sean partners, clientes u otros empleados", explica Cargos García Arce, añadiendo que se empieza por generare "un nuevo graph de inteligencia que nos permite ver el correo bueno, el correo auténtico, y desechar lo que no es correcto sin necesidad de estar esperando la resolución de una sandbox, que para nosotros es una tecnología obsoleta".

Recuerda Carlos García Arce que el Phishing genera pérdidas anuales por valor de 18 millones de dólares y que los cibercriminales ya no buscan romper el perímetro sino impactar en las personas de la organización recogiendo información de diferentes fuentes "para saber quién eres, dónde estás, con quién te mueves, dónde compras o qué haces". Este conocimiento que los ciberdelincuentes consiguen de las empresas, y que pueden utilizar para hacer daño, ha llevado a Agari a incluir en su propuesta una solución de Brand Protection que permite actuar y responder ante una suplantación de identidad que haga creer a los clientes que están recibiendo un correo de una empresa o proveedor cuando quien está detrás es un ciberdelincuente. "A través de Brand Protection nosotros estamos simplificando y automatizando la aplicación del DMARC para que las empresas tengan una autenticación y aplicación de seguridad de correo electrónico saliente mucho más fuerte y efectiva donde realmente se reconozca que eres tú quien está mandando el correo", dice Carlos García Arce.

Agari Cyber Intelligence Division, o ACID, rastrea la actividad de los ciberdelincuentes para detectar compromisos del correo electrónico empresarial y ataques de spear phishing

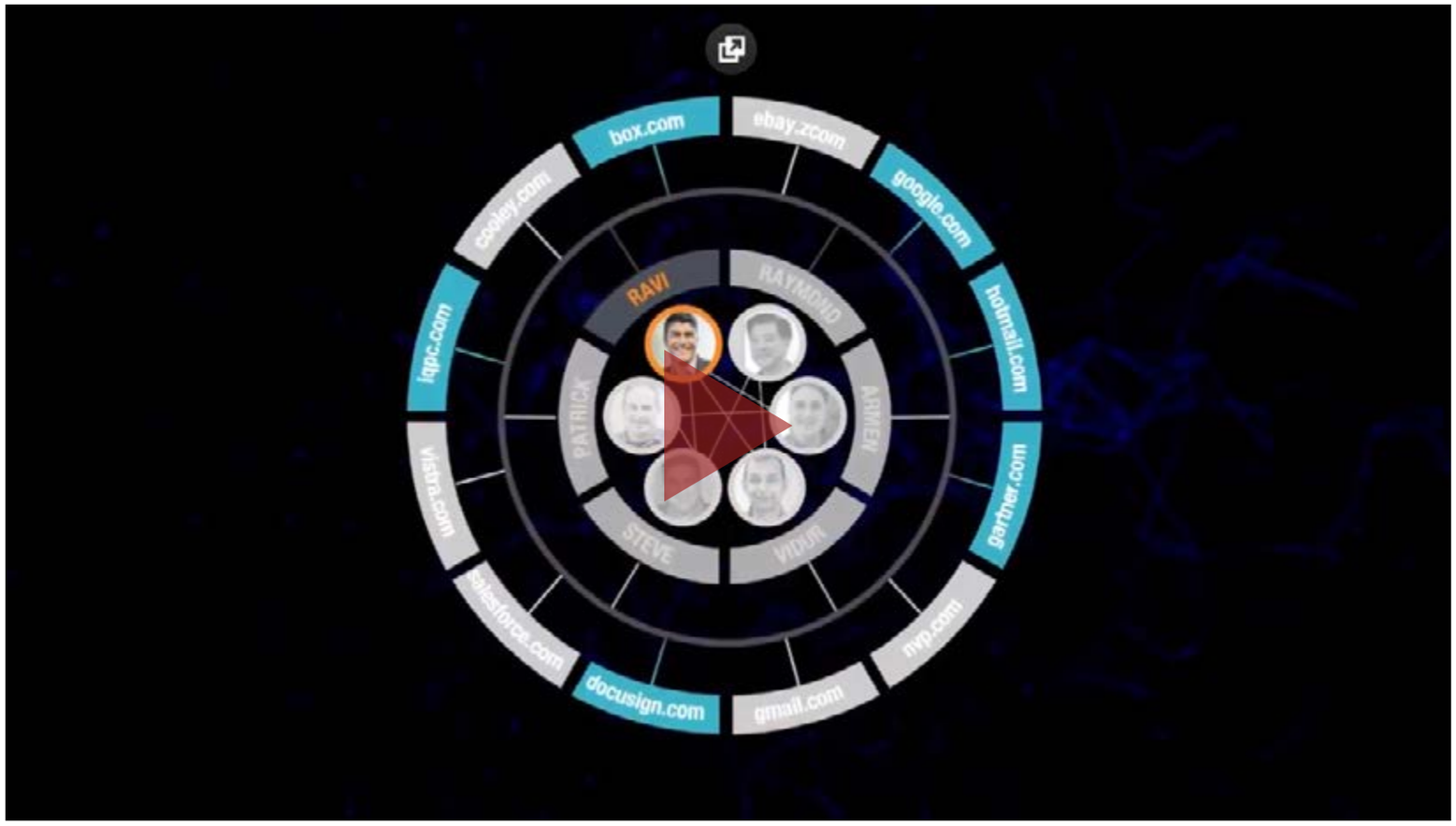
La experiencia del cliente queda garantizada gracia a un equipo de Customer Service que está apoyando constantemente a los clientes en la utilización de las soluciones de Agari

Asegurando que Agari está impulsando la adopción de DMARC como una parte de protección esencial, dice también el directivo que en España "el porcentaje de las empresas que tienen un DMARC bien colocado es muy reducido –no llega al 10%" y que uno de los objetivos de la compañía es concienciar en el uso de DMARC; "queremos devolverles a los empleados y a los usuarios la confianza en el correo electrónico, que puedas abrir un email y sea identificado correctamente".

Dentro de las soluciones que la compañía está promoviendo destaca Carlos García Arce un servicio de inteligencia, Agari Cyber Intelligence Division, o ACID, que rastrea la actividad de los ciberdelincuentes para detectar compromisos del correo electrónico empresarial y ataques de spear phishing. La compañía asegura que su División de Ciberinteligencia es el único grupo de investigación de contrainteligencia del mundo dedicado a la investigación del compromiso del correo electrónico empresarial (BEC) y la mitigación de los delitos cibernéticos. Desde mayo de 2019, ACID ha participado en más de 12.000 acciones contra ciberdelincuentes y trabaja en estrecha colaboración con los CISO, las fuerzas del orden y otros socios para detener el phishing basado en identidad y los delitos cibernéticos de ingeniería social.

Replicando el slogan de la compañía, la estrategia de Agari en España es la de generar confianza en la identidad del email. "Tenemos el compromiso con el mercado empresarial de generar un correo electrónico de confianza, reduciendo las amenazas de spoofing phishing de la cadena de suministro, el spear phishing, los ataques basados en cuentas comprometidas y, en general, restaurar la confianza en la bandeja de entrada del correo electrónico", explica Carlos García Arce.

El negocio de Agari en España se realizará a través de partners. Asegura el directivo que la compañía tiene la capacidad de ser ágil "y nuestro objetivo es apoyarles, ayudándoles a mejorar la ciberseguridad de sus clientes con la mejor tecnología, desde el inicio del proyecto hasta el despliegue y de manera continua". La experiencia del cliente queda garantizada gracia a un equipo



AGARI IDENTITY GRAPH

CLICAR PARA VER EL VÍDEO

Enlaces de interés...

- Agari Cyber Intelligence Division
- El phishing aumentó casi un 35% en 2020
- Microsoft sigue siendo la marca más suplantada en los ataques de phishing
- Los kits de phishing y de exploits encabezan la demanda de crimen como servicio

Agari está impulsando la adopción de DMARC como una parte esencial de la protección del email

de Customer Service “que está apoyando constantemente a los clientes en la utilización de las soluciones de Agari”, lo que, en opinión de Carlos García Arce, es uno de los puntos clave del éxito de Agari, no solo en Estados Unidos sino en todo el mundo.

Inicialmente la compañía está manteniendo reuniones con varios integradores en la región, a quienes han mostrado la propuesta y se plantean asociarse con un mayorista en un futuro.

Compartir en RRSS

2021

SONICWALL®

INFORME DE CIBERAMENAZAS

SONICWALL.COM | @SONICWALLSPAIN

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

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

OBTENGA EL INFORME COMPLETO

sonicwall.com/threatreport

EL MALWARE CAE AL NIVEL MÁS BAJO DESDE 2014

IDENTIFICACIÓN MÁS RÁPIDA DE MALWARE "NUNCA ANTES VISTO"

EL RANSOMWARE ALCANZA UNA CIFRA RÉCORD

INSPECCIÓN DE MEMORIA PROFUNDA MEJOR QUE NUNCA

EL CRYPTOJACKING HA VUELTO

EL MALWARE DE IOT AUMENTA UN 66%

INTENTOS DE INTRUSIÓN EN CONSTANTE CRECIMIENTO

‘No conozco ninguna herramienta única que realmente te ayude a hacer una gestión de la parte cíber más sencilla’

(Alejandro Sánchez, SEAT)

Rosalía Arroyo

Alejandro Sánchez es el CISO de SEAT, una empresa en la que lleva trabajando desde hace más de quince años. Dice que la ciberseguridad se ha convertido en un pilar básico desde el punto de vista de negocio; que la sostenibilidad es la clave a la hora de escoger una solución o tecnología; que es en la inteligencia donde el servicio gestionado aporta un valor añadido considerable; que eliminar el riesgo de los usuarios es muy complejo o que securizar el IoT pasa por la microsegmentación.

La figura del CISO ha cambiado bastante, tanto como la propia evolución del mercado y el concepto de la seguridad. Hace unos años se hablaba del IT Security y ahora se habla de la Information Security, dice Alejandro Sánchez, CISO de SEAT, añadiendo que dentro de la parte de Security no sólo se contempla la parte del hardware, sino los riesgos, cómo afecta a la empresa la ciberseguridad, “con lo cual se ha convertido en un pilar básico desde el punto de vista de negocio”. Por otra parte, el hecho de que todos los datos de la compañía estén cada vez más distribuidos refuerza la posición del CISO dentro de las compañías. Sobre el futuro del responsable de ciberseguridad en las empresas, dice Alejandro Sánchez que cada vez tendrá más peso con el objetivo de gestionar la seguridad del dato y la identidad.

El de seguridad es uno de los mercados más fragmentados. Hay, literalmente, decenas de fabricantes por cada capa de seguridad que se tiene que implementar. Dice Alejandro Sánchez que escoger es complejo porque en medio de un gran abanico de fabricantes “siempre hay uno que te da una mini funcionalidad que te va muy bien en un caso determinado, pero que los otros no cumplen”. La clave es la “sostenibilidad”, asegura el directivo hablando de la complejidad de tener un montón de sistemas totalmente diferentes que se tienen que gestionar; se prioriza por tanto “la sostenibilidad de las soluciones y que haya una convergencia. Por ejemplo, si estás implementando un tema de DLP intentamos buscar una solución que te cubra todos los aspectos, tanto el aspecto on-premise, el aspecto del endpoint y el aspecto del cloud en lugar de tener tres soluciones” con el fin de reducir la cantidad de herramientas que se tienen, a pesar de que en seguridad “hay casos de uso en los que es bueno tener dos soluciones diferentes que hagan lo mismo”.

La sostenibilidad que menciona el CISO de SEAT hace frente a la etapa del “Best of Breed” por la que pasó la industria tecnológica hace unos años. La rápida evolución de las tecnologías y soluciones, el avance de las amenazas, llevó a optar por lo mejor de cada casa, lo que aumentó la complejidad de la gestión y una demanda de automatización que llega hasta nuestros días. El ciclo parece estarse

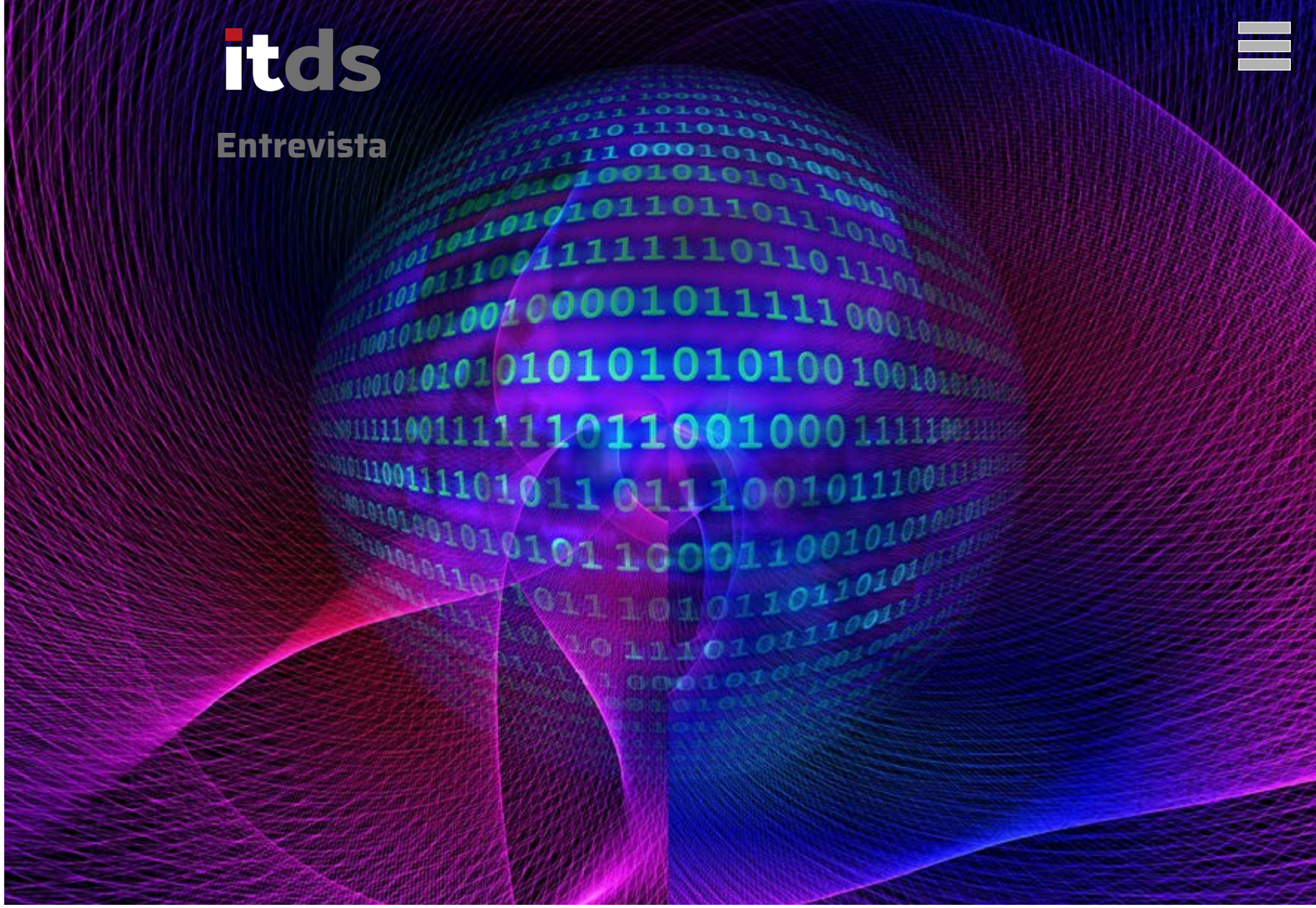
"Para la seguridad del IoT es fundamental el blueprint de seguridad establecido con guías de bastionado"

"La ciberseguridad se ha convertido en un pilar básico desde el punto de vista de negocio"

cerrando con la propuesta de arquitecturas de seguridad abiertas en las que integrar herramientas de propios y extraños que faciliten la visibilidad y control de la ciberseguridad. “Yo no conozco ninguna herramienta que realmente te ayude a hacer una gestión de la parte cíber más sencilla”, asegura Alejandro Sánchez, añadiendo que “al final tienes que tocar diferentes tecnologías, ir con cuidado y priorizar esa sostenibilidad”.

Sobre la sensibilización de la empresa española hacia la seguridad, dice el CISO de SEAT que, a pesar de que la concienciación y la sensibilización han crecido, aún queda mucho camino por recorrer, sobre todo en ser conscientes de los datos, en saber dónde los tienes o que los estás dando cada vez que instalas alguna aplicación en el móvil, por ejemplo.

En cuanto a los servicios gestionados de seguridad, está de acuerdo el directivo de SEAT en que sí son necesarios, pero no en su totalidad. “Yo no soy partidario de un 100% de servicios gestionados, porque al final el que más interés va a tener en gestionar tu seguridad eres tú. Creo en los modelos mixtos”. Destaca la inteligencia como elemento a tener en cuenta en un servicio gestionado explicando que las compañías generan inteligencia, entre otras cosas de los productos que tienen instalados, pero hay que tener en cuenta que los servicios gestionados tratan diferentes clientes, “y por tanto la inteligencia que un proveedor de servicios puede recolectar es mayor que la tuya como empresa individual, y ahí sí que creo que aporta un valor añadido considerable”.



Seguimos lanzando preguntas a Alejandro Sánchez, ahora en torno al impacto del elemento humano y la cadena de suministro en la seguridad empresarial. Recordamos que el impacto de SolarWinds sigue coleando meses después de haberse producido la brecha, y que por el camino se han visto impactadas otras empresas de seguridad que han anunciado vulnerabilidades en algunos de sus productos. Asegura que “eliminar el riesgo de los usuarios es muy complejo y muy difícil”, al tiempo que añade que hasta ahora el mayor vector de ataque que tienen las organizaciones es el phishing, y el phishing lo que busca es que el usuario se descuide, engañarlo y que pinche en el enlace, “y esto lo corriges con la parte de concienciación y formación”. En todo caso asegurando que el riesgo se puede minimizar, señala también que no se puede eliminar porque se llega a una frontera: la propia libertad del usuario; “y eso es lo que añade un nivel de complejidad radical”. Para eliminar el riesgo con garantías, continúa diciendo el CISO de SEAT, tendrías que plantearte dejar de hacer vídeoconferencias, no enviar ningún documento por correo electrónico… y esto es volver a 20 años atrás.

¿Qué tecnologías de seguridad crees que son imprescindibles para cualquier empresa? Tiene claro Alejandro Sánchez que la herramienta tiene que ir asociado a la visibilidad de la seguridad porque sólo puedes responder a lo que ves. Es decir, cualquier empresa necesita es un SIEM, “pero de nada te vale un SIEM sin datos; y si sólo recibes los datos de un firewall, te están faltando los de otros componentes de la red, aplicaciones, etc., que dotan de contexto a ese dato”. Ahora está de moda la detección y la respuesta, pero por lo mismo, “no se puede responder si tú no tienes el contexto de lo que está ocurriendo. Ese contexto te lo va a dar un SIEM porque tienes los datos, y un SOAR porque automatizas y realmente puedes hacer una gestión de ese incidente”.

"Eliminar el riesgo de los usuarios es muy complejo y muy difícil"

¿Si tuvieras un talón en blanco, y el tiempo no fuera un problema, qué tecnología de seguridad adoptarías? “Más que el talón y el tiempo, lo más crítico es el compromiso, el alineamiento del 100% de las organización”, asegura Alejandro Sánchez. Y es que de nada vale invertir mil millones si al final el usuario y contraseña es ‘admin’.

En todo caso, si tuviera que hacer una recomendación respecto a una tecnología escogería un DLP

"Yo no soy partidario de un 100% de servicios gestionados, porque al final el que más interés va a tener en gestionar tu seguridad eres tú. Creo en los modelos mixtos".

(Data Lost Prevention) en el que convergiera el mundo cloud y el mundo on-premise, porque lo importante es el dato y lo que tiene que prevenirse es la fuga, o pérdida, del mismo. Y si se quiere invertir más, invita Alejandro Sánchez a interesarse por el Machine Learning y los algoritmos matemáticos de correlación de eventos que te puede ayudar a crear un UEBA (User and Entity Behavior Analytics), por ejemplo.

IoT

Como fabricante de automóviles, SEAT es una de las muchas empresas que ha implementado el Internet de las cosas. ¿Cómo se protege ese IoT? "Para mí es fundamental el blueprint de seguridad establecido con guías de bastionado. Una vez que eres capaz de bastionar esos dispositivos puedes hablar de la seguridad de los mismos, y eso para los diferentes dispositivos, sensores, cómo se comunican, cómo se autentican y monitorizarlo". Dice además el CISO de SEAT que la gestión y la seguridad del IoT también está unido con la microsegmentación de las redes; "la guía de bastionado es lo mejor que le puedes hacer a ese dispositivo. Si luego no puedes actualizar ese dispositivo tienes que intentar buscar en la siguiente capa de seguridad de forma que en caso de que pase algo saber cómo lo detectas y cómo cortas y remedias el problema".

Por último preguntamos al CISO de SEAT si, después de todo un año de pandemia, prevé algún cambio significativo en torno a la seguridad. Para Alejandro Sánchez los cambios que podrían verse en seguridad este año y el próximo afectarán al cloud y las cargas de trabajo, sobre todo "si tenemos en cuenta que más del 95% de las organizaciones ya tienen presencia ahí y que la necesidad de rapidez hace que a veces se descuidan ciertos controles. Entonces yo creo que durante este año y el año que viene veremos un incremento de esa seguridad". Menciona también que habrá trabajo que hacer en torno al trabajo en remoto, y de manera específica en las conexiones o las herramientas de colaboración.

Enlaces de interés...

- 'El IoT es el principal dolor de cabeza en el sector sanitario' (Josep Bardallo, CISO Recoletas Red Hospitalaria)
- 'La seguridad es una carrera de fondo prácticamente sin meta' (Carlos Asún, CISO Food Delivery Brands)
- 'SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección' (Carlos Manchado, Naturgy)
- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)

Compartir en RRSS

netskope

Su información crítica está en la nube.

¿Y su seguridad?

Netskope.com/es

‘No estamos en el momento de que sólo contratando tecnología podamos estar protegidos’

(Judit Closa, habitissimo)

Judit Closa es la CISO de habitisimo un compañía creada en 2009 que en apenas doce años cuenta con más de 50.000 profesionales de la reforma y la construcción verificados en su plataforma, y que ha sido utilizada por más de diez millones de hogares. Dice esta experta de seguridad que el modelo de responsabilidad en la nube es “esencial”; que los que los servicios gestionados “ofrecen muchos beneficios a las empresas, pero no son la solución a absolutamente todo”; que es esencial disponer de unos sistemas de autenticación y de gestión de la identidad digital muy sólidos y que la seguridad continuará evolucionando porque “habrá nuevos ataques, actores y amenazas a tener en cuenta, así como nuevos riesgos a gestionar”.

Rosalía Arroyo

"Un buen CISO debe practicar siempre la escucha activa, tanto para atender al negocio como para saber cuáles son realmente sus necesidades”, lo dice Judit Closa Ribalta, CISO de habitissimo, una compañía que cuenta con una plataforma para el sector de la reforma y reparación con información detallada y opiniones sobre profesionales, empresas y marcas de arquitectura, interiorismo, obras y reformas. Añade Judit Closa que, además, un CISO debe tener un criterio muy bien definido para asumir los riesgos y poder tomar decisiones.

Asegura la CISO de habitissimo, cuya red suma casi dos millones de profesionales de la construcción, que la seguridad va siendo, cada vez más, una prioridad para la empresa española; “todo negocio se preocupa por su continuidad y eso hace que cada vez se esté más concienciado de las amenazas”, dice, añadiendo que al tener un negocio más concienciado, unos planes de seguridad más enfocados a lo que son los riesgos de seguridad, “estamos evolucionando a que la empresa española y en general la mundial esté más pendiente de las ciberamenazas”.

Para Judit Closa hay un paralelismo entre la pandemia que estamos sufriendo y esa concienciación de las amenazas y de los planes de continuidad; asegurando que nadie se esperaba que en pleno S-XXI viniera una pandemia, dice que “aun así” es necesario contar con planes de continuidad definidos para ello, para que den una respuesta que permita sobrevivir a esta crisis.

“La pandemia nos ha hecho aprender muchísimo”, dice la CISO de habitissimo, añadiendo que los responsables de ciberseguridad de las empresas tienen que estar dispuestos “con herramientas y formación” a poder hacer frente a las crisis. Asegura también que, si la adopción de cloud desdibujó las fronteras, la pandemia las redujo aún más. Explica que hasta las empresas más tradicionales ya estaban en un proceso de adopción del cloud, y de repente “deslocalizamos a los empleados de un día para otro. Esta deslocalización permanente ha sido y seguirá siendo un riesgo que las empresas más tecnológicas tenemos que estar en constante valoración”.

Y si los CISOs han aprendido de la pandemia, los CEOs, también. ¿Se han dado cuenta de la importancia de la seguridad?, ¿ha estrechado lazos estas dos figuras? Dice Judit Closa Ribalta que la adaptación constante al cambio es algo que tiene que tener un buen CEO, que son los referentes dentro de la organización. Con respecto a si se han estrechado los lazos, asegura la directiva que si se quiere interpretar una crisis desde un punto de vista positivo, constructivo, “las dos figuras, la del CISO

"Todo negocio se preocupa por su continuidad y eso hace que cada vez se esté más concienciado de las amenazas"

y la del CEO, van a tener que trabajar más de la mano, van a tener que tenerse más en cuenta".

El cloud, ¿se está adoptando de manera segura? "Depende de en qué casa", dice Judit Closa. Explica que hay empresas en las que la seguridad se tiene más en cuenta y que, en todo caso "desde seguridad no podemos impedir que el negocio progrese, que el negocio continúe siendo puntero a nivel tecnológico"; añade también la directiva que el modelo de responsabilidad compartida que se establece entre una empresa y el proveedor de cloud es "esencial", y que se tiene que trabajar en un modelo en el que "no por tener algo externalizado el departamento de ciberseguridad tenga que dejar de ser el responsable del dato".

MSSP

Los servicios gestionados quienes los ofrecen, los MSP (Managed Service Provider), se han convertido en figura esencial dentro del ecosistema tecnológico. Cada vez son más las capas de tecnología que tienen las empresas, capas que es necesario gestionar y tienen que interoperar. Y el mundo de la ciberseguridad no es ajeno a ello; no sólo hay cada vez más herramientas involucradas en la ciberdefensa de las empresas, sino que se debe hacer frente a amenazas más sofisticadas y a una constante falta de profesionales, lo que ha colocado a los MSSP (Managed Security Service Provider) en primera línea de batalla. Para Judit Closa la contratación de este tipo de servicios depende del modelo que quiera adoptar cada empresa, y añade que, en todo caso, "la tecnología no es nada sin personas detrás. Por mucho que haya muchísimos avances en inteligencia artificial, no estamos en el momento de que sólo contratando tecnología podamos estar protegidos. Para poder operar y gestionar tecnología puntera necesitamos personas detrás; personas formadas, personas especializadas y comprometidas".

Teniendo esto en cuenta asegura la directiva de habitissimo que los servicios gestionados "ofrecen muchos beneficios a las empresas, pero no son la solución a absolutamente todo" y que igual que ocurre con el modelo de seguridad compartida de la nube, cuando hablamos de servicios

"Las dos figuras, la del CISO y la del CEO, van a tener que trabajar más de la mano, van a tener que tenerse más en cuenta"

de seguridad, la responsabilidad de la seguridad sigue siendo de la empresa, no pasa por responsabilizar a un tercero que te está operando las herramientas. En todo caso, "es un servicio que crecerá cuanto más prioritaria sea la seguridad para la empresa española".

Tecnologías imprescindibles

Habla Judit Closa de tres pilares fundamentales cuando le preguntamos por las tecnologías de seguridad que cree imprescindibles: la parte de usuario, la parte de red que se tiene que proteger y monitorizar, y el poder dar una respuesta en caso de que hay cualquier tipo de incidentes. Si nos centramos en la parte del usuario "yo creo que es esencial disponer de unos sistemas de autenticación y de gestión de la identidad digital muy sólidos; y después proteger los dispositivos con un EDR para que el dispositivo con el que trabaja el empleado a diario no sea la puerta de entrada de las principales amenazas".

Para la parte de red menciona la CISO de habitissimo las tecnologías de firewall, analizadores de paquetes, monitorización, o detección de potenciales amenazas. Especifica que cuando hablamos de monitorización "tanto podríamos irnos a la tecnología tradicional de un SIEM como a los novedosos servicios de SOC-as-a-Service, que quizá sería una solución más que factible para una empresa pequeña o mediana que empezara a tener músculo operativo en sus diferentes verticales".

Fuera de lo que serían los imprescindibles, menciona Judit Closa algunas tecnologías que hay que tener en el radar, como son las que rodean y protegen al empleado. Hay tecnologías de endpoint protection y de detección y respuesta a amenazas del puesto de usuario que son "muy prometedoras", que en los últimos años se han desarrollado muchísimo "y son muy alentadoras en cuanto a cuánto puede llegar a ser de eficaz una herramienta para proteger la operación habitual del trabajador de la empresa".

Preguntamos por la adopción más o menos generalizada en las empresas de soluciones de seguridad más proactivas, como el deception, threat Hunting o simulación de brechas y ataques de seguridad BAS). Explica la CISO de habitissimo que "hay diferentes tipos de organizaciones en cuanto a su madurez en seguridad; la banca,

Enlaces de interés...

- 'El IoT es el principal dolor de cabeza en el sector sanitario' (Josep Bardallo, CISO Recoletas Red Hospitalaria)
- 'La seguridad es una carrera de fondo prácticamente sin meta' (Carlos Asún, CISO Food Delivery Brands)
- 'SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección' (Carlos Manchado, Naturgy)
- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)

por ejemplo, ya estaba hablando de threat hunting hace cinco años o más; después de estas grandes empresas, hay otro grupo preocupado por la seguridad por su volumen y el capital que mueven, que a lo mejor no son cotizadas, pero su negocio es crítico y que quizá lleven hablando de esas tecnologías hace dos o tres años. Pero hay una gran parte de pequeñas empresas que no están en el punto de preocuparse por threat hunting, aunque sí en el de empezar a preocuparse por saber cómo tienen la seguridad de sus usuarios, o de las redes."

En los últimos tiempos hemos visto cómo las amenazas de la cadena de suministro, los ataques internos, están causando verdaderos estragos en las empresas, muchas de las cuales han tenido que reorientar su seguridad para poder hacer frente a este nuevo reto. Dice Judit Closa que los departamentos de ciberseguridad tienen que salvaguardar tanto la seguridad de su organización como también su reputación, su imagen de marca; "la empresa tiene que ser una marca segura en la que sus clientes pueden confiar a la hora de dejar los datos", y eso significa que se tienen que definir las reglas internas y los controles para que los clientes se sientan seguros utilizando los servicios que se ofrecen desde una empresa.

"¿Cuándo no ha habido un cambio significativo año a año en la seguridad?", plantea Judit Closa cuanto le preguntamos qué se espera de este 2021, de un año que estará marcado por la vuelta a las oficinas, una vuelta al perímetro. Dice que habrá empresas que continúen con el teletrabajo y que "para esas empresas que vuelvan a la oficina, si realmente la arquitectura de red corporativa ha estado evolucionando hacia una arquitectura sin fronteras, no debería haber más impacto". Por otra parte, desde el punto de vista de la seguridad, se continuará evolucionando porque "habrá nuevos ataques, actores y amenazas a tener en cuenta, así como nuevos riesgos a gestionar".

CloudGuard

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

Más información:

www.checkpoint.com/es

Check Point®
SOFTWARE TECHNOLOGIES LTD

Rosalía Arroyo

‘Los CISO nos hemos dado cuenta de que la preparación al final del día compensa’

(Fermín Serna, Citrix)

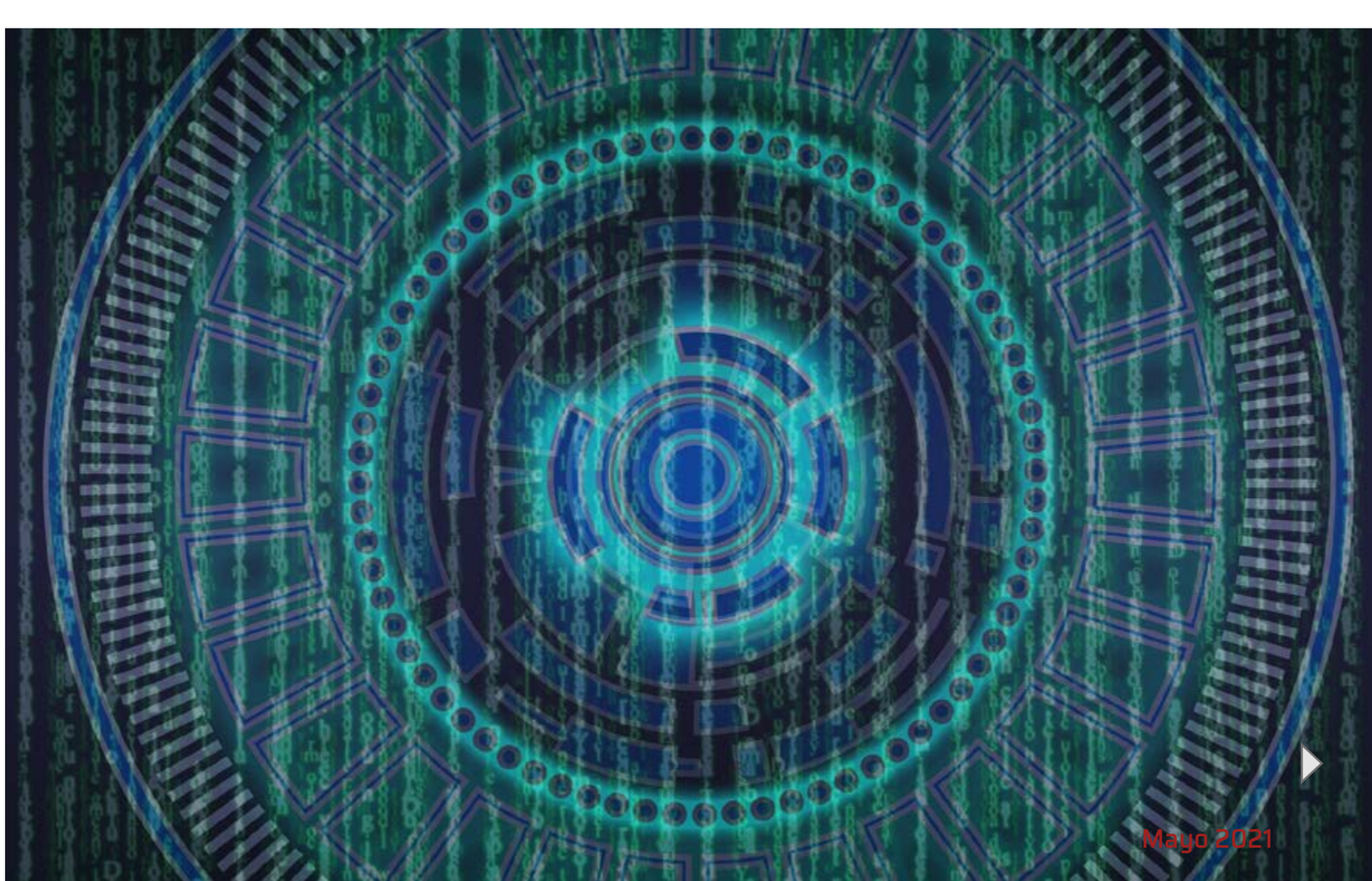
Mayo 2021

Aboga Fermín Serna por una Seguridad Invisible que ayude a los empleados a hacer su trabajo consumiendo seguridad sin saber que la está consumiendo y tomando decisiones de seguridad acertadas; dice que nos estamos quedando sin acrónimos; que el del CISO es uno de los trabajos más complicados del mundo y que hay que buscar alternativas a los antiguos problemas de seguridad.

Fermín Serna es el CISO de Citrix, una empresa con más de 30 años de vida, muchos para un mercado tan cambiante como el tecnológico. Antes de este rol fue el CISO de una empresa llamada Semmle a la que llegó después de dedicar más de diez años a realizar diferentes tareas de ciberseguridad en Google y Microsoft. Lo primero que preguntamos es qué retos tiene el CISO de una empresa que satisface un alto porcentaje de sus necesidades de TI y seguridad gracias a su oferta en torno al puesto de trabajo, incluidos la gestión de accesos y de endpoints, SD-WAN o analítica. “Ser CISO ya es difícil de por sí”, asegura el directivo añadiendo que ser CISO de una empresa de seguridad tiene dos componentes, “proteger nuestra empresa y ayudar a proteger a otros”.

En todo caso prefiere “poner un poco en contexto a qué es esto de ser un CISO”, un trabajo sobre el que asegura que es uno de los más complicados del mundo de la tecnología, entre otras cosas porque “te estás defendiendo incluso de cosas que desconoces”, y porque hay una falta de equilibrio entre el mundo ofensivo, de los atacantes, y el defensivo, que somos nosotros. Como ejemplo de esto último los 150 millones de dólares que un ciberdelincuente ganó a través del ransomware el año pasado, una cifra que según Serna tiene dos impactos: en primer lugar un ‘efecto llamada’ que hace que aumente el número de ciberdelincuentes; y en segundo lugar el alcance en la escala de operaciones, que pueden ir no ya contra 20 o 30 empresas, sino contra miles. Todo ello “a no ser que nosotros, los CISO, podamos proteger materialmente a las empresas, y a nuestros clientes y usuarios”.

El de la ciberdelincuencia es un mercado en alza. Ha evolucionado desde los primeros hackers que buscaban casi por prestigio y rebeldía adentrarse



"Los equipos de seguridad tienen que meter la seguridad en la cultura de la empresa"

en las empresas y probar qué impacto tenían los virus a ser auténticos profesionales organizados que también utilizan avances como el machine learning o el cloud para ser más eficientes. La dificultad de perseguirlos hace que sea complicado acabar con una industria tan rentable.

"Estamos siendo atacados por organizaciones, pero el rol del CISO es proteger a las empresas, no ir detrás de los ciberdelincuentes", dice Fermín Serna, añadiendo que tras un ataque lo primero es entender lo que ha sucedido, minimizar el incidente y, si hay filtración de datos comunicarlos a las autoridades, "que son las que tienen que hacer el trabajo siguiente, que es llegar hasta el cibercriminal. Y es un problema muy difícil porque la atribución en Internet en un problema complicadísimo".

Zero Trust y SASE

Preguntamos a Fermín Serna cuál es la aproximación de Citrix en torno al Zero Trust, un concepto que no es nuevo. Fue acuñado hace unos años por el vicepresidente y director general de Forrester John Kindervag, pero está ganando cada vez más tracción y despertando el interés de las empresas, y eso es porque "hay una necesidad nueva", dice el CISO de Citrix.

Echando la vista atrás, explica que en 2019 ya se veían dos transformaciones. Por un lado una tendencia a trabajar fuera de la oficina, tanto desde casa, como a conectarse desde un cibercafé, o en el aeropuerto; "de alguna forma la gente ya estaba trabajando un poco en remoto, bien sea horas o permanentemente". La segunda transformación, continúa Serna, es que todas estas aplicaciones, todos estos servicios que antes estaban en oficinas están en el cloud, "de forma que todos los controles de seguridad que se han puesto de antimalware, de firewall, de detectores de intrusión… no quiero decir que sean obsoletas, sino que no se aplican para ese modelo de trabajo".

Y es ahí donde el concepto de Zero Trust encaja, porque lo que se necesita es una seguridad contextual que responda a cada petición de acceso teniendo en cuenta que el usuario tiene, o no, las credenciales válidas, que accede desde una

"Hay que buscar alternativas a los antiguos problemas de seguridad"

localización lógica, que lo hace desde un dispositivo que está convenientemente protegido… "y en base a ese contexto es cuando yo apruebo esa petición, o decido no aprobarla porque aunque tengas unas credenciales válidas la petición me está viniendo desde Nigeria y me está viniendo a las 3 de la mañana, o incluso esta petición viene con credenciales buenas desde España, pero el portátil tiene algún problema y no permito el acceso".

En definitiva, no es que las empresas se están dando cuenta ahora que Zero Trust es una estrategia de seguridad necesaria, sino que los tiempos y las tecnologías evolucionan, que la gente trabaja desde casa, que cada vez se mueven más cosas al cloud "y hay que buscar alternativas a los antiguos problemas de seguridad".

¿Cómo puede Citrix ayudar a sus clientes a llevar a cabo una estrategia Zero Trust? "Cuando vamos a un cliente, lo primero que hacemos es entender qué problema están intentando solucionar", dice Fermín Serna, mencionando que puede ser tanto gestionar el trabajo remoto de forma segura como afrontar la integración de dos empresas tras una adquisición. En este caso se necesita conectar al personal, pero puede hacerse mediante la apertura de mi firewall y mi VPN, "que es una opción obsoleta porque estás exponiendo toda tu red perimetral", o utilizar otro tipo de soluciones como es el Virtual Desktop o Virtualized Applications con los que "puedes proveer un acceso seguro a los nuevos empleados" para que desde unos portátiles que no están gestionados puedan seguir trabajando de forma segura"

Tras hablar de Zero Trust nos adentramos en el mundo SASE (Secure Access Service Edge), otro concepto que está despertando un enorme interés en el mercado. Asegura Fermín Serna que se trata de un concepto muy interesante que también se ha visto impulsado por las dos transformaciones que se mencionaban antes: migración al cloud y trabajo en remoto. Explica Fermín Serna que SASE se puede dividir en dos grandes componentes: Secure Web Gateway, que es un proxy en el cloud donde se lleva todo el tráfico y se limpia; y el CASB, o Cloud Access Security Broker, que permite poner restricciones al cloud, como

"El del CISO es uno de los trabajos más complicados del mundo de la tecnología, entre otras cosas porque te estás defendiendo incluso de cosas que desconoces"

establecer que desde los portátiles de la empresa se pueda ir a Google Drive, pero solo a la carpeta corporativa. "Y esto tiene sentido, y lo va a tenar cada vez más".

CISOS y Pandemias

¿Qué crees que han aprendido los CISOs de la pandemia? Responde Fermín Serna que los CISO han aprendido varias cosas. Una de ellas es adaptarse muy rápido, "como ha sido el tener que implementar herramientas de colaboración y videoconferencia rápidamente sin que a veces se tuviera muy claro cómo compartir archivos de forma segura con herramientas como Zoom.

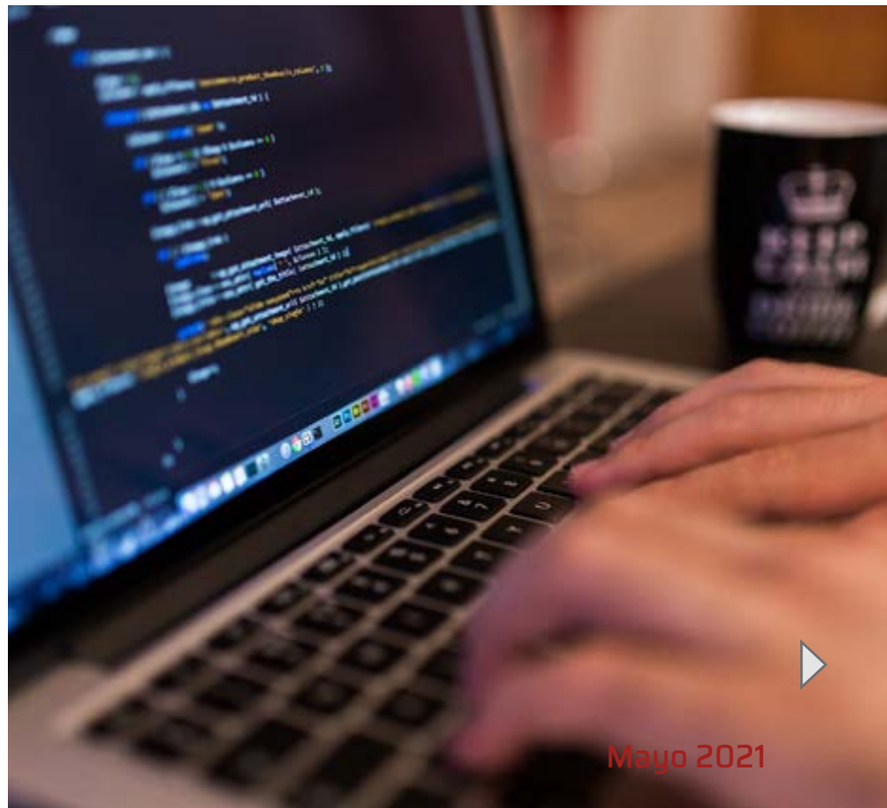
Además, los CISOs "se han dado cuenta de que la preparación al final del día compensa. Todos esos años de controles, de planes contingencia, de hacer las cosas bien tienen sentido en situaciones como las que hemos vivido".

Y Citrix, ¿qué ha aprendido de la pandemia? "Que somos una empresa que podemos ayudar. Somos una empresa que proveemos acceso seguro a aplicaciones y desktops, proveemos servicios para el trabajo donde quiera que estés y hemos ayudado a muchas empresas a través de nuestras soluciones, a través de nuestros servicios y a través de nuestros consejos".

En medio de la revolución de la seguridad endpoint hacia el EDR, del empuje de herramientas como el threat hunting, el NDR, XDR o los SIEM de nueva generación, ¿cuál crees que será el siguiente campo de batalla en la seguridad? "Yo creo que nos estamos quedando ya sin acrónimos", empieza contestando Fermín Serna para a continuación comentar que el gran problema del mercado de seguridad es el factor humano; "los equipos de seguridad tienen que meter la seguridad en la cultura de la empresa, que el usuario haga su trabajo consumiendo seguridad sin saber que la está consumiendo y tomando decisiones de seguridad acertadas". Es lo que conoce como Seguridad Invisible.

Enlaces de interés...

- 'El IoT es el principal dolor de cabeza en el sector sanitario' (Josep Bardallo, CISO Recoletas Red Hospitalaria)
- 'La seguridad es una carrera de fondo prácticamente sin meta' (Carlos Asún, CISO Food Delivery Brands)
- 'SASE no será algo que pase de refilón. Todas las empresas iremos en esa dirección' (Carlos Manchado, Naturgy)
- 'El cloud no viene ni a ni a resolver ni a empeorar la situación a nivel de seguridad' (Elena García, Indra)



Foro Administración Digital 2021

EVENTO ONLINE

Nuevos impulsos para la evolución de la Administración digital

18 de mayo · 9:00 h

Organiza

it Digital MEDIA GROUP

Socios estratégicos

Astic

Foro CPP colaboración público-privada TECNOLOGÍA & INNOVACIÓN

Patrocinador Platinum

salesforce

Patrocinadores Gold

aruba a Hewlett Packard Enterprise company

paloalto NETWORKS

Forcepoint

PEGA

MicroStrategy

V-Valley the Value of esprinet

Patrocinadores Silver

Bitdefender

SOPHOS Cybersecurity evolved.

CYTOMIC a WatchGuard brand

VMRAY

THALES

‘La confianza sigue siendo el gran agujero de la seguridad’

(Alex Zaragoza, Logicalis)

Rosalía Arroyo

Tiene claro Alex Zaragoza, director general de Logicalis Spain, que la empresa española demanda servicios de seguridad integrales; que el teletrabajo hace muy necesario por reforzar los controles de protección sobre la identidad digital; que en el futuro serán imprescindibles soluciones basadas en la protección de los entornos de DevOps, contenedores o serverless, y que el drama del sector TI es encontrar gente preparada para las tecnologías emergentes. seguridad

Logicalis es un System Integrator, que está ubicado dentro de un grupo internacional con sede en Londres y que opera en las cuatro geografías principales: Norteamérica, Latinoamérica, Asia Pacífico y Europa. Nos lo cuenta Alex Zaragoza, el responsable de Logicalis Spain donde trabajan unas 800 personas ofreciendo productos y servicios en torno a tres conceptos: el ciclo de vida del activo, referido a todos el aprovisionamiento de la infraestructura, bien sea on premise, cloud o en modelos híbridos; analytics y business intelligence; y seguridad.

Sobre esta última dice Alex Zaragoza que es una apuesta que se inició en 2007 y que “a diferencia de otras áreas, donde sí se ha realizado alguna adquisición, se ha ido creando orgánicamente”. Si bien los primeros años fueron complicados a pesar de que todo el mundo hablaba de seguridad, “de cuatro años aquí el tema ha explotado y la división de seguridad es la que más está creciendo y es, sin duda, la que más dificultad tiene en encontrar perfiles” dice el directivo, añadiendo: “Hoy en día el drama del sector TI es la contratación, encontrar gente preparada para las tecnologías emergentes”.

Tiene claro Alex Zaragoza que lo que está demandando la empresa española son “servicios de seguridad integrales” que sean gestionados por “empresas de confianza que les permitan afrontar

"Las empresas deben adaptar mecanismos cada vez más robustos de autenticación basada en entornos contextuales"

con garantía los retos relacionados con la transformación digital".

Explica el director general de Logicalis Spain que los servicios que se ofrecen a las empresas deben abarcar desde la integración tecnológica hasta unos servicios gestionados flexibles que se adapten a cada organización y que incluyan al mismo tiempo actividades de auditoría, de cumplimiento normativo o de servicios de seguridad avanzada, como puede ser un SOC; "y esto nos lleva a poder plantear soluciones de seguridad 360 grados".

Sobre si la pandemia ha impactado en las previsiones y los hábitos de compra de TI, dice Alex Zaragoza que ha acelerado una tendencia que ya estaba latente en el mercado: el modelo de aprovisionamiento basado en cloud, y específicamente en cloud pública, ha explosionado más de lo que estaban previendo todos los analistas, "y esto ha obligado a las organizaciones a adquirir el conocimiento necesario para tener los modelos de gobierno y las tecnologías apropiadas para ello".

Sobre el teletrabajo, que según Alex Zaragoza "es un concepto que se va a quedar en nuestra sociedad", dice que requiere proteger muy bien los datos y las aplicaciones desde cualquier ubicación y tener terminales seguros, "y esto hace muy necesario reforzar los controles de protección sobre la identidad digital, adaptando el famoso modelo Zero Trust". El teletrabajo está impulsando la demanda de soluciones relacionadas con la autenticación multifactorial, nuevas técnicas de protección de navegación y del correo electrónico, así como securización de las APIs o de acceso a los distintos Cloud Service Providers.

"Tenemos la obligación de añadir una capa de servicios gestionados, potentes y especializados alrededor de seguridad"

Compra de Áudea

A primeros de Abril Logicalis Spain anunciaba la compra de Áudea, una compañía que proporciona servicios de ciberseguridad y cumplimiento normativo, "dos áreas de nosotros no estábamos cubriendo dentro de nuestro offering, por lo que es una compra que nos fortalece y nos va a permitir ayudar en más campos a nuestros clientes en su transformación digital", explica Alex Zaragoza, añadiendo que Áudea y Logicalis son dos empresas absolutamente complementarias.

Áudea seguirá realizando su trabajo de manera independiente a la división de seguridad de los Logicalis, pero el acuerdo de compra permite a esta última ofrecer un porfolio más amplio y contar con un extenso equipo de especialistas en ciberseguridad y en cumplimiento normativo "que nos aportan valor interna y externamente".

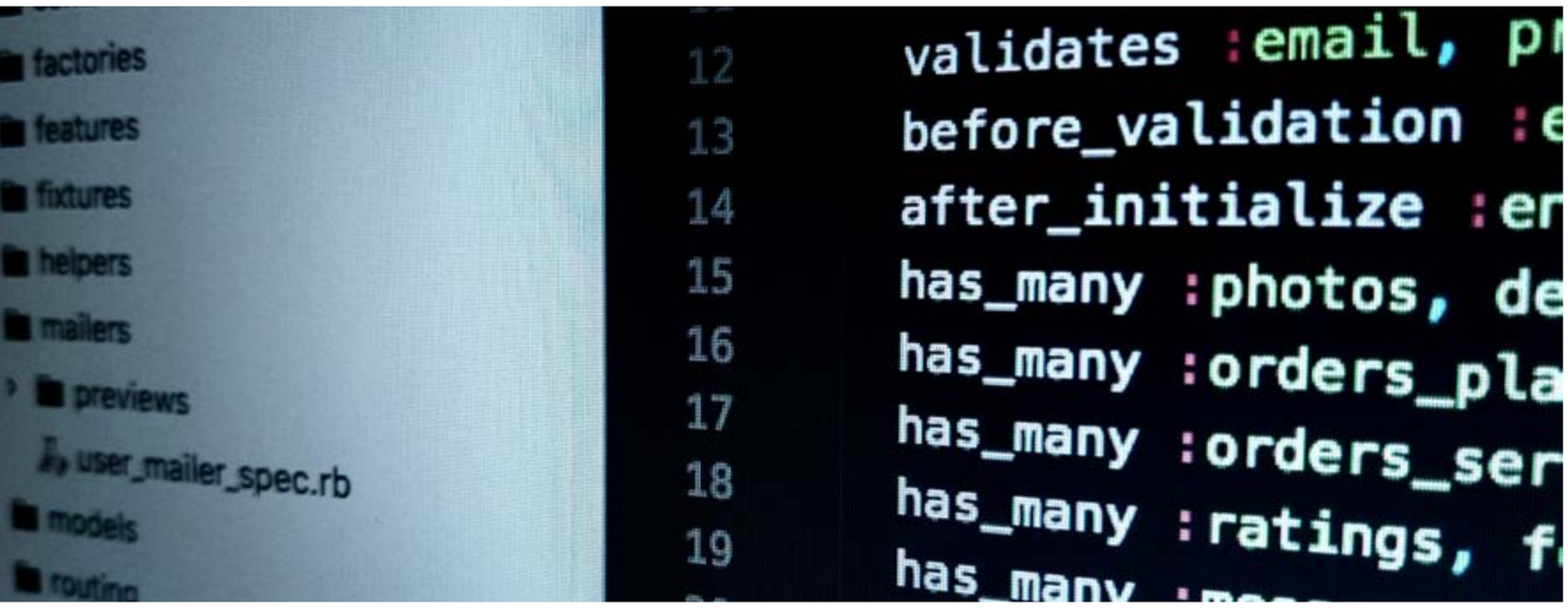
"Las empresas españolas, en mi opinión, están bastante sensibilizadas respecto a la importancia del cumplimiento normativo", dice Alex Zaragoza haciendo referencia al esfuerzo realizado en los últimos años con la LOPD, la GDPR y otras normativas más sectoriales como PCI-DSS.

La presencia de Alex Zaragoza en algunos comités europeos le permite asegurar que "España está al nivel de cualquier país europeo", en lo que se refiere a cumplimiento normativo. Añade que en el proceso de transformación digital y de migración al cloud "este cumplimiento ya viene casi de forma explícita".

La seguridad del futuro

"En nuestro negocio casi te has de reinventar cada semana", asegura el directivo cuando le preguntamos por dónde va a ir la seguridad en los próximos años, qué tecnologías de seguridad que aún no están ampliamente adoptadas serán imprescindibles en el futuro cercano. Dice que constantemente aparecen nuevas soluciones, bien creadas por los grandes proveedores de seguridad o por las empresas de nicho y que para el futuro serán imprescindibles "soluciones basadas en la protección de los entornos de DevOps, contenedores, serverless, soluciones basadas en microsegmentación de aplicaciones, gestión de APIs, automoción, soluciones que faciliten y securicen la conexión de los usuarios con los datos de las aplicaciones". Continúa diciendo el directivo de Logicalis Spain que para cubrir esas necesidades "las empresas deben adaptar mecanismos de seguridad que proporciona SASE (Secure Access Service Edge) complementados con una buena gestión de identidades y de usuarios privilegiados, así como

"El teletrabajo está impulsando la demanda de soluciones relacionadas con la autenticación multifactorial, nuevas técnicas de protección de navegación y del correo electrónico, así como securización de las APIs o de acceso a los distintos Cloud Service Providers"



mecanismos cada vez más robustos de autenticación basados en entornos contextuales".

Del lado de los proveedores, dice Alex Zaragoza que "tenemos la obligación de añadir una capa de servicios gestionados, potentes, especializados alrededor de seguridad, y aquí veo claramente un nicho de negocio para nosotros en el futuro".

Sobre el impulso de modelos como Zero Trust o SASE, asegura Alex Zaragoza que la confianza que sigue siendo el gran agujero de la seguridad" y que confianza es lo que están aportando modelos como los mencionados, que "están diseñados para prevenir brechas de seguridad y eliminar la confianza que las personas tenemos en el mundo de lo digital mediante verificaciones constantes de todos los usuarios, dispositivos, aplicaciones y de todas las ubicaciones".

Dice también el directivo que se trata de una estrategia que permite abarcar todo, desde las identidades, dispositivos, datos, cargas de trabajo o red "desde una aproximación de alto nivel y que tiene en cuenta qué hay que tener para proporcionar seguridad a una organización" y que además "facilita una implementación por fases en función del estado de madurez en el que se encuentre cada una de las de las corporaciones".

Enlaces de interés...

- 'La gente es ahora mucho más receptiva al discurso del HSM' (Javier Sánchez, Entrust)
- 'Más que fichar empresas soy de fichar buenos profesionales' (Alberto Pérez, V-Valley Seguridad)
- 'El gran riesgo en las cuentas privilegiadas es que se olviden de ellas' (Roberto Testa, Thycotic)
- 'Las empresas no pueden ser negligentes en la gestión de dato' (Francisco Valencia, Secure&IT)

Compartir en RRSS

SNi20

SNi40

STORMSHIELD

PROTECCIÓN DE **INSTALACIONES INDUSTRIALES**

De amenazas dirigidas a estaciones de trabajo o provenientes de la red

www.stormshield.com

IT Webinars

Descubriendo SASE

y las últimas tecnologías de detección de amenazas

Bitdefender ExtraHop Forcepoint RAPID7

Mayo 2021

Descubriendo SASE y las últimas tecnologías de detección de amenazas

La visibilidad, que se fue perdiendo conforme avanzaba la movilidad y el BYOD, y se complicó con el cloud y el trabajo en remoto, acelerados el año pasado debido a la pandemia, se ha convertido en un punto débil para las empresas. Para detectar amenazas y responder a ellas, necesitamos visibilidad de los múltiples entornos y capas de tecnología que utilizan nuestras organizaciones. Los centros de operaciones de seguridad (SOC) utilizan herramientas como la detección y respuesta de puntos finales (EDR), la detección y respuesta de red (NDR) y la gestión de eventos e información de seguridad (SIEM), una combinación de tecnologías comúnmente conocida como "la triada del SOC", para hacer frente a esta necesidad.

Al mismo tiempo, el mercado está impulsando una nueva arquitectura, bautizada como SASE (Secure Access Service Edge), que permite proporcionar un acceso seguro con independencia de la ubicación de los usuarios, los datos, las aplicaciones o los dispositivos.

Tres tecnologías: EDR, NDR, SIEM y una arquitectura, SASE, que están llamados a proporcionar la seguridad que toda empresa digital necesita y sobre las que debatimos con un grupo de expertos, empezando por Lucas Rey, Channel Manager Spain & Portugal de Forcepoint; Christian Buhrow, Sales Director DACH, IBERIA & ITALY de Extra-Hop; Daniel Vaquero, Cybersecurity Engineer de Ingecom y experto en Rapid7 y Horatiu Bandoiu,

XXXXXXXXX

CLICAR PARA VER EL VÍDEO

> "La mejor manera de detectar una anomalía, una brecha o una amenaza de seguridad es a través del análisis de tráfico"
>
> Christian Buhrow, Sales Director DACH, IBERIA & ITALY, ExtraHop

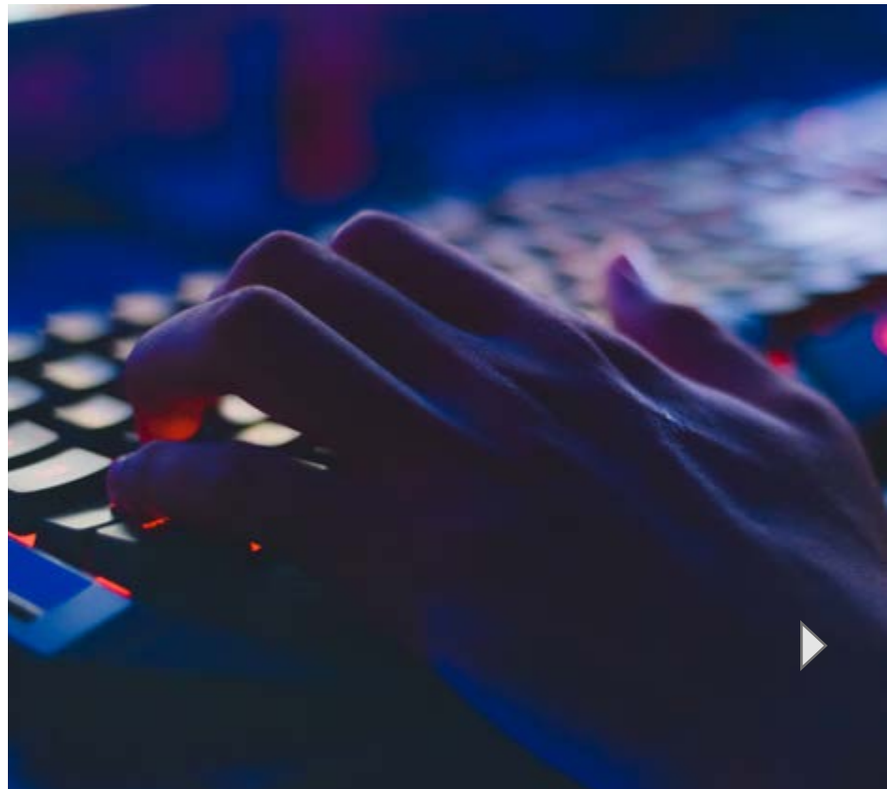
Channel Marketing Manager, SE & LATAM de Bitdefender.

Iniciamos el debate preguntando a Lucas Rey qué es SASE y qué viene a solucionar. Asegura este directivo que SASE es un modelo de entrega de seguridad como servicio que está orientado a cubrir problemas de adopción de servicios cloud en modalidad SaaS, PaaS o IaaS con un conjunto de tecnologías.

Las soluciones de Network Detection and Response, NDR, empiezan a imponerse en el mercado. Se trata de una tecnología "bastante novedosa que cubre la necesidad de tener visibilidad de lo que está pasando en las redes de las empresas", asegura Christian Buhrow. Explica el directivo que los ataques son cada vez más sofisticados y difíciles de detectar y que "la mejor manera de detectar una anomalía, una brecha o una amenaza de seguridad es a través del análisis de tráfico". Asegura también que son muchas las empresas que "se dan cuenta de que tienen falta de visibilidad, que no saben realmente quién está comunicando en mi red, en mi datacenter, y quién se está moviendo dentro de mi infraestructura". NDR viene a solucionar este problema.

Igual que NDR se va imponiendo, las soluciones de EDR (Endpoint Detection and Response) ya están más asentadas en el mercado. Evolución de las soluciones de seguridad de puesto de trabajo, los EDR se están volviendo imprescindibles porque "las empresas se dan cuenta de que el paradigma tradicional de 'tengo un cortafuego y un antivirus y estoy cubierto' ya no funciona", explica Horatiu Bandoiu. Añade este directivo que los EDR son ideales porque trabajan en tiempo real con alertas que proporcionan visibilidad a los analistas de seguridad, pero también ofrecen contención automática para muchas de las incidencias detectadas.

Pasamos a hablar de SIEM preguntando a Daniel Vaquero qué solucionan este tipo de tecnologías y para qué tipo de clientes están pensadas. Frente a las distintas propuestas de seguridad que se han ido planteando dice este experto que se necesita una herramienta que los gobierne a todos, un



centro de mando capaz de recopilar la información de las distintas fuentes y además aportar información relevante que permita ejecutar algún tipo de acción para poder contener las brechas que estamos detectando. Añade que la mayoría de las soluciones hacen la detección y respuesta, “pero cuando queremos automatizar esas respuestas entre distintas herramientas de ciberseguridad, necesitamos que algo los orqueste y en este caso son los SIEM los que toman este liderazgo para poder desplegar acciones lo más automáticas posible”.

Las empresas se enfrentan a cada vez más retos de seguridad, más amenazas y más avanzadas sin un incremento de los prepuestos de seguridad, ¿cómo puede un CISO hacer más con menos? Para el responsable de canal de Forcepoint para España

"La diferencia principal entre las herramientas de gestión de logs y los SIEM es la inteligencia"

Daniel Vaquero, Cybersecurity Engineer de Ingecom y experto en Rapid7

y Portugal, la clave está en utilizar un modelo de plataforma que pueda ajustarse a los desafíos de los propios clientes. “Buscamos una homogeneización de las tecnologías que no sólo genera una mejor operativa, sino que genera ahorros al conseguir una predictibilidad del gasto”, asegura Lucas Rey, apuntando a que esto ya genera ciertos ahorros, a lo que se añade la menor complejidad que conlleva contar con un único fabricante.

Frente a las soluciones de análisis de tráfico de red (NTA) más tradicionales, las soluciones de NDR implican una respuesta. Explica el responsable de ExtraHop en España que el análisis de tráfico es como parte ND antes de la R, y que “por una parte tienes que analizar y luego responder de forma automatizada”

“Aunque los EDR pueden ser tecnologías bastante democráticas, yo empezaría por recomendar dos pre-requisitos”, dice el representante de Bitdefender cuando el preguntamos qué se necesita tener para adoptar una solución de endpoint detection and response. “Para sacar provecho de la herramienta es importante tener al menos un equipo dedicado de seguridad y un proceso de incident response”, asegura Horatiu Bandoiu añadiendo que los EDR son herramientas en tiempo real y tienes que tomar decisiones al instante, por lo que “tienes que mantener una interacción continua con la herramienta,

ALINEADOS CON TU NEGOCIO

www.ingecom.net **Ingecom** info@ingecom.net

BILBAO C/ Elcano 9, 3ª pl - 48008 Bilbao - Tel.: +34 944 395 678 // **MADRID** C/ Infanta Mercedes 90, 8ª pl izq - 28020 Madrid - Tel: +34 915 715 196

algosec · ALIEN VAULT · allot See. Control. Secure. · Array NETWORKS · Bitdefender · CYBONET · Cymulate · efficient iP · ExtraHop · Forcepoint · FORESCOUT · GARLAND · Guardicore

Hdiv · KELA · MEDIGATE · mobileiron · okta · RAPID7 · sealpath · thycotic · Vicarius · viewtinet · wbsgo · ZEROFOX · ZIMPERIUM

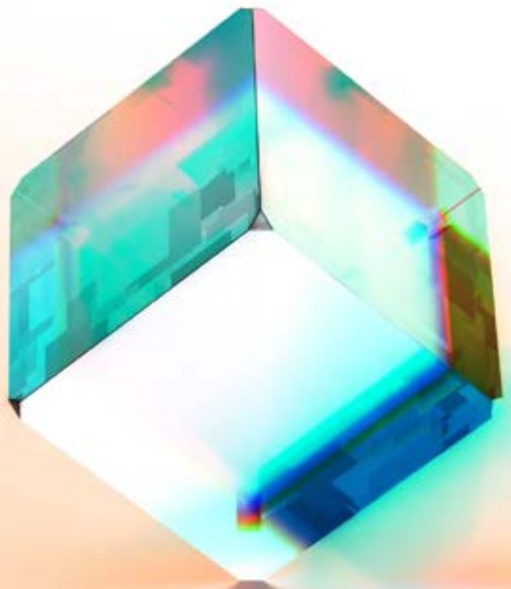
entender las alertas que te da, investigar y, en caso de necesidad, tienes que actuar cortando conexiones, terminando procesos, aislando equipos para su inspección y remediación, etc.”.

El nivel de integración es, en opinión de Daniel Vaquero, una de las características que tiene que tener un buen SIEM, que debe poder recoger información tanto de tecnologías heredadas como de nuevos servicios o productos para poder analizarla y convertirla en una información relevante para poder realizar una toma de decisiones que “debería hacerse de forma automática”.

El servicio SASE trata de consolidar la mayor cantidad de funciones de seguridad en sus nodos, y por tanto se han de considerar la protección en las comunicaciones y accesos y la protección de la información, explica Lucas Rey, añadiendo que una solución SASE debe tener en cuenta la gestión de identidades como uno de sus elementos claves a la hora de tener adoptar esta nueva arquitectura.

Junto con el EDR y el SIEM, el NDR es uno de los tres elementos que forman parte de lo que se denomina la “Triada del SOC” un concepto desarrollado por Gartner que para Christian Buhrow tiene mucho sentido porque son tres tecnologías y fuentes de datos muy diferentes que permiten conseguir en el SOC una visibilidad de 360 grados. “Las tres partes son esenciales”, asegura el directivo de Extra-Hop apuntando a que cronológicamente el SIEM ha sido la primera tecnología en la mayoría de las empresas, que el EDR ha llegado con muchísima inteligencia, conexión a la nube y tiempo real y que NDR cubre la parte de la red donde no se tiene la visibilidad.

La enorme escasez de especialistas de seguridad está impulsando la adopción de servicios de seguridad. Y el hecho de que uno de los retos de la adopción de un EDR sea la necesidad de contar con personal dedicado, ha llevado a algunas empresas, entre ellas Bitdefender, a crear soluciones de MDR



> "Una solución SASE debe tener en cuenta la gestión de identidades como uno de sus elementos claves a la hora de tener adoptar esta nueva arquitectura"
>
> Lucas Rey, Channel Manager Spain + Portugal, Forcepoint

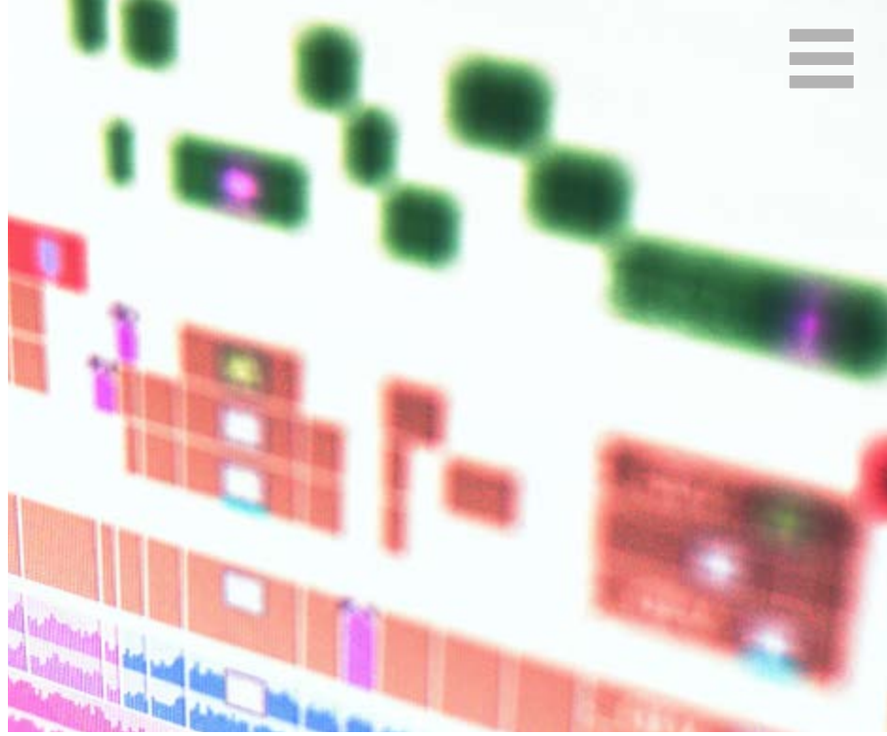
"La tendencia es incorporar las dos tecnologías, EDR y antivirus, y evolucionar hacia el XDR para conseguir una visibilidad completa y una respuesta rápida"

Horatiu Bandoiu, Channel Marketing Manager, SE & LATAM, Bitdefender

(Managed Detection and Response) que ponen a disposición de las empresas "los expertos que pueden hacerse cargo de varios aspectos, desde la detección e investigación y notificación hasta el Incident Response; intervenir y arreglar el problema en su lugar". Cuando el cliente es más avanzado se añaden servicios más avanzados, como el de Threat Hunting, que empieza identificado los activos más importantes del cliente para que después los expertos desarrollen escenarios avanzados de ataque; o la monitorización de la Dark Web para buscar indicios de que uno va a ser atacado o ya le han robado los datos y los quieren vender, por ejemplo.

Al igual que planteábamos la diferencia ente un NDR y una herramienta de análisis de tráfico de red, plantamos cuál es la diferencia entre un SIEM y una solución de gestión de logs. Para Daniel Vaquero estas últimas son importantes y no se suelen tener en cuenta. Asegurando que en algún momento toda empresa será ciberatacada, dice que es importantes analizar qué ha pasado, "y para ello vamos a necesitar la evaluación de los logs. La diferencia principal de estas herramientas con los SIEM es la inteligencia porque "de nada sirve tener logs y eventos infinitos si no podemos utilizarlos". Añade que el SIEM permite hacer correlaciones y "poder desarrollar las respuestas lo más automáticamente posible y con fundamento".

La protección de los usuarios remotos frente al contenido web malicioso y el uso indebido de las aplicaciones en nube es uno de los aspectos a tener en cuenta a la hora de escoger una plataforma



SASE, dice Lucas Rey. Añade el directivo de Forcepoint la capacidad de acceder a las aplicaciones privadas sin necesidad de utilizar VPN, simplemente a través del acceso a nuestra plataforma cloud: "el tercero es la protección del uso de la información en cualquier lugar" y un cuarto aspecto sería "la adopción progresiva con la capacidad de comenzar con unas necesidades inmediatas de SASE y poder ir incrementando otro tipo capacidades a lo largo del tiempo". Menciona Lucas Rey que también debe tenerse en cuenta que la plataforma sea nativa en cloud y capaz de evolucionar para adoptar todas las capacidades que se necesitan actualmente y en el futuro, y que el acceso a los servicios sea flexible.

"Para nosotros análisis de tráfico se refiere a analizar paquetes y hacerlo en detalle y no de manera superficial", dice Christian Buhrow cuando le preguntamos en qué hay que fijarse a la hora de escoger un buen NDR. ExtraHop analiza los paquetes que corren el red desde la capa 2 a la capa 7, se analiza "cada comunicación, cada transacción con la posibilidad de, con dos clics de ratón, entrar en

los paquetes para tener la prueba" de una brecha o de una amenaza. "Para nosotros es imprescindible al hacer análisis de paquetes para llegar al fondo y diferenciar entre sospechar y saber", añade el directivo.

Las soluciones de EDR, ¿reemplazan elementos o tecnologías de seguridad endpoint existentes? Dice Bandoiu que es más lo que aportan que lo que reemplazan. De forma que se puede tener la solución antivirus de toda la vida y montar encima un EDR para que aporte la visibilidad o incluso la capacidad de actuar. Asegura el Channel Marketing Manager de Bitdefender que "la tendencia es de incorporar las dos tecnologías" evolucionando hacia el XDR, o Extended Detection and Response que la compañía ha empezado a proponer al mercado "para conseguir una visibilidad completa y una respuesta rápida".

"La flexibilidad y la escalabilidad son los principales beneficios que aportan los SIEM que han migrado al cloud", dice Daniel Vaquero, añadiendo que constantemente vamos evolucionando y que lo que antiguamente nos parecía que era óptimo se nos ha quedado pequeño y cada vez tenemos más herramientas, más sistemas o incluso más usuarios. Un entorno cloud, dice también este ejecutivo, también nos va a aportar "las actualizaciones de ciberseguridad y la inteligencia en el mismo momento en el que el fabricante las incluye", así como aprovechar toda la capacidad del cloud "para hacer un procesamiento en profundidad, analizar el comportamiento de los usuarios (UEBA o UBA)", y la posibilidad de hacer una orquestación de todas las herramientas de ciberseguridad para no trabajar en silos de forma que se puedan tomar esas decisiones de una manera consciente y con confianza. it

Enlaces de interés...

- Guía para la integración de SecOps y NetOps
- Forcepoint SASE
- Prevención y mitigación de ransomware con Bitdefender GravityZone
- Impulsando el valor de un SIEM en la nube

Compartir en RRSS

itds

Webinar

¿Cómo puedo proteger la empresa digital?

“INSIGHTIDR REVOLUCIONA EL CONCEPTO DE SIEM” (RAPID7)

“TRABAJAMOS CON LOS CLIENTES EN UN GASTO PREDECIBLE Y FLEXIBILIDAD FRETE A LOS CAMBIOS” (FORCEPOINT)

“NDR ES EL PILAR FUNDAMENTAL DE LAS TECNOLOGÍA DE DETECCIÓN DE AMENAZAS Y ANOMALÍAS” (EXTRAHOP)

“BITDEFENDER PROPORCIONA UNA PLATAFORMA UNIFICADA DE SEGURIDAD BASADA EN VARIAS CAPAS” (BITDEFENDER)

Clicar para ver los vídeos

Mayo 2021

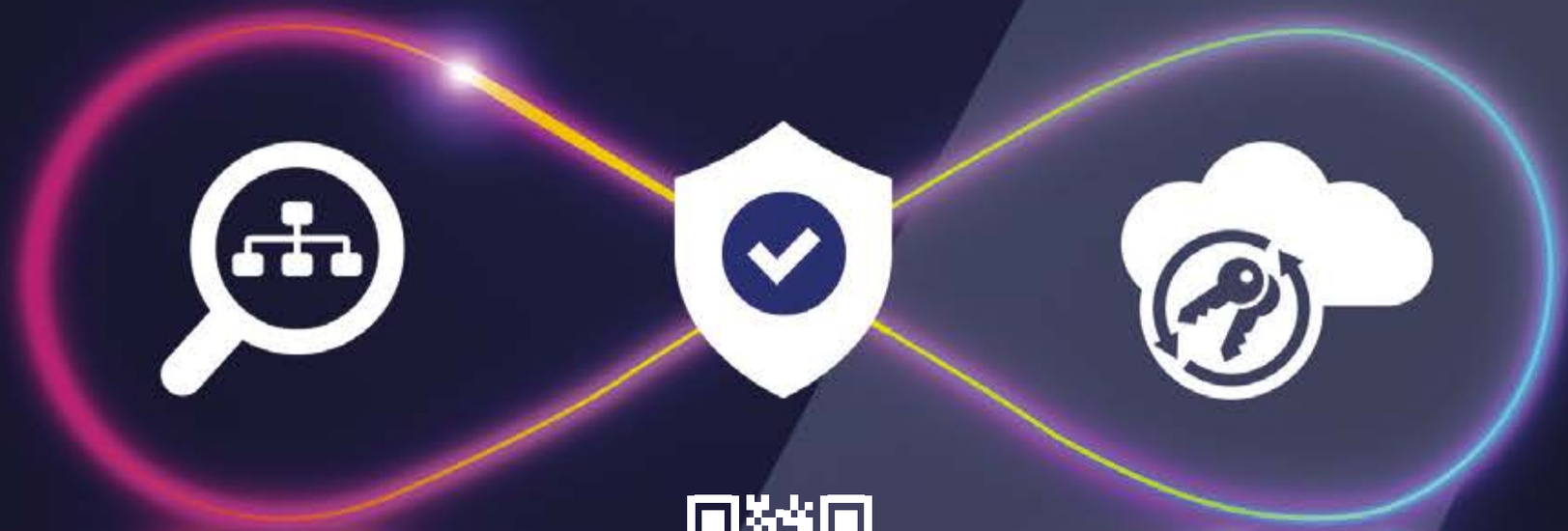
cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

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

Localizar Proteger Controlar



Empiece a localizar, proteger y controlar sus datos hoy mismo

Estados-Nación, licencia para hackear

Una vez limitados a delincuentes oportunistas, los ciberataques se están convirtiendo en un arma clave para los gobiernos que buscan defender la soberanía nacional y proyectar su poder nacional. Hoy, los Estados están detrás del 23% de los ciberataques del mundo. Los ciberataques cuestan muy poco en comparación con las operaciones militares tradicionales; generalmente son más fáciles de realizar, más frecuentes y más variados. Los ciberdelincuentes que están detrás de ellos pueden formar parte de un ciberejército o ser mercenarios, pero saben muy bien el caos que generan y lo poco que arriesgan.

Recientemente se ha publicado un estudio académico titulado "Nation States, Cyberconflic and the Web of Profit" que muestra que los ciberataques de los estados nación son cada vez más frecuentes, variados y abiertos, y que nos están acercando a un punto que bautizan como "ciberconflicto avanzado". Y es que dada la reciente escalada de tensiones en el ciberespacio, la cooperación entre gobiernos se está volviendo cada vez más complicada a medida que los sistemas políticos difieren y la competencia tecnológica aumenta.

Entre otras cosas recoge el informe, elaborado por la University of Surrey y patrocinado por HP Inc., que los ciberataques respaldados por los estados se duplicaron entre 2017 y 2020.

Tras analizar más de 200 incidentes de seguridad relacionados con actividades asociados a estados durante los últimos once años, el estudio no hace sino mostrar un panorama preocupante ante la escalada de tensiones internacionales, sobre todo en 2020, cuando la pandemia de COVID-19 se convirtió en una gran oportunidad para que los estados nación la explotaran.

Dice el Dr. Mike McGuire, Senior Lecturer en Criminology de la University of Surrey, que los datos en realidad no han sorprendido y que los estados nación "están dedicando mucho tiempo y recursos a lograr una ventaja cibernética estratégica para promover sus intereses nacionales, capacidades de recopilación de inteligencia y fuerza militar a través del espionaje, la interrupción y el robo". Añade que los intentos de obtener datos de propiedad intelectual sobre vacunas y los ataques contra las cadenas de suministro de software demuestran "hasta qué punto los estados nacionales están dispuestos a llegar para lograr sus objetivos estratégicos".

El estudio también ha identificado un aumento de ataques a la cadena de suministro. No sólo crecieron un 78% en 2019, sino que entre 2017 y 2020 se identificaron más de 27 ataques de cadena de suministro diferentes asociados a estados nación. Y el de SolarWinds, hecho público a finales del año pasado, podría considerarse uno de ellos. Se ha detectado también que más del 40% de los incidentes analizados tenían algún elemento de hibridación en el sentido de que implican un ataque físico

Lazarus Group tiene entre sus logros el ser responsable del ataque de ransomware Wannacry en 2017 que infectó más de 300.000 dispositivos en todo el mundo

a los activos así como uno digital; los ataques a la infraestructura nacional crítica entrarían en esta categoría.

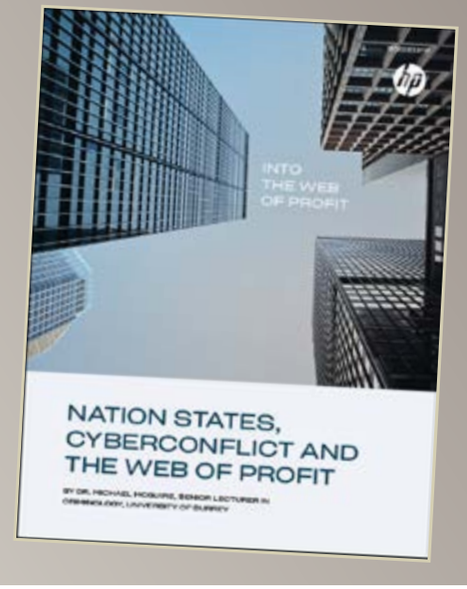
Los gobiernos que actúan de forma maliciosa en el ciberespacio utilizan cada vez más tácticas que ya han sido probadas por los delincuentes organizados, aseguran en el informe, donde también apuntan a que los actores respaldados por el gobierno parecen estar acumulando vulnerabilidades de día cero, ya que el 10-15% de las ventas de los proveedores de la Dark Web ahora se realizan a compradores atípicos o intermediarios para los gobiernos.

En este mercado negro se abren paso las herramientas ofensivas desarrolladas por agencias gubernamentales, siendo el más famoso el exploit EternalBlue utilizado en los ataques de WannaCry. El informe pone de manifiesto que aproximadamente una quinta parte de los ataques respaldados por estados usaban armamento hecho a medida, como malware dirigido probablemente desarrollado internamente, y que la mitad involucraba herramientas sencillas y fáciles de comprar compradas en la Dark Web.

Menciona el Dr. Mike McGuire en su informe que hay una "segunda generación de armamento cibernético en desarrollo que se basa en capacidades mejoradas en potencia de cómputo, inteligencia artificial e integraciones cibernéticas / físicas", y que se están desarrollando Chatbots armados "para entregar mensajes de phishing más persuasivos, reaccionar ante nuevos eventos y enviar mensajes a través de sitios de redes sociales. En el futuro, también podemos esperar ver el uso de deepfakes en el campo de batalla digital, enjambres de drones capaces de interrumpir las comunicaciones o participar en vigilancia, y dispositivos de computación cuántica con la capacidad de

NACIONES ESTADOS, CIBERCONFLICTOS Y LA WEB DEL BENEFICIO

Con programas de investigación dedicados destinados a desarrollar nuevos tipos de ciberataques, el almacenamiento de "exploits" o la combinación de herramientas y técnicas de ataque, ha habido una complejidad significativa en los métodos utilizados por los Estados nacionales para promover estos objetivos estratégicos. A medida que la gravedad, la sofisticación, la escala y el alcance de la actividad del Estado-nación continúan aumentando, debemos reinventar la seguridad para mantenernos a la vanguardia.



Impacto de la ciberguerra

Los siguientes datos ponen de manifiesto el impacto que los ataques procedentes de estados nación tienen no sólo para entornos gubernamentales, sino para cualquier empresa:

- Más del 90% de las alertas de seguridad publicadas por Microsoft sobre ciberataques de estado nación en 2020 advirtieron del peligro contra objetivos no gubernamentales o de infraestructura.
- Cerca del 60% de la actividad de los estados nación se centró en las organizaciones de TI. Los siguientes objetivos más comunes fueron: las instalaciones comerciales, la fabricación crítica, los servicios financieros y la base industrial de defensa.
- El ransomware es la herramienta más utilizada por los ciberdelincuentes de los estados nación.
- El primer semestre de 2020 de detectaron 41.000 intrusiones, una cifra superior a las 35.000 detectadas durante todo 2019, según los investigadores.
- La Interpol detectó alrededor de 907.000 mensajes de spam, 737 incidentes relacionados con malware y 48.000 URL maliciosas con trampas COVID-19 rastreadas hasta grupos de ciberdelincuencia de estados nacionales.
- El 25% de las filtraciones de datos en los últimos 12 meses se han relacionado con el espionaje.

Una quinta parte de los ataques respaldados por estados usan armamento hecho a medida, como malware dirigido probablemente desarrollado internamente

romper casi cualquier sistema encriptado", añade el académico.

Entre las conclusiones recogidas en el informe destaca la llamada a algún tipo de tratado internacional capaz de aliviar las crecientes tensiones y evitar que los estados nacionales se vean arrastrados a ciberataques más hostiles. Según McGuire un tratado de paz cibernética dependería tanto del alcance como del consenso; "cualquier tratado necesitaría especificar las partes incluidas, el rango de jurisdicciones involucradas y la actividad que cubriría".

Licencia para hackear

Pero empecemos por el comienzo, por lo métodos y motivaciones que impulsan los ciberataques de los estados nación. Ya hemos comentado que los ciberdelincuentes que están detrás de este tipo de ataques pueden formar parte de un ejército o estar a sueldo, como los mercenarios. En ambos casos trabajan sin temor a represalias legales, ya que es muy poco probable que sean arrestados en su país de origen por lo que están haciendo, y contarán con las capacidades y recursos del gobierno que les financia.

TOP 7 MOST ELITE NATION STATE HACKERS

CLICAR PARA VER EL VÍDEO

Las empresas ven los ciberataques patrocinados y liderados por el estado como un problema urgente que exige que los gobiernos actúen a nivel nacional e internacional.

Los ataques perpetrados por estos actores están motivados por el nacionalismo y tiene como objetivo obtener secretos de otras naciones o perturbarlas a través de medios online. Por otra parte, los actores detrás de los ataques de estados nación operan de manera encubierta y casi nunca reconocen la propiedad de sus acciones, sino que harán todo lo posible para cubrir sus huellas y hacer que sea lo más difícil posible para los expertos en ciberseguridad rastrear sus campañas hasta su país de origen, a menudo colocando banderas falsas para engañar los esfuerzos de atribución.

Según un artículo publicado por BAE Systems, los responsables de un ciberataque de un estado nación son especialistas con competencia para tareas específicas. Se les asignará la tarea de robar secretos industriales, interrumpir la infraestructura nacional crítica, escuchar las discusiones sobre políticas, derribar empresas que ofendan a sus líderes de alguna manera o realizar campañas de propaganda o desinformación dentro y fuera de las fronteras de su país. Además, utilizarán la ingeniería social para dirigirse a personas vulnerables o de alto perfil con correos electrónicos de spear phishing cuidadosamente elaborados. Alternativamente, pueden comprometer sitios web estratégicos, utilizándolos para ofrecer software malicioso a sus visitantes y engañando a su víctima al hacerlo.

Al contar con una importante cantidad de recursos a su disposición, puede realizar ataques complejos contra hardware específico, como ya ocurrió con el malware Stuxnet, desarrollado presuntamente por Estados Unidos e Israel contra las instalaciones de fabricación nuclear de Irán en Natanz. Y como una extensión del aparato de seguridad del estado, el Actor del Estado-Nación puede tener la tarea de rastrear, interrumpir y perseguir a los disidentes o activistas; otros grupos de Actores del Estado

Nación se especializan en propaganda y desinformación en el ciberespacio, formando ejércitos que luchan contra los medios de comunicación desfavorables, controlados o sesgados para intentar elevar la reputación de sus empleadores.

El temor se extiende

En el pasado, la ciberdelincuencia procedente de un estado era un concepto más distante para las empresas. Si bien siempre han sido una preocupación para la seguridad nacional y una posible amenaza para las infraestructuras críticas, era poco probable que las empresas o los gobiernos locales tuvieran que hacer frente a este tipo de amenazas.

Sin embargo, actualmente la mayoría de las empresas consideran los ataques liderados o patrocinados por los estados como una amenaza importante, según una investigación patrocinada por Cybersecurity Tech Accord y realizada por la Economist Intelligent Unit a partir de entrevistas con más de 500 ejecutivos de nivel de director o superiores de empresas de Asia-Pacífico, Europa y Estados Unidos.

Los ciberataques respaldados por los estados se duplicaron entre 2017 y 2020

Los datos muestras que un 80% de estos ejecutivos está preocupado por ser víctima de un ataque de un estado nacional, y una mayoría afirma que estas preocupaciones han aumentado en los últimos cinco años. Y eso que la encuesta se realizó antes de salir a la luz la brecha de SolarWinds. Además, quieren que sus respectivos gobiernos desempeñen un papel más importante en el cumplimiento de estos desafíos: el 60% dijo que su país solo ofrece un nivel de protección medio o bajo.

Los resultados de este estudio muestran que las empresas ven los ciberataques patrocinados y liderados por el estado como un problema urgente que exige que los gobiernos actúen a nivel nacional e internacional.

SP 800-172, la herramienta del NIST para la defensa de los ataques patrocinados por un Estados Nación

Asegurando que “los ciberataques se llevan a cabo con armas silenciosas y, en algunas situaciones, esas armas son indetectables”, Ron Ross, científico informático y miembro del NIST explicaba a través de un comunicado que fue una brecha realizada en 2018 que comprometió información confidencial federal la que había inspirado directamente el trabajo del equipo de NIST en SP 800-172, que ofrece recomendaciones adicionales para manejar información no controlada clasificada (CUI - controlled unclassified information) en situaciones donde esa información corre un riesgo de exposición más alto que el habitual. CUI incluye una amplia variedad de tipos de información, desde nombres de personas o números de Seguro Social hasta información de defensa crítica.

“Desarrollamos el SP 800-171 en respuesta a los principales ciberataques en la infraestructura crítica de EE. UU., y su documento complementario SP 800-172 está diseñado para mitigar los ataques avanzados como APT”, dijo Ross.

Los requisitos en SP 800-172 se aplican a los componentes de sistemas no federales que procesan, almacenan o transmiten CUI o que brindan protección para dichos componentes. Para reducir aún más el alcance, los requisitos se aplican solo cuando la CUI designada está asociada con un programa crítico o activo de alto valor, la máxima prioridad para la protección.

Desarrollada principalmente para administradores como gerentes de programas, CIO y auditores de sistemas, la publicación aborda la protección de CUI para los componentes del sistema mediante la promoción de una arquitectura resistente a la penetración, operaciones que limitan los daños y diseños para lograr la resistencia y supervivencia cibernéticas. Sus herramientas, divididas en 14 familias, no están pensadas para ser implementadas en masa, sino seleccionadas según las necesidades de la organización.

Los intentos de obtener datos de propiedad intelectual sobre vacunas y los ataques contra las cadenas de suministro de software demuestran hasta qué punto los estados nacionales están dispuestos a llegar para lograr sus objetivos estratégicos

A pesar de que dos tercios de los ejecutivos (68%) creen que sus organizaciones están “muy” o “completamente” preparadas para tratar con un ciberataque, hay que tener en cuenta que las bandas de ciberdelincuencia de un estado-nación son especialmente problemáticas para las empresas porque son sofisticados, experimentados e innovadores, con manuales profundos y acceso a tecnología de vanguardia para facilitar sus ataques; son pacientes y están dispuestos a hacer un trabajo lento y personalizado para eliminar los objetivos correctos.

Actualmente la ciberdelincuencia de los estados es un problema de todos e impactan directamente en nuestra vida cotidiana. Aunque el robo de datos suele ser el propósito, no es el único objetivo de estos actores de amenazas, les gusta ir un paso más allá, utilizando herramientas como ransomware y otro malware para cerrar la fabricación, interferir con la logística e interrumpir investigaciones importantes. Están especialmente predispuestos a abrirse camino más allá de la seguridad de una empresa al colarse a través de un proveedor externo o en la cadena de suministro.

Los grupos más conocidos

Como hemos dicho, los ataques de actores patrocinados por el estado no se realizan exclusivamente contra organizaciones gubernamentales, instalaciones nucleares y bases militares. Los disidentes, los opositores políticos así como las empresas privadas que incluyen a las instituciones públicas como sus clientes tienen la misma probabilidad de ser blanco de grupos de piratas informáticos respaldados por un estado.

Las empresas de seguridad siguen cuidadosamente la labor de estos grupos de ciberdelincuentes patrocinados por los estados, que a menudo reciben diferentes nombres. FireEye, por ejemplo, los bautiza con las siglas APT, de Advanced Persistent Threat, seguido de un número. De forma que APT29 también son conocidos como Cozi Bear; APT38 como Lazarus Group; APT41 como Double Dragon, o APT28 como Fancy Bear.

Fancy Bear

También conocido por APT28, Strontium o Sednit, se cree que Fancy Bear opera desde Rusia. Destacan por el buen uso que hace en spear phishing. Fancy Bear se ha dividido en diferentes subgrupos, cada uno de los cuales es responsable de una parte diferente del ataque, de forma que un subconjunto se centra en la suplantación de identidad en tantos objetivos como sea posible mientras que otro está especializado en mantener la persistencia.

Según CrowdStrike, Fancy Bear “ha dedicado un tiempo considerable al desarrollo de su implante primario conocido como XAgent y a aprovechar

Stuxnet, el malware que cambió las reglas del juego

Hablamos de ciberdelincuentes y ciberataques patrocinados por estados y lo habitual es pensar en Rusia, China, Corea del Norte, Irán, Europa del Este... pero Estados Unidos e Israel también son jugadores importantes en este nuevo mundo de ciberguerra. De hecho, son muchos los expertos que opinan que hay un antes y un después de Stuxnet, que este virus lo cambió todo.

Stuxnet fue un malware atribuido a Estados Unidos e Israel y desarrollado para ir contra las instalaciones nucleares iraníes. Su descubrimiento en 2010 cambió el juego. De repente, los estados se dieron cuenta de que podían utilizar ciberataques para lograr sus objetivos políticos, comerciales y militares.

La compañía de seguridad Kaspersky Lab describió a Stuxnet en una nota de prensa como “un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial” y que los ataques sólo pudieron producirse “con el apoyo de una nación soberana”, convirtiendo a Irán en el primer objetivo de una guerra cibernética real.

> Los ciberdelincuentes patrocinados por los estados trabajan sin temor a represalias legales y cuentan con las capacidades y recursos del gobierno que les financia

herramientas como X-Tunnel, WinIDS, Foozer y DownRange".

En 2020, el grupo supuestamente llevó a cabo decenas de ataques cibernéticos contra múltiples agencias federales de EE. UU.

Lazarus Group

También conocido como APT38, DarkSeoul o Hermit, este grupo de hackers respaldado por el régimen norcoreano de Pyongyang tiene entre sus logros el ser responsable del ataque de ransomware Wannacry en 2017 que infectó más de 300.000 dispositivos en todo el mundo.

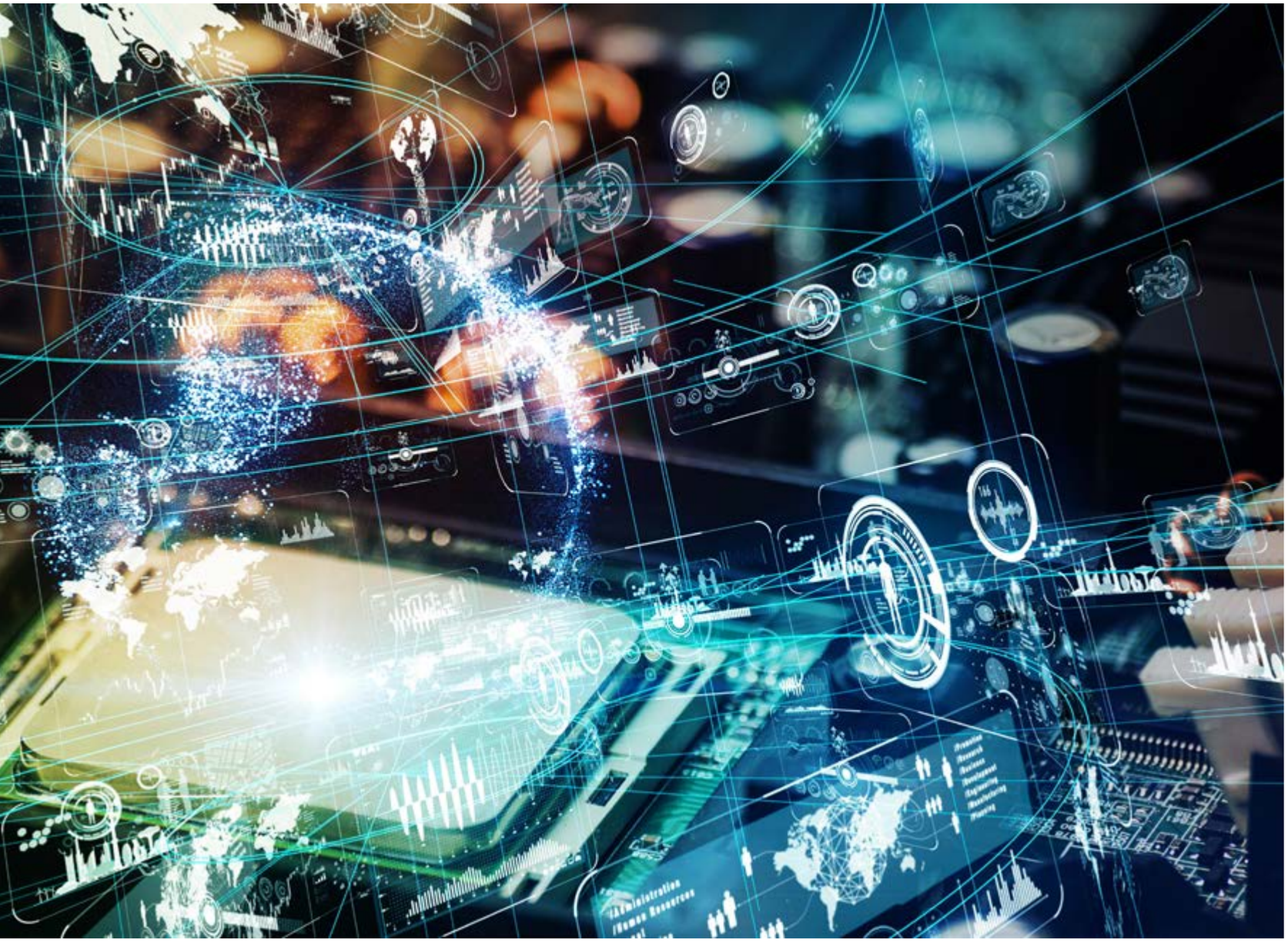
La última redada a gran escala del grupo involucró ataques a una compañía farmacéutica y un ministerio de sanidad en un intento de robar datos de la vacuna COVID-19. Expertos de Kaspersky sospechan que los piratas informáticos robaron los datos de la empresa farmacéutica al implementar el malware Bookcode en un ataque a la cadena de suministro a través de otra empresa, mientras que los servidores del ministerio se vieron comprometidos al instalar wAgent, un sofisticado programa de malware sin archivos que obtiene cargas útiles maliciosas adicionales de un servidor remoto.

Se asegura además que si bien la mayoría de los grupos respaldados por los estados nación limitan sus actividades al espionaje o la destrucción, la práctica adicional del delito cibernético financiero parece ser exclusiva de Corea del Norte.

Double Dragon

También conocido como APT41 o Cicada, se cree que este grupo opera desde China. Activo desde 2012 se le atribuye una campaña masiva de piratería global en 2020 que incluye operaciones de espionaje contra 14 países diferentes, incluidos Estados Unidos y Reino Unido.

Desde sus primeros avistamientos por expertos en seguridad, se ha observado a Double Dragon realizando una amplia gama de operaciones, desde ataques a la cadena de suministro y exfiltración de



datos, así como el uso de complejas herramientas patentadas.

Además de atacar directamente a las instituciones gubernamentales, Double Dragon también está apuntando a empresas privadas en las industrias de viajes y telecomunicaciones para acceder a datos que pueden usar para operaciones de vigilancia. Según FireEye, Double Dragon "también lleva a cabo una actividad explícita motivada financieramente, que ha incluido el uso de herramientas que de otro modo se utilizan exclusivamente en campañas que apoyan los intereses del estado". En otras palabras, el grupo utiliza herramientas de espionaje de primer nivel para robar dinero para sí mismos "fuera de sus trabajos habituales".

Diversificando las tácticas

A finales del año pasado Accenture publicó su informe 2020 Cyber Threatscape Report en el que destacó que algunos de ciberdelincuentes patrocinados por el estado y las bandas de ransomware más notorias están desplegando un arsenal de nuevas herramientas para realizar sus fechorías. No sólo menciona el uso de herramientas listas para usar, infraestructura de alojamiento compartido, código de explotación desarrollado públicamente, sino pruebas de penetración de código abierto para llevar a cabo ciberataques y ocultar sus huellas.

Tras rastrear a un grupo de ciberdelincuentes con sede en Irán conocido como Sourface, activo desde al menos desde 2014 y conocido por sus ciberataques en las industrias de petróleo y gas, comunicaciones, transporte y otras en los EE. UU., Israel, Europa, Arabia Saudita, Australia y otras regiones, los analistas de Accenture CTI observaron que Sourface utiliza funciones legítimas de Windows y herramientas disponibles gratuitamente como Mimikatz para el volcado de credenciales. Esta técnica se utiliza para robar credenciales de autenticación de usuarios y permitir que los atacantes escalen privilegios o se muevan a través de la red para

comprometer otros sistemas y cuentas mientras se disfrazan como un usuario válido.

Según el informe, es muy probable que los actores sofisticados, incluidos los grupos delictivos organizados y patrocinados por el estado, continúen utilizando herramientas de prueba de penetración y listas para usar en el futuro previsible, ya que son fáciles de usar, efectivas y económicas.

El informe señala también cómo un grupo notorio se ha dirigido agresivamente a los sistemas que admiten Microsoft Exchange y Outlook Web Access, y luego utiliza estos sistemas comprometidos dentro del entorno de una víctima para ocultar el tráfico, transmitir comandos, comprometer el correo electrónico, robar datos y recopilar credenciales para el espionaje. El grupo, al que Accenture se refiere como Belugasturgeon (también conocido como Turla o Snake), opera desde Rusia, ha estado activo durante más de 10 años y está asociado con numerosos ciberataques dirigidos a agencias gubernamentales y firmas de investigación de política exterior de todo el mundo.

Enlaces de interés...

- Ciberataques del Estado-nación: SolarWinds, Microsoft solo el comienzo
- NIST ofrece herramientas para ayudar a defenderse de los ciberdelincuentes patrocinados por el estado
- W World War C: Entendiendo los motivos del Estado-nación detrás de los ciberataques avanzados de hoy
- W Estados Nación: por qué hackean
- W 2020 Cyber Threatscape

Compartir en RRSS

ACCEDIENDO A UNA NUBE SEGURA

LA CONEXIÓN EN LA NUBE NO SIGNIFICA MENOS PROTECCIÓN

ENTRUST

it Digital Security
Tribuna W4C Spain

Trabajar desde los cimientos para construir un futuro diverso e inclusivo en la ciberseguridad

BEGOÑA GARCÍA

MIEMBRO DEL CONSEJO WOMEN4CYBER SPAIN

Ingeniera Informática por la Universidad Pontificia de Salamanca (Madrid), Begoña García tiene más de 20 años de experiencia en diferentes campos de la ciberseguridad. Actualmente forma parte del equipo de Corporate Security en BBVA en el que desempeña la función de cultura y concienciación de seguridad para todo el Grupo. Trabajó en el equipo de Prevención de Fraude Tecnológico y durante varios años lideró el equipo de monitorización y respuesta BBVA CERT. Es miembro del Consejo de Women4Cyber Spain, el capítulo nacional dependiente de la Fundación Women4Cyber de la European Cyber Security Organization.

Compartir en RRSS

Según datos de la UNESCO sólo un 30% de las mujeres del mundo estudia carreras "STEM" (porcentaje que se reduce hasta el 3% en carreras relacionadas con tecnologías de la información o el 8% en carreras de ingeniería).

Según los informes publicados por el (ISC)2, en 2013 sólo el 11% de los puestos de la industria de la ciberseguridad se ocupaban por mujeres, frente a cerca de la cuarta parte de la fuerza laboral que se contabilizaron en 2020 por esta misma organización. Un dato muy positivo debido al crecimiento en el sector de la ciberseguridad en los últimos años, aunque muy revelador en cuanto al camino que aún queda por recorrer para alcanzar un sector más equitativo.

Según la AAUW (American Association of University Women) los motivos por los que se dan estas desigualdades son principalmente los estereotipos de género, la escasez de "role model" femeninos y los entornos profesionales masculinos.

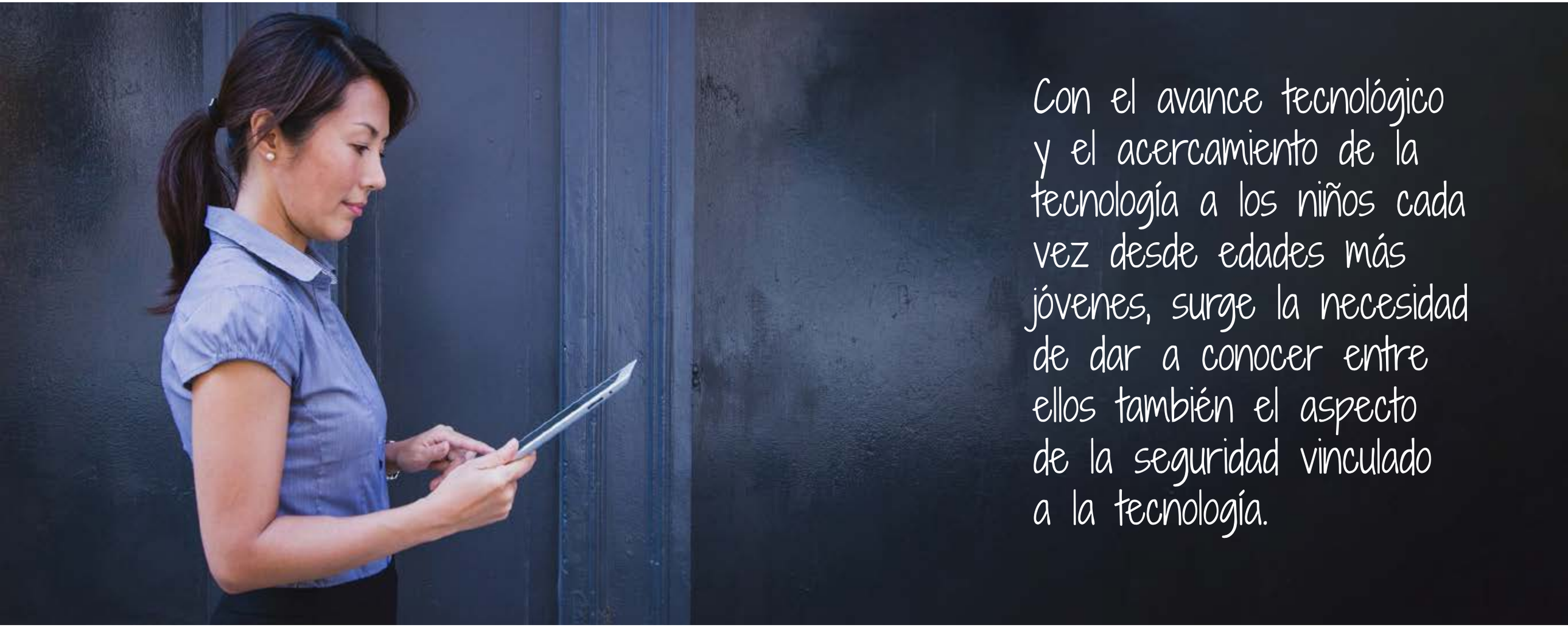
La educación clave para el desarrollo de la sociedad

La ciencia y la igualdad de género son esenciales para el desarrollo sostenible. Un factor esencial para seguir avanzando en este camino y conseguir más presencia de la mujer en las STEM, y en particular en el sector de la ciberseguridad, es la educación. La educación es la base para corregir las desigualdades y que permite crecer sin sesgos de género que puedan limitar a las mujeres a acceder a carreras STEM o puestos tecnológicos.

Además de ser el vehículo para el desarrollo de las personas, para adquirir habilidades y conocimientos, con la educación también se aprenden conductas y se adquieren los valores fundamentales. Debemos verla por tanto como una herramienta para conseguir el desarrollo de la sociedad, esencial para alcanzar una sociedad concienciada y conocedora de los riesgos a los que nos enfrentamos en el mundo digital, y por otro lado también para alcanzar un futuro más diverso e inclusivo.

Enseñar a las generaciones más jóvenes para crear un futuro digital seguro

La digitalización, la tecnología, y las RR. SS traen consigo nuevos retos pero también riesgos y amenazas, para los que las nuevas generaciones tendrán que estar preparados. Los jóvenes, que nacen con la tecnología entre las manos, deben aprender a hacer un uso responsable de la tecnología y RR. SS, aprender a ser críticos con lo que reciben y con lo que publican. Con el avance tecnológico y el acercamiento de la tecnología a los niños cada vez desde edades más jóvenes, surge



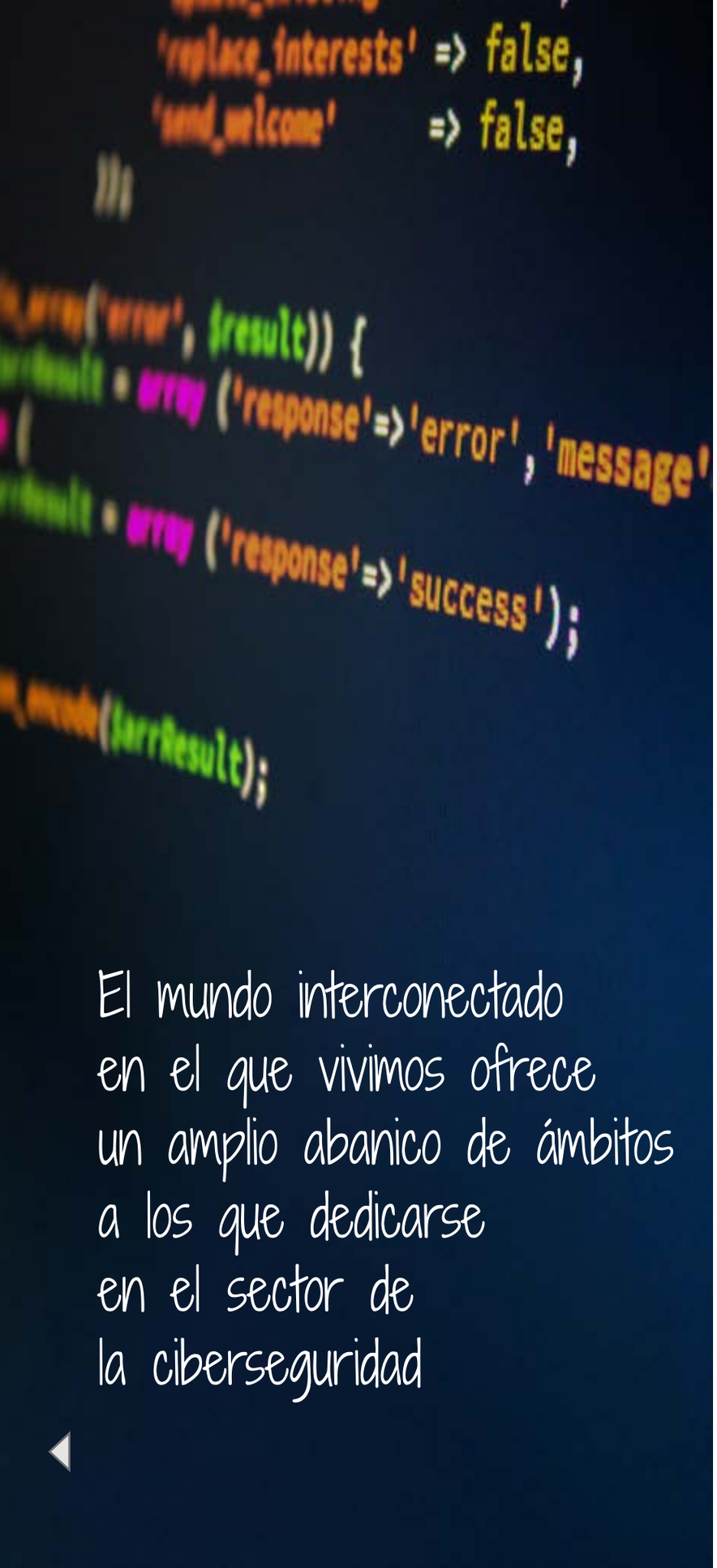
la necesidad de dar a conocer entre ellos también el aspecto de la seguridad vinculado a la tecnología. Esto supone una gran oportunidad para incorporar una cultura de ciberseguridad entre ellos. Conocer los riesgos, saber manejarlos, desarrollar pensamiento crítico, son algunas de las capacidades que se tendrán que desarrollar para conseguir una sociedad conocedora y concienciada de los riesgos del mundo digital.

El sector de la ciberseguridad una oportunidad para dedicarse a futuro

Si hablamos del ámbito laboral en la ciberseguridad según el World Economic Forum, en su informe "The Future of World Report 2020" sitúa la encriptación y ciberseguridad, junto con otras como Big Data, Inteligencia Artificial y Cloud Computing, como las tecnologías en las que se prevé mayor crecimiento en las empresas en los próximos años.

En 2025 más del 70% de las medianas y grandes empresas de todos los sectores implementarán servicios de ciberseguridad. La industria de la ciberseguridad tiene por delante el gran reto de hacer frente a esta necesidad de creciente demanda de profesionales en el sector de la ciberseguridad a futuro.

La previsión de aumento de la demanda de profesionales para cubrir puestos de trabajo relacionados con la ciberseguridad supone una



oportunidad para dar a conocer este sector como una opción profesional a la que dedicarse.

El sector de la ciberseguridad ha experimentado una gran evolución con el avance de la tecnología, la digitalización y las RR. SS. Hoy en día el mundo interconectado en el que vivimos ofrece un amplio abanico de ámbitos a los que dedicarse en el sector de la ciberseguridad, no sólo tecnológicos, sino también otros como por ejemplo los más cercanos a los riesgos relacionados con el factor humano, como la formación, la concienciación o la comunicación. Esto ha hecho que se convierta en una ámbito profesional lleno de oportunidades para perfiles muy diversos.

Los cimientos para construir un futuro más concienciado, más formado para afrontar las necesidades futuras y más equitativo

Todos estos aspectos suponen una gran oportunidad para construir un futuro digital más seguro. Para dar a conocer la ciberseguridad y generar interés entre los jóvenes, y hacer de la ciberseguridad un sector en el que poder adquirir conocimientos y habilidades para desarrollarse profesionalmente con oportunidades y futuro. Y para eliminar desigualdades, disminuir la brecha de género y generar oportunidades para todos.

W4C lanza varias líneas de trabajo con las que consideramos se contribuye a la labor de impulsar la inclusión y la diversidad en el sector y fomentar la ciberseguridad desde edades tempranas:

- **Divulgar y representar el rol femenino en el sector de la ciberseguridad, así como ayudar a visibilizar los distintos proyectos e iniciativas en los que participan mujeres del sector de la ciberseguridad.** De esta forma podemos contribuir a motivar e inspirar a otras mujeres para que puedan verse reflejadas en estos roles para fomentar la participación y el atractivo hacia este sector.
- **Animar a la comunidad W4C a impulsar, compartir y visibilizar la ciberseguridad.**
- **Brindar el apoyo de personas con experiencia mediante nuestro programa de mentoring.** A través de procesos de orientación profesional, se puede ayudar a que las más jóvenes tengan toda la información a la hora de decidirse para realizar carreras STEM e incluso, contribuir al desarrollo de sus carreras profesionales o hacia qué ámbito de la ciberseguridad quieren enfocarse.
- **Facilitar el acceso a redes profesionales y promover iniciativas para fomentar las carreras tecnológicas entre las niñas y adolescentes a través de fundaciones con este mismo objetivo para conectarlas con el mundo de la tecnología y de la ciberseguridad.**

Enlaces de interés...

- Women4Cyber Spain
- American Association of University Women
- ‘Hay una voluntad real de que haya más diversidad’ (Eduvigis Ortiz)

Mejorando la experiencia del trabajador remoto

10 de junio · 11:00 h CET

REGISTRO

#EncuentrosITTrends

it TRENDS

JOSÉ CANO

DIRECTOR DE ANÁLISIS Y CONSULTORÍA DE IDC ESPAÑA

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

La ciber resiliencia y su papel en el diseño de una estrategia de ciberseguridad

Mayo 2021

Cuando nos referimos a resiliencia, queremos enfatizar la capacidad del ser humano para adaptarse a las situaciones adversas con resultados positivos. Proviene del término latín *resilio*, «volver atrás, volver de un salto, resaltar, rebotar», y se ha utilizado en psicología y otras ciencias sociales para referirse a la capacidad de la empresa o persona que, a pesar de haber sufrido situaciones estresantes, no son afectadas por ellas.

Así, el término ciber resiliencia hace referencia a la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes. En este sentido, las empresas deben estar preparadas para dar respuestas rápidas a los ataques. El objetivo debe ser tratar que los servicios que prestan no se vean paralizados o suspendidos, por lo que es esencial fortalecer sus capacidades de identificación, detección, contención, recuperación, cooperación y mejora continua para hacer frente a todo tipo de amenazas.

Por ello, es necesario no sólo garantizar la adopción de la ciber resiliencia como punto de partida, combinándola con otras estrategias como las arquitecturas de confianza cero (Zero Trust). La dramática fuerza del cambio, impulsada por el COVID-19, y la migración masiva de empleados a sus hogares, no tiene precedentes. La pandemia COVID-19 ha llevado a las empresas a movilizarse en torno al trabajo desde el hogar (*Working from Home* ó WFH) para frenar la propagación del virus, la atención y bienestar de los empleados y garantizar la continuidad del negocio.

"Los análisis de seguridad se deberán utilizan constantemente para evaluar el estado y la actividad en todo el entorno, identificando amenazas y otras actividades malintencionadas"

Esta nueva realidad, obliga a repensar las políticas de seguridad de la organización incorporando los propios hogares (y dispositivos en muchas ocasiones) de los empleados dentro del perímetro de seguridad. Se requiere por tanto abordar la problemática del consumo de la seguridad y cómo

este cambio conlleva a su vez nuevos desafíos en la política de seguridad de las organizaciones (acceso y consumo de servicios y aplicaciones), así como en la relación con el ecosistema de proveedores.

Los servicios en la nube pueden ayudar a alcanzar los objetivos de negocio creando, desplegando y gestionando las cargas de trabajo en un entorno multicloud integrado con la infraestructura tradicional. A medida que las infraestructuras estrechamente integradas se sustituyen por servicios gestionados y modulares en un entorno de nube híbrida privada y/o pública, las cargas de trabajo deben migrarse, optimizarse y habilitarse para obtener ventajas competitivas de las aplicaciones en la nube. Es en este escenario donde garantizar la seguridad del dato se vuelve cada vez más complejo y necesario.

Según datos de IDC, el 70% del tiempo del personal de ciberseguridad se destina a la gestión de herramientas y aplicativos de seguridad. Por ello, evolucionar hacia una plataforma de ciberseguridad integral, o racionalizar el entorno de seguridad fomentando la automatización y la respuesta proactiva ante incidentes resulta una prioridad para las empresas en la búsqueda de la ciber resiliencia deseada.

En la actualidad, el 90% de las empresas españolas afirma disponer de un modelo de cloud híbrida (on prem con algún tipo de nube, y con múltiples servicios en la nube). En este escenario, el consumo de la seguridad como servicio lleva al establecimiento de un marco unificado de seguridad, donde la postura de seguridad de los activos y recursos del ecosistema se debe fortalece a través de técnicas de gestión de vulnerabilidades y reevaluarse y actualizarse constantemente a través de procesos

"Las empresas deben estar preparadas para dar respuestas rápidas a los ataques"

"Evolucionar hacia una plataforma de ciberseguridad integral resulta una prioridad para las empresas en la búsqueda de la ciber resiliencia deseada"

orquestados. Los orígenes de actividad, como los usuarios y los dispositivos, se deberán autentican mediante credenciales que se aprovisionen y administren en función de las necesidades, aplicándose políticas adecuadas al uso de los datos y las aplicaciones.

Los activos de TI, por tanto, deben aprovechar los certificados de confianza que apliquen medidas criptográficas para garantizar la confidencialidad e integridad de los datos a medida que fluyan por todo el entorno. Por último, los análisis de seguridad se deberán utilizan constantemente para evaluar el estado y la actividad en todo el entorno, identificando amenazas y otras actividades malintencionadas que se puedan abordar a través de acciones de respuesta para mantener un entorno resistente.

Solo de esta forma, la empresa estará en condiciones de poder afrontar una estrategia de ciber resiliencia que habilite a la empresa a reaccionar de una manera ágil y fuerte ante cualquier incidente de seguridad. Todo ello en un entorno donde hemos visto que el progresivo desplazamiento de los modelos de TI de las organizaciones al entorno cloud y el consumo de cada vez más servicios en diferentes nubes está motivando el desarrollo de productos, servicios y experiencias de usuario que están basadas en datos.

Esta securización del dato requiere un cambio profundo en la forma en la que las empresas se enfrentan a este desafío en un entorno multicloud, donde la frontera de seguridad se difumina y el riesgo digital adquiere cada vez más importancia. La cuantificación de este riesgo digital es la principal clave para que la organización pueda estructurar una estrategia de ciberseguridad adecuada que posteriormente pueda integrar en su plataforma digital.

Enlaces de interés...

- Solo el 17% de las organizaciones se consideran 'líderes' en ciberresiliencia
- La mitad de los empleados no técnicos no informan de las amenazas que encuentran

it User
TECH & BUSINESS

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.

Redes Zero Trust:

El aislamiento y la bidireccionalidad

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

La filosofía de diseño de redes basas en los principios Zero Trust persigue un objetivo sencillo de entender: Evitar la posibilidad de que un paciente cero dentro de una red pueda propagar su carga activa al resto de los elementos de la red.

Es decir, una Red Zero Trust tiene exactamente la misma posibilidad que una red normal de tener una máquina infectada. Pero cuando se da este evento, las redes “normales” confían en que los mecanismos de seguridad eviten la propagación al resto de los sistemas. Sin embargo una Red Zero Trust impide por su propio diseño que exista propagación al resto de la red.

La diferencia principal entre estos dos modelos es que todo sistema de protección tiene posibilidad de fallos debido bien a errores de configuración o a la aparición de vulnerabilidades.

Cuando una red se protege por diseño siguiendo modelos Zero Trust no está sujeta a errores de gestión y no pueden aparecer vulnerabilidades que le afecten, salvo las propias de los elementos que estructuran la propia red.

Pero… ¿cómo debería ser la morfología de una red Zero Trust?

Hay que poner en marcha tres reglas básicas en el diseño de las redes Zero Trust.

Una Red Zero Trust tiene exactamente la misma posibilidad que una red normal de tener una máquina infectada, pero impide por su propio diseño que exista propagación al resto de la red

Separar los puestos de trabajo de los servidores que les dan servicio.

Las redes de los puestos de trabajo deberían estar separadas de las redes en la que se ubiquen los servidores que les den servicio como los Active Directory, Samba, Discos compartidos, proxy…

Entre los puestos de trabajo y los servidores debe ubicarse algún tipo de elemento de control que impida la visibilidad directa entre ellos.

¿Cómo reduce esta medida la capacidad de propagación de un paciente cero?

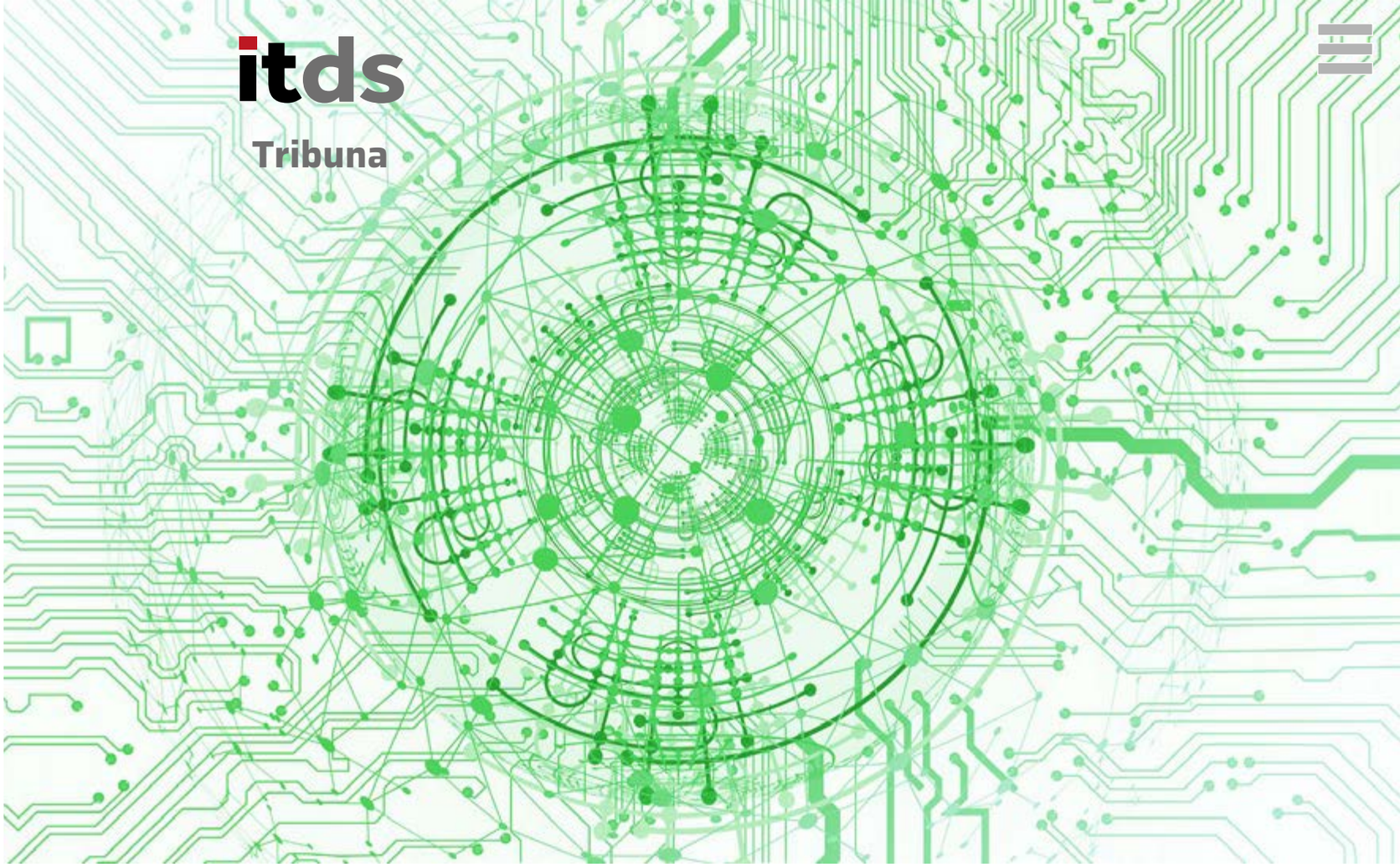
Aunque pueda parecer obvio, los puestos de trabajo solo deben alcanzar a los servidores que les dan servicio a través de los puertos y los protocolos específicos que necesitan para su trabajo, debiendo están específicamente bloqueados todos los demás puertos y protocolos.

Recordemos en este punto que todo lo que no es intrínsecamente necesario debe estar específicamente prohibido.

Impedir la visibilidad entre los puestos de trabajo.

Todas las redes deben estar configuradas de tal manera que los elementos que las integran no tengan visibilidad entre ellas. Especialmente las redes de puestos de trabajo.

Este principio de diseño de redes Zero Trust muchas veces es difícil de conseguir ya que la forma de diseñar históricamente la comunicación entre los sistemas daba por hecho la visibilidad entre ellos.



Aún hoy nos encontramos con docenas de elementos en nuestras redes que requieren tener una visibilidad muy amplia de los elementos con los que deben comunicarse. Los ingenieros de comunicaciones y sistemas se encuentran a veces con retos complejos de gestionar para cumplir con este principio. Pero no deberíamos dejar de afrontarlo por complejo que pueda parecer.

¿Cómo reduce esta medida la capacidad de propagación de un paciente cero?

Parece evidente. Una red donde los elementos no tienen, por diseño, visibilidad entre ellos va a complicar mucho, no sólo la propagación de un paciente cero, sino los movimientos laterales que requieren habitualmente ataques más sofisticados no basados en propagación de malware.

Impedir la bidireccionalidad entre puestos de trabajo y servidores

Con las dos medidas anteriores tenemos mermada la capacidad de propagación por un lado entre servidores y puestos de trabajo, y por otro lado anulada la propagación entre elementos (especialmente puestos de trabajo) dentro de la misma red.

Una vez separados los servidores de los puestos de trabajo, nos toca trabajar sobre las reglas de comunicación entre ambos.

Es fundamental eliminar la bidireccionalidad entre puestos de trabajo y servidores.

Podemos agrupar los servidores en dos tipos:

- **Los que son accedidos por los puestos de trabajo.**

Todo lo que no es intrínsecamente necesario debe estar específicamente prohibido

- **Los que aceden a los puesto de trabajo.**

Dentro de nuestros modelos arquitectónicos utilizados para diseñar redes, deberíamos considerar tres tipos de redes excluyentes, las dos anteriores más las redes de los puestos de trabajo.

Es decir, la comunicación entre las redes de puestos de trabajo y las redes de servidores siempre debería ser unidireccional:

- **Si una red de puestos de trabajo puede acceder a una red servidores, esta no puede acceder a la red de los puestos.**
- **Si una red de servidores puede acceder a una red de los puestos de trabajo, esta última no puede acceder a esa red de servidores.**

No pueden estar mezclados en la misma red los servidores que necesitan acceder a las redes de los puestos de trabajo (como servidores de Backup, monitorización, gestión de los puestos…) con los servidores que son accedidos por los puestos de trabajo (AD, LDAP, correo, NAS…)

¿Cómo reduce esta medida la capacidad de propagación de un paciente cero?

Enlaces de interés...

- Desayuno ITDS. Afrontando el modelo Zero Trust
- La seguridad 'Zero Trust' moverá 51.600 millones de dólares en cinco años
- Zero Trust: en qué consiste y por qué es ahora más relevante que hace un año

> Todas las redes deben estar configuradas de tal manera que los elementos que las integran no tengan visibilidad entre ellas

La utilidad de esta medida es menos evidente que la de los dos casos anteriores, aunque es fundamental para no anular la aportación positiva de ambas.

Esta media persigue evitar que un paciente cero en un puesto de trabajo puede utilizar como elemento de propagación un servidor al que deba tener acceso para su funcionamiento normal, y que este a su vez, si es contagiado, pueda generar una propagación masiva al resto de los puestos de trabajo. Este es un modelo de propagación utilizado por múltiples malware.

Siguiendo estos tres mecanismos de diseño de redes Zero Trust no sólo reduces drásticamente la capacidad de propagación de un paciente cero, sino que simplificas mucho la complejidad de las reglas de seguridad entre las redes de puestos de trabajo y las redes de servidores.

El volumen de trabajo que genera la implantación de estas medidas en grandes redes hace que haya pocos proyectos en la industria de transformación de redes a modelos Zero Trust. Pero si en algún momento vuestra empresa aborda algún proyecto SDN o de migración a la nube, no lo dudéis… ¡Es el momento de aplicarlas!


it Reseller
TECH&CONSULTING
El puesto de trabajo
se reinventa más allá del dispositivo
nº 67
MAYO 2021
La era del IoT impulsa la demanda de soluciones de ciberseguridad
Reina el optimismo en las empresas TIC a pesar de la caída de la facturación
La distribución de TI en España finalizó 2020 con una subida del 20%
it Reseller
TECH&CONSULTING
Cada mes en la revista,
cada día en la web.

it Digital Security
Tribuna Tecnología y Negocio

Escasez de chips y lucha por el podio entre Intel, Nvidia, Samsung, Apple, AMD, TSMC y Qualcomm

JORGE DÍAZ-CARDIEL

SOCIO DIRECTOR GENERAL DE ADVICE STRATEGIC CONSULTANTS

Economista, sociólogo, abogado, historiador, filósofo y periodista. Autor de más de veinte mil de artículos de economía y relaciones internacionales, ha publicado más de una veintena de libros, cinco sobre Digitalización. Ha sido director de Intel, Ipsos Public Affairs, Porter Novelli International, Brodeur Worldwide y Shandwick Consultants.

El gigante de chips gráficos Nvidia está aumentando la presión competitiva sobre Intel con planes para comenzar a vender unidades de procesamiento central (CPU) y atender al floreciente mercado de centros de datos. Nvidia dijo que su primer procesador para data centers funcionaría 10 veces más rápido que los chips de Intel. Llamado Grace, en honor a la famosa científica de la computación y militar norteamericana, Grace Hopper, el chip se basa en tecnología desarrollada por ARM, el diseñador de chips del Reino Unido que Nvidia está en proceso de compra por 40.000 millones de dólares.

El nuevo chip pone a Nvidia, con sede en Santa Clara, California, conocida por sus veloces procesadores que impulsan el hardware de los videojuegos, en plena competencia con Intel, que domina el mercado global en el suministro de chips a los data centers, según Mercury Research. Advanced Micro Devices (AMD) está situado en muy un distante segundo lugar en cuanto a chips para centros de datos.

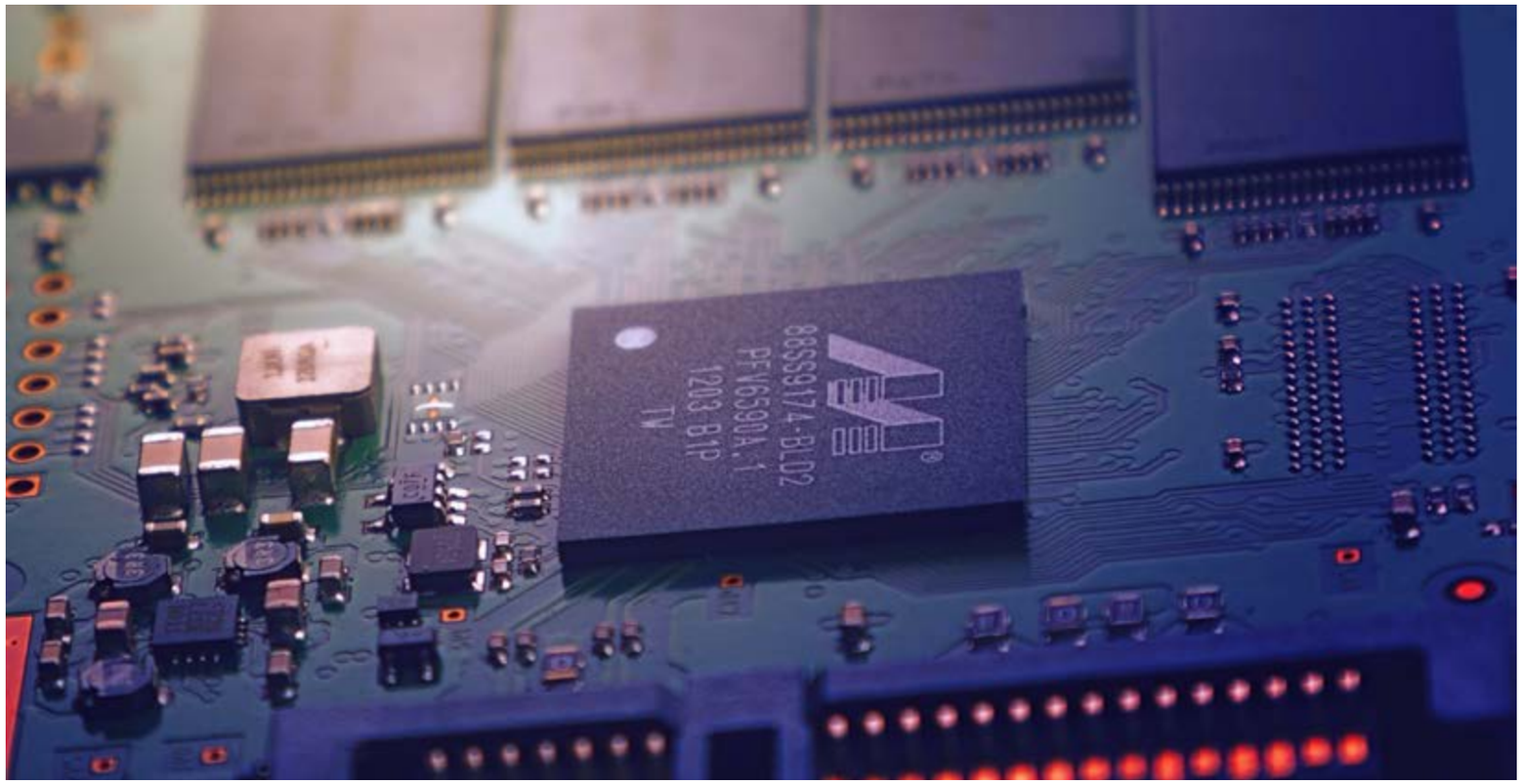
La competencia aprieta: en 2020 Nvidia superó a Intel como el mayor fabricante de chips por valor de mercado en bolsa. Sus acciones se han disparado debido a su apuesta por algunos de los campos más candentes de la tecnología, los videojuegos y la Inteligencia Artificial.

Según Nvidia, el chip Grace -que a Intel y a AMD no les hace nada de grace- tiene como objetivo poder manejar un segmento específico de la informática donde los procesadores necesitan analizar grandes conjuntos de datos rápidamente, un proceso que requiere un rendimiento informático rápido y una memoria masiva. Se puede utilizar para tareas como el procesamiento del lenguaje y la Inteligencia Artificial.

El valor de mercado de Nvidia se ha disparado a 319.800 millones, superando la valoración de Intel de 214.500 millones, a pesar de que Nvidia tuvo 10.920 millones en ventas anuales en su último año fiscal, en comparación con 71.970 millones de Intel, siete veces más. El enfado en Intel fue tan

¿A QUÉ SE DEBE LA ESCASEZ DE CHIPS? ¿QUÉ PROVOCA?

CLICAR PARA VER EL VÍDEO



Muchas de las principales empresas de tecnología y fabricantes de chips se han movido a un modelo en el que solo diseñan chips, pero recurren a fábricas asiáticas de TSMC y Samsung para fabricarlos

gordo que, entre otros motivos, por esto, cambiaron en febrero de CEO.

Y, hasta aquí todo… casi normal: business as usual y competencia entre Intel y Nvidia y AMD. Pero el contexto, la madre del cordero, es la escasez de chips, que afecta tanto a quien los fabrica como a sus clientes, desde electrónica de consumo e informática a la industria del automóvil que, por falta de componentes, han tenido que retrasar la fabricación temporalmente, perdiendo miles de millones de dólares.

En EE.UU., Joe Biden se reunió el 12 de abril con representantes de la industria de semiconductores para presentar su propuesta de infraestructura de 2,3 billones de dólares, dentro de la cual, prevé dedicar una partida específica para impulsar la fabricación de microprocesadores, chips y semiconductores en América, “Made in América”. “Siempre he dicho que, respecto a las Tecnologías de la Información (TIC), China y el resto del mundo NO nos están esperando”, señalaba, y añadía que “no hay ninguna razón por la que los estadounidenses deban esperar. Estamos invirtiendo agresivamente en áreas como semiconductores y baterías; eso es lo que están haciendo ellos y otros, también debemos hacerlo nosotros”. Obvio.

Biden habló con los CEO de Ford Motor, General Motors, Intel, Alphabet (Google, YouTube) y otros fabricantes (Apple, a pesar de fabricar ahora sus chips, abandonando a Intel, como anticipamos aquí en IT User hace un año, no cualifica como fabricante de chips todavía, para el gobierno norteamericano…) para abordar la escasez global de chips, que ha provocado una desaceleración de la producción con la fabricación de automóviles y otras industrias, incluida la de fabricantes de ordenadores, tabletas y smartphones, entre otras.

¿POR QUÉ SE HA PRODUCIDO UNA ESCASEZ GLOBAL DE CHIPS?

CLICAR PARA VER EL VÍDEO

La escasez mundial de semiconductores, que obstaculiza la disponibilidad de todo, desde automóviles hasta refrigeradores, no ha reducido las ganancias de las grandes tecnológicas

Clientes y proveedores de chips enfatizaron ante Biden la necesidad de poner foco en la cadena de suministro de semiconductores para ayudar a mitigar la escasez. Si Biden les entendió, es harina de otro costal, porque toda su carrera es política y su única relación con las empresas y más aún con las TIC es lo que ha visto en las películas, aunque también esto es dudoso, porque por edad, solo ve cine en blanco y negro… Anyway, la transparencia es esencial para ambas partes: por ejemplo, los fabricantes de automóviles necesitan una mejor percepción de los fabricantes de chips sobre cuántos y cuándo estarán disponibles antes de arrancar la producción. Los fabricantes de chips quieren tener una idea más clara de la demanda real, con la esperanza de evitar posibles pedidos fantasma que acaban por cancelarse, como sucedió en 2020.

La gran escasez de chips para automóviles es mala para la industria automotriz, pero solo temporalmente. Los verdaderos perdedores son los consumidores que necesitan coches para volver al trabajo, especialmente en EE.UU., donde hay demanda. En España, no aplica, porque apenas se venden coches.

General Motors ha suspendido la actividad en 3 fábricas afectadas por la escasez mundial de semiconductores. La mayoría de los grandes fabricantes

Intel seguirá fabricando la mayoría de sus chips de alta gama, pero también gestionará fábricas para otras empresas, que tienen su sede en EE.UU. y Europa

de automóviles han reducido la producción. Los microchips para automóviles son pocos, debido a los recortes de pedidos realizados al inicio de la pandemia y la fuerte demanda de otros sectores.

La menor producción afecta a los resultados de los fabricantes de automóviles porque registran las ventas al enviar el inventario a los concesionarios. En febrero, GM y Ford pronosticaron que el impacto negativo en sus resultados operativos de 2021 ascendería a miles de millones de dólares. Desde entonces, la escasez de semiconductores ha empeorado, por lo que el impacto estimado podría ser aún mayor cuando las empresas informen los resultados del primer trimestre.

Por contraste con la industria automovilística, la escasez mundial de semiconductores, que obstaculiza la disponibilidad de todo, desde automóviles hasta refrigeradores, no ha reducido las ganancias de las grandes tecnológicas.

Un barómetro temprano de la fortaleza financiera de la industria TIC es Samsung Electronics, que anticipa un aumento del 44% de su resultado operativo, a pesar de que su producción de chips en Estados Unidos se paró durante semanas debido a la fortísima nevada en Texas.

Por su parte, Intel tiene un nuevo chip de centro de datos (al igual que nuevo CEO, desde febrero de este año). Después de varios trimestres de retrasos, Intel lanzó oficialmente sus chips de servidor “Ice Lake”. Los nuevos chips Ice Lake de Intel cuentan con un aumento de rendimiento del 46%, y están hechos con su procesador de 10 nanómetros. Intel comenzó el envío del producto en el primer trimestre, una señal para los inversores de que la compañía está comenzando a recuperarse de los retrasos en la fabricación antes comentados. Es una tecnología dirigida específicamente a acelerar los cálculos de Inteligencia Artificial y las características de ciberseguridad. El chip también incluye funciones que ayudan con el cifrado y el descifrado, tareas que son particularmente difíciles de realizar para los microprocesadores.

La nueva generación de chips para servidores de Intel llega cuando la compañía ha perdido cuota en ese mercado frente a Advanced Micro Devices (AMD) en el primer trimestre de 2021. Según datos de Mercury Research, AMD ganó 2,6 puntos porcentuales para captar el 7,1% del mercado de servidores en el cuarto trimestre, sin contar los dispositivos que forman parte de la llamada Internet de las Cosas. La participación de Intel disminuyó…

Los inversores siguen de cerca también el debut del chip Sapphire Rapids de última generación de Intel. Sapphire Rapids utiliza la técnica de fabricación de 10 nanómetros de segunda generación de Intel y es el primer producto que combina “completamente” varios semiconductores distintos en

un solo paquete. Sapphire Rapids se lanzará en la segunda mitad de este año. Los envíos en volúmenes significativos comenzarán en 2022.

"Intel ha vuelto. El Intel antiguo es ahora el nuevo Intel" (en breve lo explicamos para los que ignoran de qué va la fiesta… porque dicho así, es difícil entender la frase, sin conocer la historia de Intel).

En medio de la escasez de chips y aumento de la competencia con Nvidia y AMD, Intel estrenó CEO el pasado febrero: Pat Gelsinger, para quien Intel, "el gigante estadounidense de la fabricación de chips, está recuperando su gloria". Es nuevo CEO, pero no nuevo en la empresa, donde trabajó 30 años con la vieja guardia de Intel de Andy Grove, hasta que fue despedido y ahora vuelve como Bruce Willis en "Jungla de Cristal 6.0", con ganas de pelear.

Para empezar, duplicará la fabricación e invertirá 20.000 millones de dólares en construir dos nuevas fábricas de chips en Arizona. Made in América. Biden ayudará al sector con otros 50.000 millones de dólares, cifra que, seguramente, subirá hasta los 100.000 millones, para estimular la oferta de chips, puesto que la demanda está hambrienta…

> El valor de mercado de Nvidia se ha disparado a 319.800 millones, superando la valoración de Intel de 214.500 millones, a pesar de que Nvidia tuvo 10.920 millones en ventas anuales en su último año fiscal, en comparación con 71.970 millones de Intel, siete veces más

Se espera que Gelsinger, quien comenzó su carrera con más de 30 años en Intel, pueda encauzar el rumbo del barco después de años de desafíos, en los que su desarrollo de chips más avanzado se estancó y fue superado por rivales asiáticos, como TSMC, que actualmente puede fabricar transistores más pequeños, y, por lo tanto, chips superiores. Para los que hemos trabajado en y para Intel, este hecho de hoy, hubiera sido impensable hace 15 años.

El cambio de estrategia más significativo es una nueva división llamada Intel Foundry Services, que aprovecha una de las mayores tendencias en el mundo de los semiconductores. Muchas de las principales empresas de tecnología y fabricantes de chips se han movido a un modelo en el que solo diseñan chips, pero recurren a fábricas asiáticas de TSMC y Samsung para fabricarlos. Tendencia que al presidente Trump le ponía los pelos de punta y, falta de pelo, pone muy nervioso

al actual presidente norteamericano, Joe Biden: el outsourcing de la producción de chips americanos a TSMC y Samsung, por mucho que sean aliados, provoca pérdida de empleos en América y potenciales robos de propiedad intelectual, de los que la administración de Trump acusó a empresas chinas, por ejemplo, sin repetir nombres por todos conocidos.

Intel seguirá fabricando la mayoría de sus chips de alta gama, pero también gestionará fábricas para otras empresas, que tienen su sede en EE.UU. y Europa. La estrategia de foundry/fundición (significado de foundry en castellano) también destaca la posición de Intel como un importante fabricante estadounidense, que muchos legisladores han tratado de proteger con incentivos, ya que los problemas de la cadena de suministro y la escasez de chips han revelado "lagunas" en la fabricación de chips en Taiwán (TSMC) y Corea (Samsung).

El anuncio de Intel y su inversión de 20.000 millones de dólares en nuevas fábricas en suelo estadounidense sugieren que, en unos pocos años, las empresas que podrían haberse visto obligadas a ir a Asia para fabricar semiconductores podrían obtener un rendimiento similar de chips fabricados en lugares como Arizona.

Intel sugiere que había mucha demanda de sus servicios de fundición, especialmente de las grandes empresas de tecnología estadounidenses. Según su nuevo CEO, "ha recibido ofertas por sus servicios de fundición/foundry de compañías como Amazon, Cisco, Google, IBM y Qualcomm. El CEO de Microsoft, Satya Nadella, ha respaldado públicamente el plan de Intel.

Apple no está en esa lista de potenciales clientes, porque, como antes dijimos, reemplazó los chips Intel con los suyos propios, en su última línea de ordenadores portátiles, lo que provocó miedos sobre el futuro de Intel.

Intel está ahora haciendo anuncios que comparan sus chips con los de Apple, utilizando al mismo actor que hace años hacía anuncios promocionando a los Mac y hoy, haciendo lo contrario, defiende a Intel.

Enlaces de interés...

- La demanda de equipos para teletrabajo impacta en la fabricación de chips
- La demanda de criptomonedas acelera el mercado de prueba de chips
- La industria automotriz se enfrenta a una posible escasez de chips y placas base
- El líder de la industria americana de chips recurre a las fundiciones taiwanesas
- Escasez de chips

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

¡Descubra en nuestro

Centro de Recursos IT User

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

Con la colaboración de: brother