it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

JULIO/AGOSTO 2019 - nº 21

Zero Trust, no te fíes de nada ni de nadie

Ciberseguridad en Femenino. Viaje a Israel

'La manera en que hacemos la seguridad está equivocada'

The Edge, el nuevo reto del CISO

Desayunos ITDS. Seguridad web y del email

IT Trends. Insfraestructuras, aplicaciones y datos

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 Bárbara Becares y Jaime Velázquez

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 IT User 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@itdmroup.es

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

Ciberseguridad en femenino

Según un informe de Society for Human Resources Management del pasado mes de marzo, el sector de la ciberseguridad crecerá hasta alcanzar los 152.000 millones de euros en 2020, y con ello también aumentará la demanda de empleo hasta situarse en los seis millones de puestos de trabajo en todo el mundo para este año. Sólo en Europa, se estima que en el año 2022 el sector creará 350.000 empleos más que el número de trabajadores capaces de realizar estas tareas, según se muestra en Global Information Security Workforce Study.

Se necesitan todo tipo de perfiles y las mujeres son claves para poder cubrir la demanda del sector. Según datos publicados por el informe publicado por Women in Cybersecurity, el porcentaje de mujeres que trabaja en ciberseguridad se sitúa en el 11%. No sólo debe incrementarse el porcentaje, sino el número de referentes.

Lo que no ve un joven lo ve una persona de mediana edad; lo que no observa un soltero, o soltera, lo ve una persona casada; lo que no percibe un hombre, puede percibirlo una mujer. Y bajo esta diversidad es como las empresas crecen, evolucionan y se enriquecen.

Hay un gran grupo de profesionales femeninas en el mercado de la ciberseguridad, pero disfrutan de menos visibilidad. Y al igual que ocurre con la seguridad, la visibilidad es fundamental, sobre todo a la hora de normalizar.

Por eso el viaje organizado por Daniela Kominsky, Country Manager de Cymulate, que ha tenido un gran eco en redes sociales profesionales, podría considerarse un punto de inflexión. Quizá la próxima vez que desde los medios de comunicación pidamos una declaración para un reportaje, un invitado a una mesa redonda, o un portavoz para una entrevista, se piense en femenino, sin que esto signifique, nada más lejos de mi intención, una cruzada feminista.

Gracias Daniela. Y demos gracias a las empresas y expertas en ciberseguridad por participar en este primer viaje, por formar parte de esta primera delegación de mujeres deseosa de aprender más, de compartir, de asomarse a la innovación.

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

itds

Sumario

En Portada

Zero Trust,
la confianza se ha acabado

Entrevista

'La manera en que estamos haciendo la seguridad está equivocada' (Cymulate)

Actualidad

Ciberseguridad **en Femenino**

The Edge, el nuevo reto de los CISOs

Definiendo una estrategia de **gestión de datos** para garantizar la seguridad

'Los **CISOs** en España sienten una presión muy elevada para optimizar sus presupuestos' (Deloitte)

No solo IT

Alineación de la gestión del riesgo con el plan de ciberseguridad

La figura del CISO, clave para la seguridad de la empresa y el éxito del negocio

CiberSeguridad, La clave del Factor Humano (II) Pertenencia

Índice de anunciantes

Reportaje

¿Quién puede hacer qué?

Desayunos ITDS

Seguridad web y del email

Revistas especiales

LA COMISIÓN EUROPEA RESPALDA A KASPERSKY LAB

LA COMISIÓN EUROPEA REAFIRMA QUE NO HAY INDICACIÓN ALGUNA DE PELIGRO ASOCIADO A ESTE MOTOR ANTI-VIRUS

El pasado 16 de abril de 2019, la comisaria de la UE para la Economía y la Sociedad Digitales, Mariya Gabriel, respondió públicamente a la petición realizada por el eurodiputado Gerolf Annemans sobre la Resolución del Parlamento Europeo adoptada el 13 de junio de 2018 en la que, entre otras cosas, se calificó a los productos de Kaspersky Lab como 'maliciosos'. La respuesta de la Comisión Europea ha sido categórica: **"La Comisión no dispone de ninguna prueba sobre los posibles problemas relacionados con el uso de los productos de Kaspersky Lab". 16 de abril de 2019.**

Es la segunda vez que la Comisión Europea se pronuncia con respecto a Kaspersky Lab, reafirmándose en las dos ocasiones en los mismos términos: **"La Comisión no tiene indicación alguna de peligro asociado a este motor anti-virus". 6 de abril de 2018.**
Con estas dos declaraciones, la Comisión Europea pone fin a las falsas acusaciones difundidas contra la compañía durante los últimos meses; quedando Kaspersky Lab libre de toda sospecha.

El deseo personal de Daniela Kominsky. Esa ha sido la semilla que ha generado la primera delegación de mujeres españolas relacionadas con el mundo de la ciberseguridad que visita Israel, un país reconocido por ser un referente en tecnología. Durante diez años Daniela Kominsky se dedicó a conectar empresas españolas e israelíes, ayudando a las compañías y tecnologías israelíes de ciberseguridad a desarrollar el negocio local, en usuarios finales y canales, en los mercados español y portugués. Diez años conectando hombres con hombres.

Ciberseguridad **en Femenino**

Daniela Kominsky, Country Manager Iberia, Cymulate

“Misión cumplida. Que este viaje haya servido para dar visibilidad e impulso al talento femenino en el mundo de la ciberseguridad, así como el intercambio con referentes del potente Ecosistema tecnológico Israelí. Un honor haber liderado un grupo de profesionales con una sólida experiencia y de gran inspiración”

El ecosistema de ciberseguridad israelí es uno de los más potentes del mundo. La formación de expertos informáticos es crucial en todos los países, pero en Israel se ha convertido en una razón de estado que impulsa la aparición de jóvenes empresas con un alto grado de innovación. Este rico ecosistema es el que ha recibido a la primera delegación española compuesta por 15 mujeres expertas en diferentes aspectos del mercado de la ciberseguridad. “Surgió como una iniciativa personal. Tras varios años viajando con delegaciones de hombres del mundo de la ciberseguridad a Israel me apetecía hacer un viaje diferente que pudiese dar visibilidad a las mujeres y promover referentes en un sector donde hace falta una mayor participación femenina”, explica Daniela Kominsky, artífice de este viaje que tenía una misión clara: tomar contacto con el potente ecosistema de ciberseguridad israelí. Y durante dos intensos días lo hicimos.

El grupo, formado por Julia Perea, Director Digital Security en Telefónica; Amaya Rioja, Security Manager en Telefónica; Trina de Miguel, Prevention eFraud and Information Security Manager en Bankinter; Elsa Vicario Ceballos, Agente especialista SCDTI en Ertzaintza; Victoria Gámez Simarro, Global Projects Manager en Naturgy; Carmen López, IT Security Coordinator en B. Braun; Sonia Fernández, IT Security Coordinator en S21SEC; Pilar Vila Avendaño, CEO en Forensic & Security; Belén Pérez Rodríguez, Network and Cybersecurity Engineer en Balidea; Paloma Llaneza, CEO and head of Information Technology en Razona LegalTech; Julia Barruso, Channel manager en Forcepoint; Eduvigis Ortiz, experta en Cybersecurity; Rosalía Arroyo, Directora de IT Digital Security; África Semprún Wilde, Editor de El Economista

Victoria Gamez Simarro, Global Projects Manager, Naturgy

“En ciberseguridad afrontamos dos grandes retos: concienciar de que no es una responsabilidad exclusiva de TI y hacer crecer la presencia de la mujer. Este viaje ha sido un gran foro que contribuye a ambos retos”

Eduvigis Ortiz, Experta en Cybersecurity

“Este viaje para conocer de primera mano el ecosistema de ciberseguridad en Israel ha sido un gran acierto en todos los sentidos. Encontrar mujeres de tanta calidad profesional y humana para compartirlo ha sido un gran regalo”

y Daniela Kominsky, Country Manager Iberia de Cymulate.

Primera visita obligada fue Beerseba, un parque tecnológico al que algunos han bautizado como el Silicon Valley Israelí y que se presenta como uno de los centros de inteligencia del país, que ha establecido allí uno de sus CERT (Computer Emergency Response Team) y que está invirtiendo tanto en recursos humanos como en infraestructuras. El parque tecnológico a las puertas del desierto acogerá toda la red informática militar, que se suma a la universidad y la red de empresas creadas en el sector de la seguridad. En los próximos años acogerá todo el entramado de la inteligencia

Recepción Oficial

La delegación de 15 mujeres que viajamos a Israel para estrechar lazos con el ecosistema de ciberseguridad del país, contamos con el apoyo de la embajada de España en Israel, que organizó en la casa del embajador una recepción a la qua asistieron otras 15 mujeres el entorno de TI y ciberseguridad del país, procedentes de Check Point, de NSO, de empresas de inversión o de Cymulate.

Se agradece de manera especial la colaboración de Alejandra del Río Novo, responsable de la segunda jefatura de la embajada y a Emilio López Viñuela, Consejero económico y comercial jefe de la oficina Económica y Comercio de la Embajada de España en Israel, son cuya ayuda no se hubiera podido celebrar este encuentro.

Durante la ronda de presentaciones quedó claro que las mujeres tienen mucho que aportar al sector, y que se carece de una gran, enorme, falta de visibilidad. Están -y no incluyo ahora a la prensa, pero se las ve poco. Quizá por ahí es por donde debería empezarse. Como en seguridad, la visibilidad es fundamental.

Sonia Fernández, IT Security Coordinator, S2ISEC

“Este encuentro entre mujeres dedicadas a la ciberseguridad ha sido muy inspirador, lleno de experiencias y motivaciones. Para mí ha sido un honor estar rodeada de magníficas profesionales, tanto españolas como israelíes, aprendiendo las unas de las otras y mirando hacia el futuro con una visión conjunta. Ojalá este tipo de eventos se promocionen y puedan realizarse más a menudo”

militar del segundo país más atacado del mundo a través de Internet después de Estados Unidos. Tiene previsto acoger en 200.000 metros cuadrados 15 nuevas sedes, 300.000 trabajadores, 3.000 militares y 20.000 estudiantes.

Los responsables del CERT se refieren a Beerseba como la capital de la ciberseguridad de Israel, y están contentos de contar con IBM, Paypal, EMC-RSA, Microsoft, ARM o Akamai como las primeras empresas que han establecido oficinas en este parque empresarial de alta tecnología. Explican algunos responsables del CERT a la delegación española que el equipo de respuesta establece tres capas de protección. Una centrada en impedir el ataque; una segunda que permita volver a la normalidad lo más rápidamente posible en caso de sufrir el ataque y una tercera en la que, si el ataque persiste, se contrataca. Todo ello desde un centro de control al que se accede por un pasillo previo depósito de cualquier dispositivos electrónicos en unos casilleros colocados en la entrada. Lógicamente los monitores de ese centro de control no muestran toda la información, oculta a ojos extraños. Tan sólo la dirección de algunos ataques contra Isael, más de cien mil diarios. Todos los sectores son atacados, porque no se ataca el sector sino a Israel, dicen. Todos los sectores sufren amenazas y la misión del CERT es asistir a todos, no sólo a las entidades gubernamentales.

En un edificio cercano al que acoge el CERT de Beerseba se encuentra un centro de excelencia en ciberseguridad de PwC, con maquetas que recrean una ciudad virtual y que permiten mostrar posibles ataques a infraestructuras críticas. Se habla de IT y de OT, de que la frecuencia e intensidad de los ataques se ha multiplicado en los últimos años, de que desde el momento en que te conectas al mundo exterior estás en peligros, se menciona a Tritón, un malware creado para atacar sistemas industriales y del principal

Julia Barruso, Directora de canal, Forcepoint

“Muy buena iniciativa con visitas interesantes a startups, CERT y clientes que ha servido también para reforzar y ayudar a dar visibilidad a un grupo de mujeres heterogéneo con un interés común, la ciberseguridad”

Julia Perea, Director Digital Security en Telefónica

“Este viaje, diseñado para que una delegación de mujeres españolas del sector de la ciberseguridad visite instituciones y empresas punteras de Israel en nuestro contexto diario, ha sido sumamente enriquecedor y productivo. Hemos conversado de tú a tú y compartido puntos de vista, presente y futuro, con líderes israelitas e innovadores en ciberseguridad que han reafirmado que en este colectivo sabemos de lo que hablamos”

reto de este entorno: se necesita convencer a los responsables de que inviertan en seguridad. Y hay que convencerlos porque Israel no tiene una Ley de Ciberseguridad, sino una regulación, un marco creado a partir diferentes estándares de seguridad de todo el mundo, desde las conocida NIST, al DfT, NERC, CSA… Y así han creado un marco regulatorio que no obliga y recoge lo que consideran mejor de cada normativa que hay en el mundo.

La siguiente parada fue en el Discount Bank de Israel, cuyo CISO tiene claro que lo mejor es “no ser un objetivo atractivo para los atacantes”. Se adoptan las medidas de seguridad más avanzadas, entre ellas una solución que permite simular ataques contra diferentes vectores con el fin de comprobar de manera constante el nivel de seguridad de la empresa. La herramienta es de Cylmulate y fue adoptada en 2017.

Innovación

La segunda jornada del viaje llevó a la delegación española de expertas en ciberseguridad a tomar el pulso de la innovación en Israel, para lo que se visitaron dos empresas: Team8 y Cymulate. La primera es un acelerador de empresas, un ‘builder’ creado por antiguos miembros de la Unidad 8200, la unidad de ciberinteligencia de Israel, que hace una semana anunciaba la creación de una empresa conjunta con Moodys con el objetivo de establecer un estándar global para evaluar el ciber riesgo para las empresas.

Pilar Vila Avendaño, CEO, Forensic & Security

“En Israel se hacen grandísimos proyectos y muchísima investigación ya que existe una mentalidad de gran financiación para todo ello. Lo mejor ha sido compartirlo, comentarlo y aprender con grandísimas compañeras del sector. Una experiencia inolvidable”

El objetivo de Team8 es “entender el mercado, las prioridades”, o lo que es lo mismo: detectar problemas existentes para después encontrar empresas que estén buscando la forma de solucionarlos. Una de las escogidas fue Illusive Networks,

Trina de Miguel, Prevention eFraud and Information Security Manager, Bankinter

“En este viaje he conocido a personas con las que comparto una pasión, que es la ciber seguridad, y un punto de vista que es diferente al que este sector está acostumbrado. En Israel hemos compartido experiencias, conocimientos, consejos, risas… creando importantes lazos”

que desarrolla tecnología de decepción y es competencia directa de la española Countercraft. Por cada camino verdadero que puede seguir el ciberdelincuente se crean cuatro o cinco falsos que permiten no sólo minimizar el ataque sino poder estudiarlo para responder a él.

Fundada en 2014 Claroty es una compañía que busca proteger los entornos OT. Entre sus competidores cabe mencionar a Nozomi Networks o Security Matter. La Plataforma Claroty es un conjunto integrado de productos de seguridad que proporciona visibilidad extrema, detección de amenazas, acceso remoto seguro y evaluaciones de riesgos para redes de control industrial (ICS/OT).

En cuanto a Hysolate, la última de las empresas bajo el paraguas de Team8 con la que la delegación española pudo tener contacto, no pide un replanteamiento del endpoint, o al menos de su seguridad. La tecnología que aplica la compañía vendría a ser similar a lo que hace Samsung Knox en los móviles: crear diferentes entornos dentro del ordenador a través de virtualización, lo que permite reducir los riesgos sin impactar en la productividad.

La última parada fue la de Cymulate, una empresa fundada hace tres años que busca liderar el mercado BAS, o de Breach and Attack Simulation con el objetivo de “cambiar el mercado, cómo los clientes hacen y entienden la tecnología”, nos contaba Eyal Wachsman, CEO de la compañía, y uno de sus fundadores. Este tipo de soluciones detectan las vulnerabilidades de los sistemas de seguridad de las empresas mediante la simulación constante de ataques en diferentes vectores, lo que permite saber a ciencia cierta cuán preparada está una empresa para enfrentarse a un ataque.

Enlaces de interés…

- Solo el 11% de los profesionales en ciberseguridad son mujeres
- Closing the Gap, la iniciativa con la que Trend Micro quiere cerrar la brecha de género en tecnología
- Nace Women in Cybersecurity of Spain

Belén Pérez Rodríguez, Network and Cybersecurity Engineer, Balidea

“Un lujo de compañía. Un viaje intenso pero muy productivo. En cuanto a las infraestructuras críticas: mal de muchos…. Por suerte o por desgracia vamos a la par y la senda es similar”

TREND MICRO™

POWERED BY XGen™ SECURITY

Detectar y prevenir las brechas a la velocidad del rayo

Su compañía se encuentra en el punto de mira de una variedad cada vez más compleja de amenazas: ransomware, amenazas avanzadas, ataques dirigidos, vulnerabilidades y exploits.

Solo la visibilidad completa de todo el tráfico y actividad de la red situará la seguridad de su red por delante de los actuales ataques específicamente diseñados que eluden controles tradicionales, explotan las vulnerabilidades de red y secuestran o roban datos confidenciales, comunicaciones y propiedad intelectual.

Trend Micro Network Defense detecta y evita las infracciones a la velocidad del rayo en cualquier lugar de su red para proteger sus datos críticos y su reputación.

Capacidad probada

Trend Micro Deep Discovery:
Sistema de Detección de Brechas "Recomendado" con 4 años consecutivos con tasas de detección del 100%.

Trend Micro TippingPoint:
Sistema de Prevención de Intrusiones de Última Generación "Recomendado" y 99,6% de efectividad de seguridad.

NSS LABS RECOMMENDED

Inteligencia de amenazas líder del sector

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

www.trendmicro.es

“La manera en que estamos haciendo la seguridad está equivocada”

(Cymulate)

Tel Aviv. Existe un problema fundamental en el mercado de seguridad, repetido en multitud de estudios que toman el pulso y el sentir de los responsables de seguridad: no saben realmente cuán segura está su empresa; si las soluciones de seguridad en las que han invertido funcionan; si, llegado el momento, frente a un ataque, esas soluciones se comportarán como deben.

Rosalía Arroyo

Hasta no hace mucho tiempo la evaluación del daño que un ciberataque podría causar en los sistemas pasaba por ejecutar pruebas de pentesting, evaluaciones de seguridad, auditorías, Threat Hunting, etc. Pero cada uno de estos enfoques tiene limitaciones que impiden proporcionar una imagen

"Hemos cambiado la manera en que las organizaciones compran nuevos productos de seguridad"

Eyal Wachsman, CEO de Cymulate

completa y continua de la postura de seguridad general de una organización. La reacción del mercado ha sido desarrollar un nuevo tipo de herramienta: breach and attack simulation (BAS), del que por el momento no se tienen muchos datos, más allá de una previsión del Cyber Research Databank que apunta a que podría alcanzar los mil millones de dólares para 2020.

La tecnología de simulación de brechas y ataques pone a prueba, de manera constante, las defensas de una empresa ejecutando ataques simulados para medir la efectividad de las capacidades de prevención, detección y mitigación de una empresa. Por ejemplo, se podría simular un ataque de phishing en los sistemas de correo electrónico de una compañía, un ataque en el servidor de seguridad de la aplicación web (WAF) de la compañía, el intento de exfiltración de datos, el movimiento lateral dentro de redes o un ataque de malware en un endpoint.

Es en este mercado donde nace Cymulate en junio de 2016 de la mano de Eyal Wachsman y Avihai Ben-Yossef, convertidos ahora en CEO y CTO de la compañía respectivamente. En tres años han pasado por dos rondas de financiación que acumulan 10,5 millones de dólares. La segunda, en marzo de este año, ha alcanzado los 7,5 millones procedentes, principalmente, de Dell Technologies Capital y Vertex Ventures. Crunchbase estima que la compañía tiene unos ingresos anuales de un millón de dólares, una cifra que su CEO quiere incrementar hasta llevar a Cymulate al podio de las 'One Billion Company'. Nos lo ha contado Eyal Wachsman durante una entrevista mantenida en la sede de la compañía, en Tel Aviv.

CYMULATE BREACH & ATTACK SIMULATION PLATFORM

CLICAR PARA VER EL VÍDEO

Tres años después de la creación de la compañía Wachsman, que durante más de 20 años ha desarrollado su carrera en el mundo de la ciberseguridad, asegura seguir aprendiendo cosas nuevas. "Es mi primera vez como CEO de una compañía, de una startup, y he aprendido mucho". Tiene un objetivo: desarrollar la visión de la compañía, que no es otra que aprender de los clientes, entender qué necesitan y luego desarrollar productos

Simulación vs penetration testing

Parecidos, pero no iguales. Las pruebas de penetración, o pentesting, son realizadas por un experto de seguridad que aplican su conocimiento para romper las defensas de la red de una organización. Hasta ahora es así como se han probado las medidas de seguridad de las empresas, pero sólo ofrecen resultados de un momento en el tiempo, de forma que cuando una empresa realiza alguna modificación en las medidas de seguridad, o aparece un nuevo tipo de ataque, se vuelve al punto de partida: no saber a ciencia cierta si las medidas de seguridad están protegiendo convenientemente a la empresa.

Lo habitual es que las empresas realicen uno o dos pentesting al año, con suerte una al trimestre.

Lo que hacen las herramientas de simulación de brechas y ataques es automatizar el proceso y ejecutar la simulación de manera continua con el objetivo de saber si la seguridad de una empresa está funcionando. La capacidad de evaluar la seguridad de forma continua y automática en entornos de producción reales, a lo largo de toda la cadena, elimina las conjeturas, incorpora el contexto de riesgo empresarial y proporciona resultados procesables.

que les permitan cerrar todos los gaps que tienen en ciberseguridad. “Creo que desde que establecimos Cymulate, las organizaciones están afrontando la ciberseguridad de una manera diferente”, asegura.

Dice Wachsman que los fabricantes de ciberseguridad tienen que entender que el mercado está cambiando; “como fabricante puedes prometer que puedes proteger la organización, pero hoy no tenemos que asumir esa promesa, porque nosotros podemos confirmarla, y probarla, y si no eres bueno, te van a reemplazar, escogerán diferentes productos. Tenemos clientes, grandes clientes, que han comprado y pagado por productos de seguridad, y no voy a mencionar nombres, pero después de ver cómo nuestra plataforma los superaba, los han reemplazado”. Añade el CEO de Cymulate que la plataforma de la compañía permite a las empresas comprobar la efectividad de los controles de seguridad de forma que “si una organización quiere comprar buenos productos de seguridad, tener dos o tres fabricantes entre los que escoger, nuestro cyber lab los prueba bajo ataques reales. De forma

"No importa lo que se invierta en seguridad, en gente, en tecnología, cuando los malos deciden penetrar en tu organización, lo consiguen"

it whitepapers

GLOBAL PHISH REPORT 2019

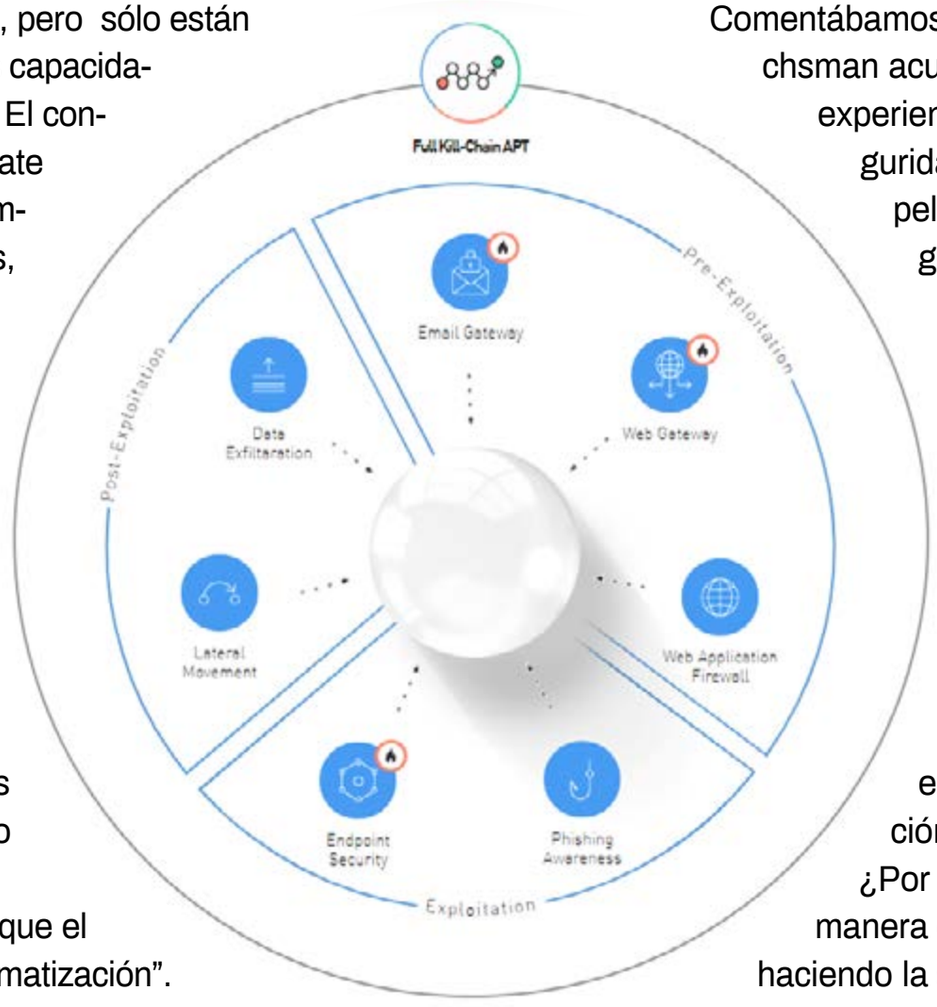
Durante la última década, los ataques de phishing se han convertido en la amenaza de correo electrónico más extendida para las organizaciones de todo el mundo. A medida que las soluciones de seguridad diseñadas para bloquear estos ataques se han vuelto más avanzadas, la sofisticación de estos ataques ha seguido su ritmo, evolucionando para evadir la detección. La tecnología basada en la nube, con todos sus beneficios, ha dado paso a una nueva era de ataques de phishing. La naturaleza de la nube proporciona aún más vectores de los que los hackers se aprovechan, e incluso un acceso más amplio a datos críticos cuando un ataque de phishing tiene éxito.

que nosotros hemos cambiado la manera en que las organizaciones compran nuevos productos de seguridad: pruébalos y escoge al mejor". Ya no hay que creer en los que dicen grandes consultoras, sino lo que se ve en la vida real, y después "decide lo que quieres hacer".

Un mercado incierto

Sobre la situación actual, dice Eyal Wachsman que nos enfrentamos con un gran problema: en los últimos tres años, cada año las organizaciones han gastado miles de millones de dólares en comprar productos de seguridad, pero sólo están utilizando el 20% de las capacidades de esos productos. El consejo del CEO de Cymulate es que antes de ir a comprar nuevas tecnologías, nuevos productos, se invierta dinero "en cambiar la configuración de los controles de seguridad que ya tienes, para pasar de ese 20% a un 80%, o más, de las capacidades. Eso es lo que estamos haciendo ahora: incrementar esas capacidades cambiando las configuraciones".

Sobre el futuro: "creo que el mundo va hacia la automatización".



En un 75% de lo que hace Cymulate está reemplazando a los consultores tradicionales de pentesting, risk assessment, etc., dice Wachsman, añadiendo que utilizar una firma de consultoría es como planificar tus vacaciones y comprobar cómo está el tiempo dos semanas antes; "las firmas de consultoría llegan a tu oficina, comprueban tu tecnología, vuelven a sus oficina y tres semanas, o mes y medio después vuelven con los resultados. Unos resultados que ya no son relevantes. Lo que nosotros hacemos en ofrecer los resultados de manera inmediata y lo hacemos de manera continua".

Comentábamos que Eyal Wachsman acumula 20 años de experiencia en ciberseguridad. De su papel como CISO en grandes empresas nació la idea de crear Cymulate, "porque no importa lo que se inviertan en seguridad, en gente, en tecnología, cuando los malos deciden penetrar en tu organización, lo consiguen". ¿Por qué? "Porque la manera en que estamos haciendo la seguridad está

"Los fabricantes de ciberseguridad tienen que entender que el mercado está cambiando. Como fabricante puedes prometer que puedes proteger la organización, pero hoy no tenemos que asumirlo, porque nosotros podemos confirmarlo, y probarlo"

Mercado BAS

Para ser una tecnología de seguridad relativamente reciente, ya hay un buen puñado de empresas en este mercado. Algunas de ellas son:

- ATTACKIP. Se fundó en 2013 en California y lleva recaudados 14,3 millones de dólares en fondos de inversión. Según recoge CrunchBase la plataforma FireDrill es un sistema basado en agentes que "requiere un tiempo de configuración mínimo y pocos recursos para implementar". Incluye un panel de control para monitorizar su postura de seguridad en curso y una sección de proyecto para ejecutar escenarios de ataque específicos.
- CYMULATE. Nombrado Cool Vendor for 2018 por Gartner, cuenta con una plataforma que aseguran poder desplegar en minutos con capacidades para comprobar diferentes vectores, incluido alertas de amenazas inmediatas, seguridad de correo electrónico, pasarela web, aplicación web, movimientos laterales, APTs, endpoint, exfiltración de datos, phishing y evaluaciones SIEM / SOC.
- PICUS SECURITY. Se fundó en abril de 2013 y se reconoce a sí misma como el pionero en tecnologías BAS. Apenas ha recibido inyecciones de capital, y se le estiman unos ingresos anuales de tres millones de dólares. La sede de la compañía está en San Francisco y tiene oficinas en Londres y Ankara, de donde proceden la mayoría de sus ejecutivos.
- SAFEBREACH. También fue nombrado Cool Vendor por Gartner, en 2017. Fundada en 2014 en Silicon Valley, y con una inversión acumulada de 34 millones de dólares, SafeBreach ofrece simuladores de nube, red y punto final que pueden detectar la infiltración, el movimiento lateral y la exfiltración de datos. Se le calculan unos ingresos anuales de 2,8 millones de dólares.
- VERODIN. Verodin es una plataforma que permite a las organizaciones medir, gestionar y mejorar la eficacia de la ciberseguridad de redes, endpoint, email y la nube. Se fundó en 2014 en Virginia (Estados Unidos) y el año pasado consiguió recaudar 28 millones de dólares de una ronda Serie B. Se estiman ingresos por valor de 5 millones de dólares anuales.

equivocada. No nos estamos testeando todo el tiempo, no estamos preparados para predecir lo que podría pasarle a nuestra red. Esa es la razón por la que creamos la compañía. Por supuesto, incluso los clientes que utilizan Cymulate pueden ser vulnerables si no reparan todas las brechas que encontramos , pero les permite estar un paso por delante".

Cymulate en el terreno de juego

El mercado de compra de startups está en auge. Ya no es habitual que las grandes empresas de-

Enlaces de interés...

- Desayuno ITDS. Thtreat Hunting
- BAS, o cómo la simulación de ataques puede aumentar tu serguridad
- Cómo BAS acaba con el pentesting

"En Europa ya somos líderes. Queremos serlo también en el mercado estadounidense"

sarrollen nuevas unidades de negocio o se adentren en nuevos mercado por sí solas. Compran tecnología. Cymulate ya ha recibido ofertas de compra, pero esa no es la visión de Wachsman, que asegura haber creado esta empresas para ser una 'One Billion Company'. "Mi filosofía es la de comprar otras compañías, no la de ser comprado. Adquirir compañías que complementen nuestra tecnología".

Le preguntamos si tendría sentido crecer hacia el mercado de Threat Hunting. "No estoy seguro todavía", dice mientras apunta que quizá las adquisiciones serían de otras compañía del mercado BAS", una categoría de mercado que quiere liderar; "en Europa ya somos líderes. Queremos serlo también en el mercado estadounidense".

Insistimos sobre la posible expansión de Cymulate hacia el mercado de Threat Hunting. "Podría ser Threat Hunting. Podría ser escaneo y gestión de vulnerabilidades", comenta Wachsman. ¿Como Qualys? "Qualys es mucho más grande que nosotros. Tenemos buena relación con ellos y otras compañías del sector, como Rapid7, Tenable… pero en mi visión está ser el siguiente Qualys, o el siguiente Tenable".

Sobre la plataforma de simulación de ataques de la compañía nos cuenta que es muy inteligente y muy simple, que no importa cuán experto sea el CISO "porque puedes utilizar nuestra plataforma con un solo click y conseguir resultados de forma inmediata, resultados en los que es muy fácil entender qué es lo que está mal". De forma que con Cymulate el CISO, el equipo de seguridad, el administrador del SOC, o el administrador de TI, dependiendo del tamaño de la organización, "tendrá una plataforma muy fácil de utilizar, incluso si está en la playa, porque es un producto basado en cloud. Pueden irse de vacaciones, lanzar el ataque desde Tailandia, o programar el ataque".

No nos marchamos sin preguntarle cuántos años cree que tardará en conseguir ser una 'One Billion Company': "En tres años a partir de ahora".

Compartir en RRSS

ÚLTIMAS PLAZAS

MÁSTER
Data, Complex Networks and Cybersecurity Sciences

¡INSCRÍBETE YA!
Inicio el 16 de septiembre

www.master-dcncsciences.com

DCNC Sciences

Universidad Rey Juan Carlos

The Edge, el nuevo reto de los CISO

Sin que el cloud haya sido plenamente adoptado, el Edge irrumpe con fuerza animado por la movilidad y el IoT. Edge computing es la tendencia de la próxima década y Aruba se posiciona con una serie de objetivos claros: proporcionar la conectividad, proporcionar la estructura de seguridad y proporcionar la capa de cómputo y almacenamiento. Así lo ha dicho durante su Atmosphere EMEA celebrado a primeros de junio en Croacia.

La última década ha sido la del cloud. La nube seguirá creciendo con sus capacidades concentradas en el datacenter, pero entramos ahora en la era del Edge Computing, la siguiente gran tendencia del mercado TI basada en la idea de que, para

hacer frente a las enormes cantidades de datos generados por el IoT, la infraestructura de red y de computación necesitan replantearse. La nueva tendencia es que muchos de esos datos deben analizarse y procesarse en ese borde de la red, en lugar de ser transportada a un centro de datos remoto centralizado.

La clave es que dado que el procesamiento se realiza cerca de donde se generan los datos, estas arquitecturas podrán ofrecer un mejor rendimiento y eficiencia y, en última instancia, permitir que las empresas reduzcan sus gastos operativos. Y como con cada nueva tecnología, los riesgos están ahí. En este caso se trata de agregar más dispositivos capaces de generar datos a una red.

El Edge computing es “mobile first, cloud-native, IoT enabled and autonomous” decía el CEO de Aruba durante el evento anual para la región de EMEA, en el que aseguraba que la nueva oleada de innovación consiste en integrar el IoT en un puesto de trabajo inalámbrico en el que Wi-Fi 6 será parte integral de la próxima generación de conectividad 5G.

“Con los puntos de acceso Wi-Fi 6 [que Aruba ha lanzado recientemente], tenemos la oportunidad de integrar esa capacidad de IoT directamente en la propia infraestructura inalámbrica. Esta es la forma en que comenzaremos el IoT mucho integrado en la infraestructura empresarial”, decía Keerti Melkote.

Edge Computing

Empecemos por el principio. Gran parte del foco del evento Atmosphere de este año ha sido el Edge Computing, una enorme oportunidad que permite crear infraestructuras con capacidades de conectividad, cómputo, control y seguridad y el propósito expreso de recopilar datos para mejorar la experiencia del cliente y, por ende, los negocios. “Es una tendencia completamente nueva”, decía Keerti Melkote, en el que cada Edge está relacionado con los datos y estará habilitado por el cloud. Habrá Edges desplegados en miles de ubicaciones, “por lo que es muy importante que el trabajo funcione a una escala distribuida”.

Aseguraba Melkote que “el IoT es una gran pieza del rompecabezas que cambia la ecuación”. Según datos de Aruba, el Internet de las Cosas y el crecimiento de datos asociados al mismo tiene un potencial de 11 trillones de dólares al año. Y para capturar este potencial, las organizaciones necesitan implementar el Edge, “una arquitectura que

Las tecnologías Edge permiten el procesamiento de datos en el borde de las redes, que es donde están los usuarios y los dispositivos

sea completamente conectada, segura, distribuida y autónoma"

Aruba Clear Pass Device Insight

Muy relacionado con el potencial del IoT es Aruba Clear Pass Device Insight. "Ha sido muy bien recibido y lo que hace es demostrar la importancia de la visibilidad de los dispositivos IoT", decía el CEO de Aruba al preguntarle por el valor de la solución que la compañía presentaba en abril de este año. Añadía Melkote que la visibilidad es el primer paso para hacer frente al riesgo del IoT y que la solución no sólo permite ver lo que está en la red, sino saber lo que el dispositivo puede hacer para después aplicar políticas; es decir: "visibility, profiling and policy".

Digamos que el famoso Shadow IT se ha descontrolado con el Internet de las Cosas. Ya no sólo hay que preocuparte por ese móvil, proyector, tablet, o reloj inteligente que se añaden a la red sin conocimiento de los responsables de TI. Hablamos de sensores de todo tipo. Aseguran desde Aruba que los métodos tradicionales de detección y creación de perfiles hace que muchas organizaciones tengan puntos ciegos y sólo una vista parcial de los dispositivos conectados, identificados como dispositivos Windows o Linux. Por ejemplo, en un hospital, una máquina de MRI y una bomba de infusión IV pueden verse exactamente iguales: un dispositivo genérico de Windows. Pero asignar a ambos dispositivos la misma política de acceso podría potencialmente impedir que uno de ellos acceda a la red, lo que tendría consecuencias desastrosas para el paciente. La falta de una visión clara de los dispositivos hace que la creación de una política de control de acceso integral sea prácticamente imposible.

Aruba ClearPass Device Insight es una solución

"Aruba Clear Pass Device Insight ha sido muy bien recibido y lo que hace es demostrar la importancia de la visibilidad de los dispositivos IoT"

Keerti Melkote,
co-fundador y CEO, Aruba

de detección de dispositivos basada en inteligencia artificial que ofrece una visión completa y granular de todo lo que hay en la red, esté conectado por cable o de forma inalámbrica. Device Insight adopta un enfoque diferente para identificar los dispositivos en la red al recopilar el tráfico de la red, extrayendo los atributos del dispositivo, como las aplicaciones a las que se accede, los puertos, los protocolos y el volumen, y utiliza estos datos para realizar identificativos en función de sus atributos de comportamiento, no de atributos estáticos.

Resumía Keerti Melkote que el objetivo de ClearPass es conectar de forma segura usuarios e IoT a aplicaciones y datos. Sobre la situación real del IoT en las empresas, aseguraba el directivo que "IoT es real. Está ocurriendo", y que son muchos los que se quedan sorprendidos cuando aplican ClearPass Device Insight en sus redes porque no sabían que tenían tantos dispositivos conectados. "El próximo paso para nosotros es integrar el IoT mejor, y hacerlo de forma segura".

IoT integrado y seguro

De forma que el siguiente paso de la evolución "se centrará en la integración de IoT con un lugar de trabajo totalmente inalámbrico y, para mí, IoT toma una forma tanto cableada como inalámbrica" decía Melkote, cuya compañía lanzó hace unos meses puntos de acceso Wi-Fi 6, diseñados para ofrecer velocidades más altas y más eficiencia en todos los espectros para adaptarse a más usuarios y dispositivos en la red.

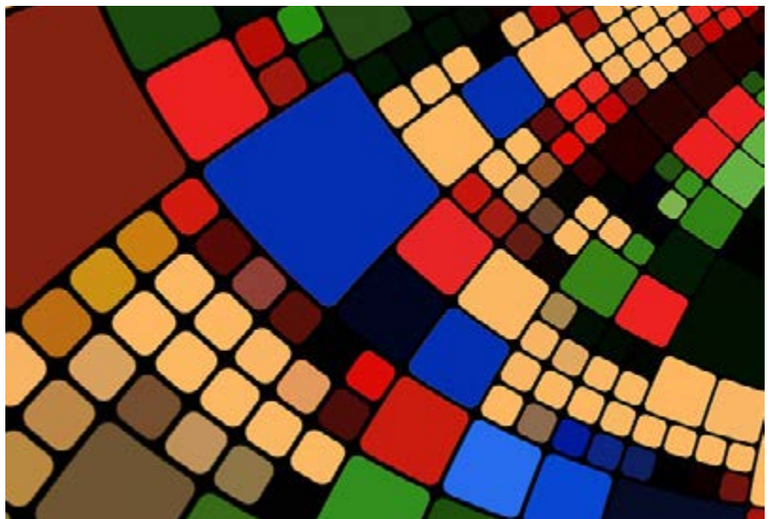
"Con los puntos de acceso Wi-Fi 6, tenemos la oportunidad de integrar esa capacidad de IoT directamente en la propia infraestructura inalámbrica", aseguraba el directivo.

"La segmentación dinámica garantiza que la red en su conjunto sea mucho más segura y más capaz que nunca de resistir la próxima tormenta de IoT"

Partha Narasimham, CTO, Aruba

Integrar IoT de una manera segura no sólo pasa por ClearPass Device Insight, sino por la capacidad de segmentación dinámica de red de la compañía. Algo en lo que incidió Partha Narasimham, CTO de Aruba, durante un encuentro con la prensa. Se da por hecho que la mayoría de los dispositivos IoT no son tan inteligentes como estamos tentados a pensar. La mayoría, decía el directivo, incorporan chipsets tan rudimentarios que es imposible hacerles inteligentes. De forma que lo que nos queda es llevar la inteligencia a la red y "dotarla de la capacidad de tomar la decisión correcta para mantener las cosas a salvo cuando los dispositivos no pueden hacerlo por sí mismos". De forma que la tecnología de Aruba aplica segmentación dinámica a todo lo que se conecta a las redes, pudiendo aplicar a cada conexión un servicio totalmente personalizado.

El proceso dinámico de segmentación que Aruba ha desarrollado tiene algunas características clave que son muy importantes para estos dispositivos IoT poco inteligentes, explicaba Narasimham, hablando del anclaje de MAC. Mencionaba la posibilidad de que un dispositivo no responda a los pings enviados para verificar que aún está vivo en el otro lado del enlace. "Aruba ha descubierto cómo conectar la dirección MAC del dispositivo IoT al puerto para que siempre se autentique hasta que se desconecte o se elimine. Y debido a que la dirección MAC del dispositivo se usa para garantizar la autenticación, también puede protegerse de alguien que conecta un dispositivo diferente e intenta secuestrar el puerto en sistemas más críticos, como los registros médicos electrónicos (EMR), por ejemplo".



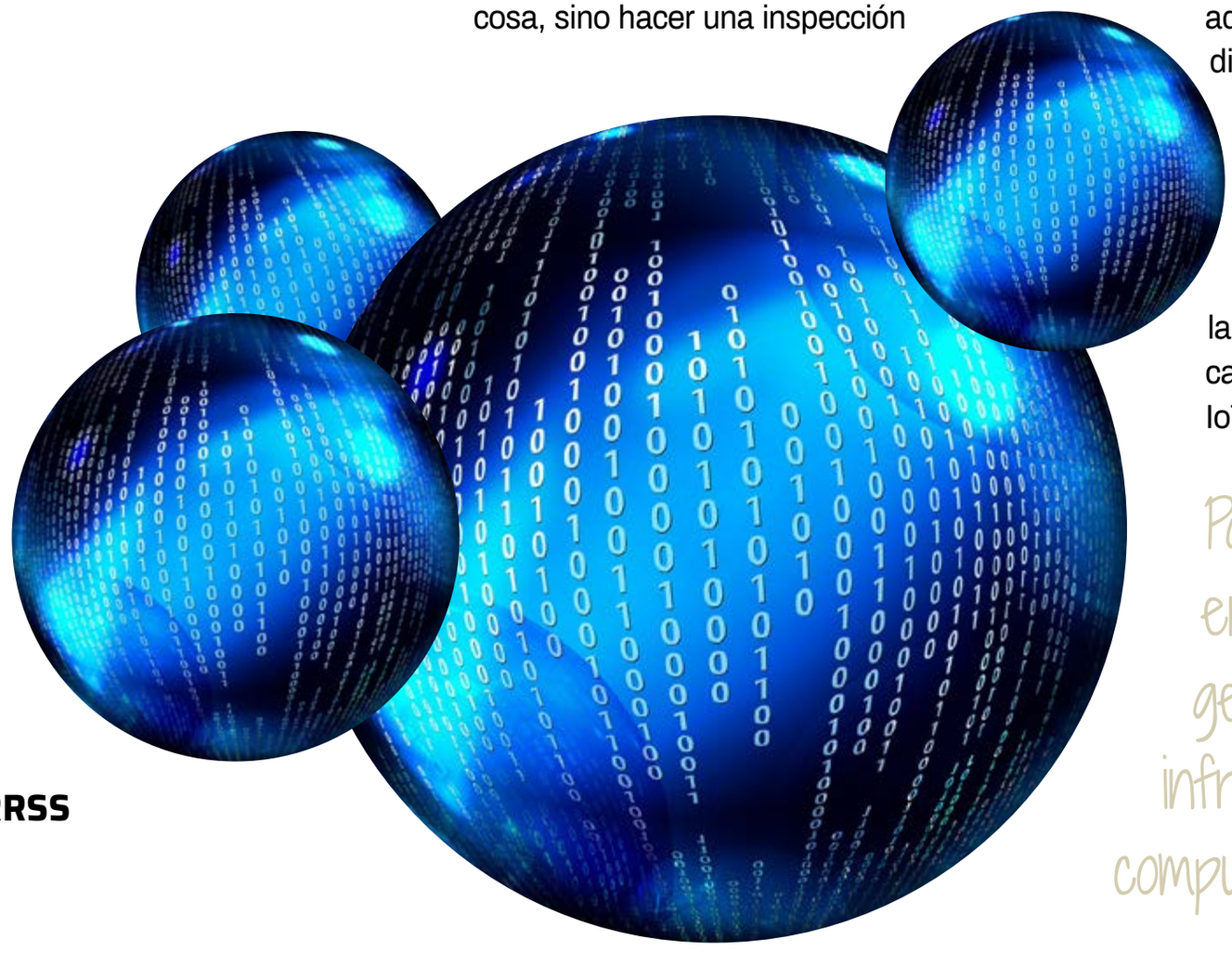
Enlaces de interés...

- HPE Aruba pone el foco en la ciberseguridad y crea en España un equipo para dar soporte al sur de Europa
- Aruba refuerza su puesta por el mercado WiFi para SMB con Instant On
- ¿Considerando un despliegue SD-WAN? Puede que tenga ya la mejor solución en su actual red

Mencionaba Narasimham los túneles basados en usuario (User-Based Tunnels) a través de tecnología Policy Enforcement Firewall (PEF) de Aruba como otra pieza importante de la segmentación dinámica. “Al igual que la infraestructura en un controlador de movilidad que canaliza el tráfico del usuario hacia el dispositivo, también el Túnel basado en el usuario puede enviar todo el tráfico de un dispositivo IoT al PEF, integrado en el Mobility Controller, y esto se puede hacer a través de APs inalámbricos, así como los interruptores cableados”.

Esto no sólo permitiría autenticar el tráfico de una cosa, sino hacer una inspección profunda de paquetes en el tráfico que viene del dispositivo para asegurar que no se utiliza como un vector de ataque; “incluso puede usar el firewall para asegurar que las cosas que no deben inundar su red se detengan cerca del borde, como las cámaras de seguridad que se usan para lanzar un ataque DDoS”.

A pesar del temor que suscita el Internet de las Cosa, al que frecuentemente se han referido como el Internet of Troubles, o el Internet of Threats, aseguraba el CTO de Aruba que el “IoT no tiene por qué dar miedo”, ya que, con la infraestructura adecuada, “puede manejar fácilmente cualquier dispositivo que aparezca, desde bombillas hasta monitores de presión arterial. Puede asegurarse de que sean capaces de comunicarse con las ubicaciones correctas en la red y que solo los dispositivos correctos pueden hacer esa comunicación. La segmentación dinámica garantiza que la red en su conjunto sea mucho más segura y más capaz que nunca de resistir la próxima tormenta de IoT”.



Para hacer frente a las enormes cantidades de datos generados por el IoT, la infraestructura de red y de computación necesitan replantearse

Compartir en RRSS

Definiendo una estrategia de gestión de datos para garantizar la seguridad

Desde que un dato entra en una empresa es necesario contar con una estrategia para su gestión. El almacenamiento de ese dato será costoso y hay que hacer que sea útil tenerlo para mejorar un negocio. Además, la seguridad será esencial. Para ello hay tres ejes principales: empleados bien formados en el manejo de datos; socios que los almacenen de una forma óptima; y herramientas de seguridad como pilar de apoyo fundamental.

Bárbara Bécares

Los datos llevan tiempo definiendo los negocios de éxito. Conocer bien a los clientes y usuarios es clave para ofrecerles lo que necesitan. Y para adaptar una empresa a las necesidades del mercado.

El problema es que muchas compañías y entidades no saben qué hacer con esos datos que van aumentando día a día. Y, peor aún, una estrategia errónea puede tener consecuencias catastróficas. Más en los casos en los que peligre la seguridad de estos.

La era digital ha llegado acompañada de una infinidad de nuevas oportunidades para la creación e innovación de nuevos productos y servicios, pero al mismo tiempo hay riesgos que llegan de la mano de

Si las empresas guardan esos volúmenes de datos, con el trabajo y el coste que eso supone, es para darles un valor

esos datos, muy jugosos para cualquier ciberdelincuente. De hecho, desde Sophos advierten que "los servidores se han convertido en un objetivo que despierta gran interés debido al volumen de datos almacenados en ellos".

Un estudio de la consultora IDC calcula que el mercado español vivirá un claro crecimiento alrededor de la analítica del dato, con crecimientos medios superiores al 6% (CAGR) hasta 2021 para el software de análisis del dato y de más del 33% (CAGR) en el entorno de las plataformas encargadas de aplicar la inteligencia capaz de obtener un valor diferenciador del dato. Ahora bien, para aprovechar esta enorme oportunidad, hay que crear una estrategia para guardar esta información y que sea de una forma segura.

Además de todo eso, la sociedad ampara la protección de las informaciones privadas. Y eso ha llevado a que cada vez más sea mayor la preocupación por parte de las empresas, así como de las administraciones públicas, tal y como se ha visto con la implantación del Reglamento General de Protección de Datos en Europa.

Clasificar y decidir dónde almacenar los datos

Hay diferentes opciones disponible para el almacenamiento de la información empresarial y esas opciones se dividen en dos grandes grupos. Por un lado la opción In-House, es decir, en servidores y equipos propios. Por otro está el cloud o la nube que consiste en ceder la gestión de esa información a terceros. Y otra opción muy común es la de mezclar ambas opciones.

Sobre el almacenamiento de la información en la nube dice Enrique Turrillo, director de Risk Advisory de BDO explica que previamente se debe realizar "una clasificación de la información (confidencial, interna o pública) y evaluar qué se sube a Cloud y qué no para evitar problemas en caso de ataques o fugas de información". Por tanto, para empezar,

se deben clasificar esos datos. No todos tienen la misma importante.

Por otro lado, continúa el experto explicando que “se podría gestionar de forma interna mediante una nube privada, lo cual permite cumplir con todas las políticas internas, ofreciendo un mayor nivel de seguridad y permitiendo un control total de los recursos”.

Ahora bien, esta tarea tiene, como recuerda Enrique Turrillo, un inconveniente principal: “el elevado coste que ello supondría, y la dependencia de un proveedor que proporcione una infraestructura”. Clatro que otra opción que se podría elegir es la externalización del servicio Cloud con un proveedor, para lo cual se deberán establecer unos estrictos requisitos de seguridad en las cláusulas contractuales, recuerda el directivo.

Herramientas de protección para grandes datos

Por su parte, Alberto R. Rodas, Sales Engineer de Sophos Iberia, explica que el mencionado Reglamento General de Protección de Datos también supone un reto a la hora llevar a cabo una gestión adecuada de los datos que se acumulan.

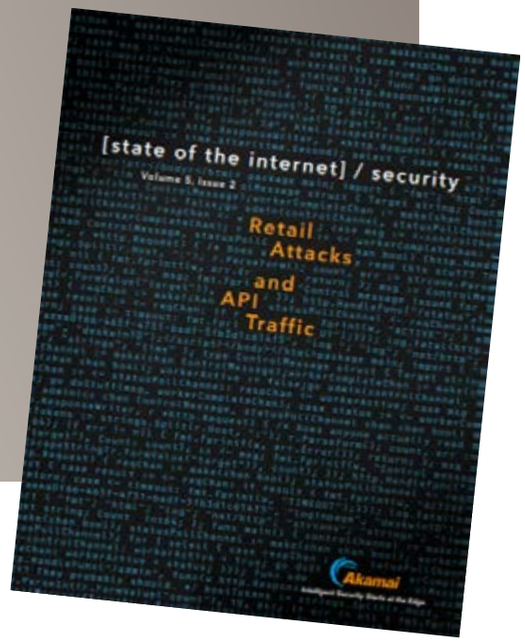
“En realidad, independientemente del lugar donde las empresas decidan almacenar sus datos, lo más importante es contar con una estrategia de seguridad adecuada a las características del lugar en donde queden almacenados”, explica el experto de la empresa de seguridad que añade que Sophos tiene bien “claro que la seguridad de los datos y de la información es una de las mayores preocupaciones actuales, por lo que contamos con diferentes soluciones de seguridad adaptadas a cada fórmula de almacenamiento” y sus servicios están enfocados en la protección de los datos almacenados en Data Center con el objetivo de proteger los endpoints para poder investigar y frenar los ataques contra servidores.

Por otro lado, en el caso de que la empresa decida almacenar sus datos en la nube, también hay soluciones que protegen la información, y que

it whitepapers

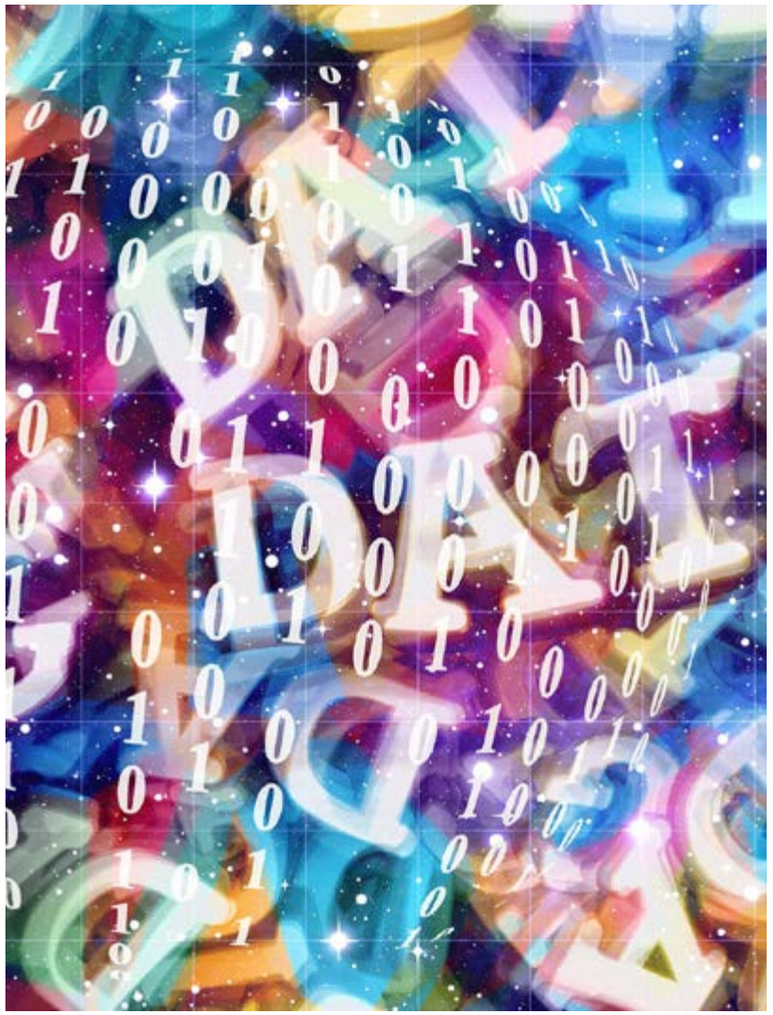
INFORME SOBRE EL ESTADO DE INTERNET - AKAMAI

Akamai detectó casi 28 mil millones de intentos de relleno de credenciales entre mayo y diciembre de 2018. Herramientas como la botnet All-in-One son responsables de un gran número de intentos contra organizaciones minoristas. Este informe de Akamai deja claro cuál es el estado de Internet.



"Es necesario identificar proveedores de Cloud que se encuentren localizados dentro del Espacio Económico Europeo o países que de alguna forma garanticen de forma correcta la protección de todos los datos de carácter personal y las garantías jurídicas adecuadas"

Enrique Turrillo, director de Risk Advisory, BDO



gracias a la Inteligencia Artificial puede proporcionar visibilidad continua de todos los elementos que hay guardados en la nube, proporcionando respuesta a las amenazas en todos los entornos cloud.

¿Guardar todos los datos o quedarse solo con algunos de ellos?

El primer trabajo es seleccionar la información que llega a la empresas. Se debe decidir en primer lugar si se guardan todos esos datos o si se hace una selección para quedarse solo con los más relevantes. En este punto, si bien es cierto que guardar todos los datos supone mucho más gasto, aún parece complicado saber cómo hacer una selección de la información que merece la pena preservar y cuál desechar.

El portavoz de BDO afirma que "no es conveniente almacenar en la nube todos los datos que vayan llegando, es recomendable realizar una clasificación de la información (información confidencial, interna o pública) y valorar qué datos es conveniente almacenar en este tipo de servicio y cuáles será mejor mantener almacenados en la propia entidad, para tener un mayor control sobre los mismos".

Actualmente existen herramientas inteligentes que ayudan en esta tarea. Desde Sophos, explica Rodas que su empresa opta por almacenar todos los datos, contando con sistemas inteligentes que realizarán la criba sobre aquellos que deben ser tenidos en cuenta por los administradores de los productos. Y estas tecnologías avanzadas se pueden adaptar a otras herramientas de seguridad.

Diferencias entre países

No todos los países tienen las mismas leyes en cuanto a privacidad y datos. Por tanto, si damos nuestra información a un tercero para que la guarde, hay que fijarse en dónde tiene sus servidores situados. Muchos permiten elegir. Y es que, mientras los países que pertenecen a la Unión Europea tienen la mencionada regulación para proteger los datos, CloudWards recuerda que Estados Unidos se ha hecho famoso por su espionaje a las informaciones ajenas y por vigilancia gubernamental.

"Para establecer una buena estrategia es importante contar con una solución que resuelva la ecuación de manera sencilla, innovadora y altamente efectiva"

Alberto R. Rodas, Sales Engineer, Sophos Iberia

También considera este experto en cloud como algo poco recomendable almacenar datos en otros países con fuerte intervención del gobierno, como China y Rusia. Y recuerda que hace unos años se descubrió que algunos países como Malasia, Bangladesh, Qatar y Pakistán, usaron spyware o software de vigilancia para acceder a informaciones ajenas.

Por su parte, desde BDO, su portavoz añade que "la localización de la información es un aspecto muy importante. Es necesario identificar proveedores de Cloud que se encuentren localizados dentro del Espacio Económico Europeo o países que de alguna forma garanticen de forma correcta la protección de todos los datos de carácter personal y las garantías jurídicas adecuadas. En cuanto a países fuera del Espacio Económico Europeo que hayan sido declarados con el nivel adecuado de protección por la Comisión Europea, se podrán llevar a cabo transferencias internacionales de datos con la única obligación de incluirlas en el registro de actividades de tratamiento, tal y como indica el artículo 30 del RGPD".

Como empresa europea con sede en el Reino Unido, Sophos explica que ofrece a sus clientes varias localizaciones, y que es el usuarios quien selecciona dónde desea que se almacenen sus datos; si desea que permanezcan en Europa así será, y lo mismo ocurre en América y Asia/Pacífico. Además, añade que hay un extra para mantener la seguridad: "las auditorías periódicas a las que nos someten entidades terceras e independientes garantizan, aún más si cabe, nuestro compromiso con la seguridad de los datos".

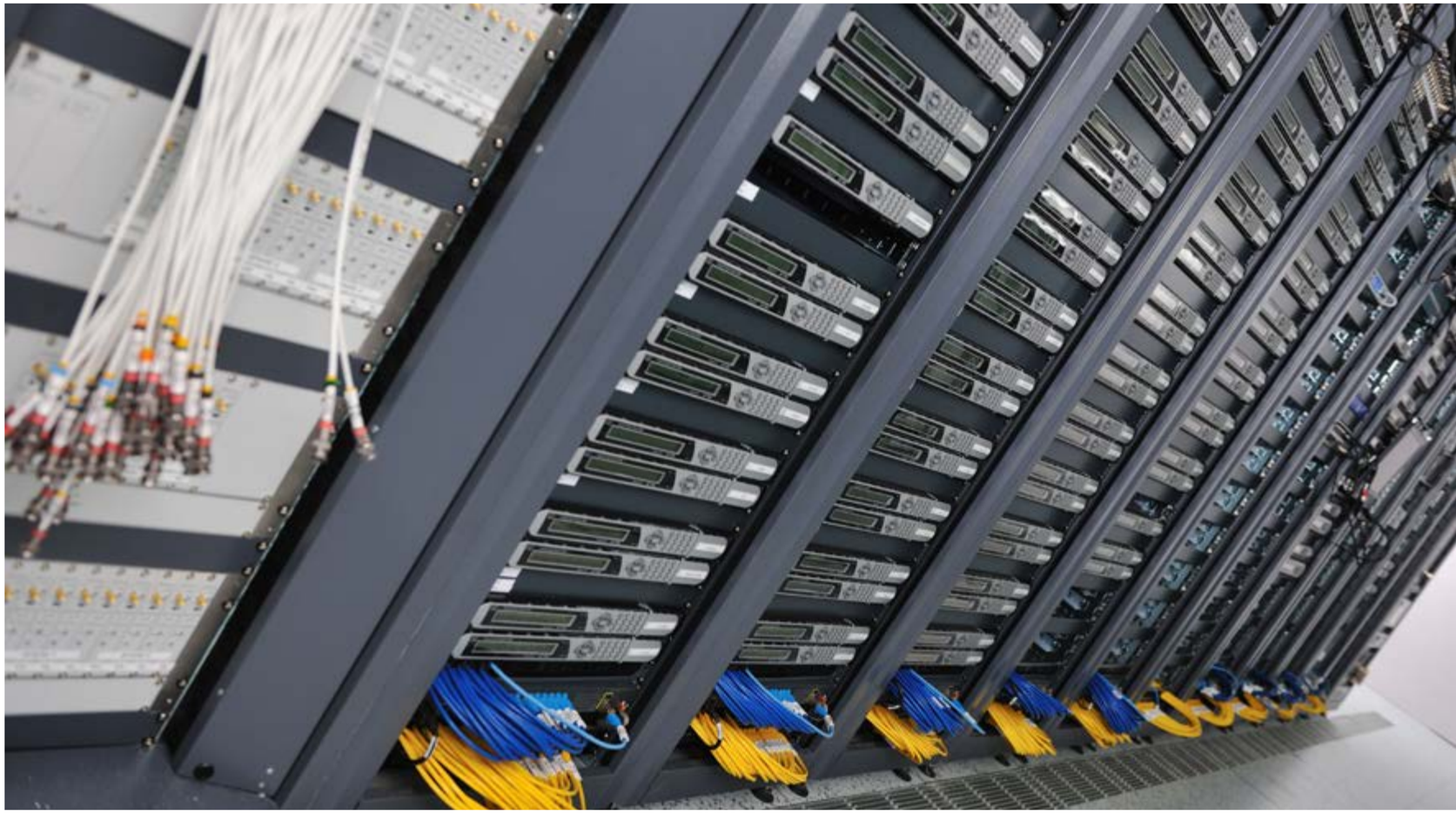
Monetización de esos datos manteniendo la seguridad

Como es lógico, si las empresas guardan esos volúmenes de datos, con el trabajo y el coste que

eso supone, es para darles un valor, que la inversión se convierta en más ingresos a la larga. Los grandes datos pueden servir a una empresa para ofrecer servicios y productos adaptados a lo que es la demanda. La información generada ayudará a conocer al mercado mejor que nunca, y también puede comercializarlos con terceros por temas de publicidad, para que esta sea dirigida.

Sea como fuere el objetivo de los datos, explica Alberto R. Rodas, Sales Engineer de Sophos Iberia, que “en cualquier empresa, la decisión de invertir en seguridad debe ser considerada una acción relevante, en la que los datos funcionan como un activo más. Precisamente por la importancia y por su monetización es fundamental poner el foco de la ciberseguridad sobre ellos”. En Sophos, se establece una doble vía de actuación para mantener al máximo la seguridad y la privacidad. Por un lado, recomiendan contar con soluciones de cifrado automático de datos que pueda cifrar los archivos de forma individual, protegiendo los datos tanto en el ordenador y en los dispositivos de almacenamiento extraíble, como en carpetas compartidas o en la nube, como explica el directivo.

La segunda vía de protección para “por una estrategia de seguridad sincronizada, en las que las soluciones de protección se interrelacionan unas con otras”. “Ya no es suficiente con contar con las mejores soluciones para cada entorno, sino que hay que adaptar y automatizar la protección para conocer cómo se relacionan todos los elementos”, advierte el experto.



La empresa Telefónica explicaba de cara a la implementación de la GDPR el pasado año que “tras el boom del Big Data, ha llegado el momento de demostrar su potencial y aplicaciones reales. Las empresas deben ser capaces de entender el auténtico valor de los datos, pero también las obligaciones que conlleva su gestión”. La monetización de los datos es una línea de negocio en sí misma. Y por tanto requiere de procesos, prácticas y perfiles homogéneos, que permitan maximizar los beneficios a la vez que se respetan unos estándares de seguridad y calidad. Y ahí, un Chief Data Officer, un director de los datos,

> Es crucial entender lo que se intenta proteger antes siquiera de pensar en cómo protegerlo

puede ser una figura clave para encargarse de implementar una estrategia segura.

Para un futuro muy cercano Enrique Turrillo, director de (IT Security) Risk Advisory de BDO, augura que el nivel de confidencialidad y la importancia que tiene un dato para el negocio de una compañía, tiene un mayor valor para la misma, y por lo tanto es más atractivo para la competencia o terceros que puedan hacer un uso de los mismos. Por ello, “en un futuro no muy lejano es más que posible que veamos que se exija que los datos sean registrados y gestionados como un activo más para las compañías, utilizando métodos de valoración incluyendo, entre otras, métricas económicas”.

Otros aspectos básicos cuando se crea una estrategia de gestión de grandes datos

Existen aspectos fundamentales a la hora de planificar una estrategia sobre cómo gestionar los datos. Entre ellos destaca Turrillo que es esencial “definir una serie de políticas, normas y procedimientos del gobierno de los datos, en los que se incluyan roles, responsables y tecnología necesaria para tratar dichos datos. También servirá para hacer un seguimiento de que estas se cumplen y resolver los posibles problemas que pudiesen ocurrir”.

> La era digital ha llegado acompañada de una infinidad de nuevas oportunidades para la creación e innovación de nuevos productos y servicios

Otro aspecto que esta empresa considera esencial es el de “definir una arquitectura corporativa de datos donde se detallen: la configuración de las bases de datos, forma de almacenamiento de los datos (Cloud por ejemplo) o el modelo de integración de los datos, entre otros”, explica el directivo.

La gestión de la seguridad de los datos y gestionar la calidad e integridad de los datos, también son elementos clave a no perder de vista ya que “es muy importante que los datos sean válidos, íntegros, consistentes, completos y unívocos, por lo tanto, se necesitan técnicas que evalúen, mejoren y puedan asegurar que los datos son correctos”.

Por otro lado, como ya publicó IT Digital Security, la integridad de los datos garantiza que los usuarios autorizados pueden acceder o modificar la información. Un ataque a la integridad de los datos compromete esa seguridad, con el objetivo de obtener acceso no autorizado para modificar datos por una serie de razones, tales como obtener ganancias financieras, hacer daño a la reputación o simplemente hacer que los datos no tengan valor. Y, en ese sentido, la empresa Palo Alto Networks recomendaba cuatro asuntos muy importantes que las empresas deben tener en cuenta.

Uno de los principales aspectos cuando implementemos una estrategia adecuada para el manejo de datos pasa por “educar a los empleados y clientes sobre los pasos que deben seguir para mantenerse seguros y proteger sus datos personales”. Siempre, tras comprender “qué datos tiene, cómo se recopilan y producen, y dónde se sientan las partes más sensibles de esos datos. Es crucial entender lo que se intenta proteger antes de siquiera pensar en cómo protegerlo”, explicaba la mencionada firma.

También es importante hacer uso de los avances tecnológicos para asegurar la protección como es la autenticación multifactor, que proporciona una capa adicional de seguridad. Finalmente, “utilizar el cifrado para proteger los datos confidenciales, ya sea a nivel local, en la nube pública o en un entorno híbrido. El cifrado es tan bueno como la estrategia de gestión de claves empleada”.

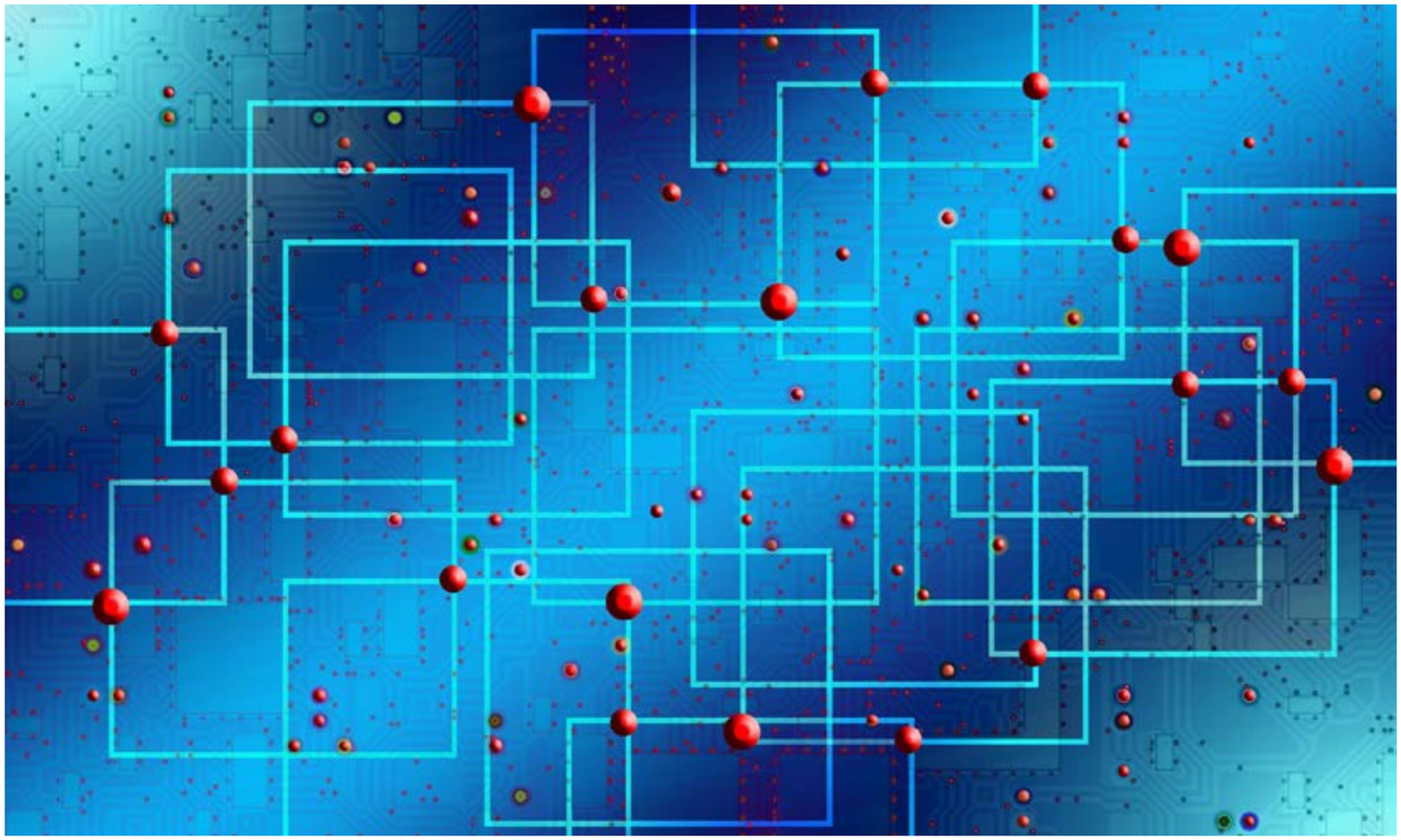
Herramientas de seguridad como pilar fundamental de apoyo

Para concluir este análisis, desde Sophos cuenta Alberto R. Rodas que “uno de los principales riesgos que corren las empresas actualmente es la falta de estrategias de seguridad integrales, y en estas estrategias, los datos son una parte fundamental. Precisamente por ser un activo valioso dentro de una empresa, son también un objetivo vulnerable frente a ciberataques”.

Además de la necesidad de buenos socios y de unos empleados que sepan lo que hacen cuando tienen los datos entre manos, “para establecer una buena estrategia es importante contar con una solución que resuelva la ecuación de manera sencilla, innovadora y altamente efectiva. Ya no sólo es importante que las empresas cuenten con un sistema de seguridad por capas que cubra todos los componentes del sistema de TI, como el correo, la red, la navegación web, los dispositivos móviles, etc., sino que también es fundamental que todas las soluciones de seguridad sean capaces de hablar entre sí, compartiendo información sobre cualquier incidente de seguridad para aumentar la fiabilidad”, explica el directivo.

Enlaces de interés...

- Big Data e IoT, utilizadas en la prevención de ciberataques en infraestructuras críticas
- Tener una estrategia sólida y detectar patrones, entre las grandes preocupaciones de las empresas en seguridad
- Un 64% de las grandes empresas españolas se enfrentaron a un ciberataque en los últimos dos años



¿Confía en la seguridad de sus datos alojados en nubes públicas?

Vea y proteja todo con Sophos Cloud Optix. Combine el poder de la IA y la automatización para simplificar el cumplimiento, administración y monitorización de la seguridad en la nube.

Sophos.com/es/cloud-optix

Cloud Optix

SOPHOS

Cybersecurity evolved.

‘Los CISO en España sienten una presión muy elevada para optimizar sus presupuestos’ (Deloitte)

Presentaba recientemente Deloitte un informe que recoge las preocupaciones de los responsables de seguridad de las empresas, los CISO, en base a una encuentra realizada a más de medio centenar de empresas españolas u organizaciones cuya base de operaciones de seguridad reside en España.

"Las preocupaciones del CISO", que así se llama el informe, recoge, entre otras cosas, que tres de cada cuadro compañías españolas ha sufrido un ciberincidente en los últimos 6 meses y que el 30% de las empresas considera que está poco o nada preparado para afrontar un ciberincidente.

Los resultados, que iremos enumerando no ha sorprendido a Deloitte. Dice Miguel Olías, gerente de Risk Advisory de la compañía que se esperaban datos "más o menos similares", lo que no significa que no hayan encontrado datos destacables, como que aquellos sectores más maduros y, a su vez, más regulados, destinan un porcentaje muy elevado a la Estrategia y Gobierno frente al resto de funciones. Sabíamos que la apuesta por esta área era alta pero no creíamos que fuera a estar por encima del 30% respecto al resto de funciones".

También preguntamos a Miguel Olías si los datos del informe reflejan que las preocupaciones de los CISOs españoles difieren de las de otros países. No es así. Las preocupaciones son similares, aunque "en otros países la preocupación por grupos hacktivistas, el ciberterrorismo o los propios riesgos geopolíticos va variando".

Destaca en todo caso el ejecutivo de Deloitte que "en los últimos tiempos, los CISOs en España sienten una presión muy elevada para optimizar sus presupuestos" y que mucho responsables de seguridad de las empresas "se han lanzado a la búsqueda de ayuda para consolidar diferentes tecnologías, automatizar procesos y buscar fórmulas para gestionar de forma correcta las operaciones".

Recoge el informe que el 76% de las empresas españolas, o compañías cuya base de operaciones de seguridad se encuentra en nuestro país, ha

El 71% de las empresas que se sienten poco o nada preparadas para hacer frente a un incidente de seguridad opta por la opción del ciberseguro

"El sector energético está haciendo bastantes esfuerzos en materia de ciberseguridad"

Miguel Olías, gerente de Risk Advisory, Deloitte

tenido un ciberincidente con consecuencias significativas en los últimos seis meses. A pesar de ello, y aunque el número de ciberamenazas ha aumentado progresivamente, así como su probabilidad e impacto, las empresas afirman haber sufrido menos ciberincidentes en el año 2018 que en 2017, según afirma el 62% de las empresas.

El dato pone de manifiesto que existe una relación directa entre el aumento progresivo de los ingresos de las empresas y el incremento en el número de ciberataques que sufren. "Por fin tenemos datos objetivos que demuestran que a mayor inversión de recursos en ciberseguridad menor número de incidentes", dice Miguel Olías, añadiendo también que el dato varía según el tamaño de la empresa porque "las compañías se convierten en un objetivo más frecuente para los atacantes según van aumentando su tamaño, además de incrementar el número de ataques que sufren debido a que su superficie de exposición aumenta al mismo tiempo".

En este sentido y según el informe, las empresas que facturan entre 2.000 y 5.000 millones de euros son las que experimentan un mayor número de incidentes al año, prácticamente cuatro. No obstante, a partir de un punto elevado de ingresos –más de 5.000 millones de euros- el número de ataques desciende, debido a las medidas preventivas y a una mayor inversión en ciberseguridad.

Ciberseguros

Entre las principales conclusiones de la encuesta, se destaca también que el 89% de las empresas que tienen un ciberseguro no lo ha tenido que utilizar nunca. Por otro lado, el 71% de las empresas que se sienten poco o nada preparadas para hacer frente a un incidente de seguridad opta por la opción del ciberseguro.

Según Miguel Olías, "se ha evidenciado que las compañías pequeñas-medianas tienen una gran predilección por el ciberseguro", y añade el gerente de Risk Advisory de Deloitte que esto "no excluye que las grandes también hagan uso de los mismos, sino que la empresas más pequeñas y medianas encuentran en los ciberseguros una forma adicional de transferir el impacto económico de los ciber-riesgos a través de un tercero que suele encajar bien en su programa de ciberseguridad. Estas empresas disponen de menores presupuestos en ciberseguridad y, por tanto, acuden a esta medida de control para intentar gestionar los futuros ciberincidentes".

Sectores

Comentábamos que el informe de Deloitte pone de manifiesto que aún existe un porcentaje de empresas españolas que carece de confianza a la hora de enfrentarse a un ciberataque, que el 30% de las empresas considera que está poco o nada preparada para hacer frente a un incidente de seguridad.

El sector de la banca, según afirma el 86%, es el que se siente más preparado a la hora de enfrentarse a un ciberataque. Asimismo, el 83% de las empresas del sector banca alinea su estrategia de ciberseguridad con el negocio, liderando esta coordinación.

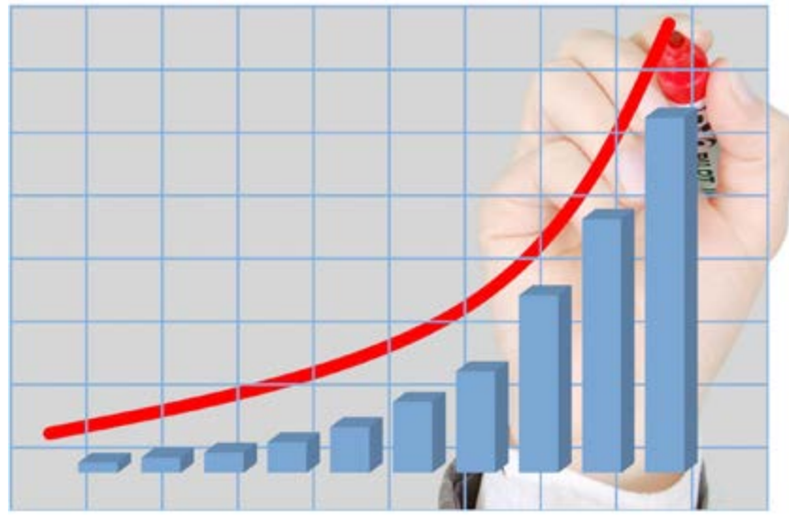
LAS PREOCUPACIONES DEL CISO

El siguiente estudio viene a compartir con la sociedad el estado de la ciberseguridad en las empresas españolas. Gracias a esta información, las empresas pueden conocer más de cerca como están dimensionadas y como están trabajando otras empresas en materia de ciberseguridad, en muchos casos a nivel sectorial.

En el sector energético, un ámbito crítico y de relevancia estratégica para nuestro país, menos de la mitad, concretamente el 47%, de las empresas se sienten preparadas para afrontar un incidente de seguridad. En este mismo sector un 93% de responsables de seguridad menciona la interrupción de las operaciones de negocio como su principal preocupación.

Sobre el sector energético dice Miguel Olías que "está haciendo bastantes esfuerzos en materia de ciberseguridad". Explica el ejecutivo que históricamente, y tanto aquí en España como en Europa, ha sido un sector menos regulado en materia de ciberseguridad con respecto a otros como la banca, lo que ha llevado a que la alta dirección haya sentido "menos presión por invertir en ciberseguridad". No obstante, "normativas como LPIC o la NIS ponen el foco de atención en la criticidad de este sector como uno de los que son clave para el buen funcionamiento del país. Esto está haciendo que cada vez se vaya tomando más conciencia en materia de ciberseguridad y que la inversión vaya aumentando".

Reconoce también Miguel Olías que el energético se enfrenta a la convergencia OT/IT, lo que aumenta la superficie de ataque y la exposición ante las ciberamenazas. Algo que Olías define como "un reto relevante" porque no hay que olvidar que "sigue habiendo una importante cantidad de tecnología legacy en el mundo OT que, además, está directamente gestionada por los proveedores y que merma la capacidad de gobierno desde el área de ciberseguridad".



Dentro del sector consumo y distribución, el 67% de las empresas afirma estar preparada para recibir un ciberataque

Por su parte, dentro del sector consumo y distribución, el 67% de las empresas afirma estar preparada para recibir un ciberataque.

Inversión en ciberseguridad

Los datos que recoge el informe señalan que las empresas españolas dedican a ciberseguridad una media del 8,5% del presupuesto destinado a IT/OT. Dentro de esta partida, deciden invertir mayor cantidad en Protección (40%); Vigilancia (26%); y, por último, en Resiliencia (18%) y Gobierno (15%).

Las empresas que invierten más del 10% del presupuesto de IT/OT en ciberseguridad reportan 0,6 incidentes de seguridad al año de media, mientras que las que dedican menos del 10% experimentan 3 incidentes por año.

Para Miguel Olías, gerente de Risk Advisory de Deloitte, “la diferencia entre ambos rangos es bastante notable, llegando a cuadriplicar el número de incidentes, lo que recalca la importancia de establecer un presupuesto adecuado para minimizar los impactos en caso de un ciberincidente o ataque”.

Tecnologías

Algunas de las tecnologías exponenciales que se están aplicando en el mercado tienen una relación muy estrecha con la ciberseguridad.

En este sentido, se puede observar que tecnologías como Inteligencia Artificial, Machine Learning o Algoritmos Predictivos están plenamente implantadas en la seguridad cibernética, ya que se usan como herramientas avanzadas para examinar grandes cantidades de información y reconocer, así, posibles amenazas.

En relación con IoT, esta tecnología también está presente en la estrategia de ciberseguridad de la empresa, tal como afirma el 86% de las empresas. Al respecto del IoT dice Olías que “la tecnología IoT abre un nuevo paradigma”, y que “por primera vez el mundo físico y el mundo lógico conviven, rompiéndose de esta manera la frontera entre lo terrenal/lo humano y lo digital/la máquina. Hasta hace relativamente poco hemos inundado nuestros hogares y ciudades con smartwatchs, asistentes de hogar (Alexa, Google Home…), drones, aspiradores inteligentes, coches inteligentes, edificios inteligentes, etc. Es la primera vez que con un simple script puedes controlar acciones del mundo físico. Esto abre un nuevo debate, el de empezar a hablar de ‘seguridad’ como un término holístico, puesto que

Tres de cada cuadro compañías españolas ha sufrido un ciberincidente en los últimos 6 meses

Enlaces de interés...

- No creemos en la cultura del miedo
- Un 58% de los CISO están preocupados por la expansión sin control de la nube
- El 25% de las empresas del sector turismo ya tienen CISO
- CEO, CIO, CISO, ¿quién responde por la seguridad de la empresa?

las amenazas empiezan a ser híbridas y las medidas del cybersecurity y safety no deben verse de forma aislada".

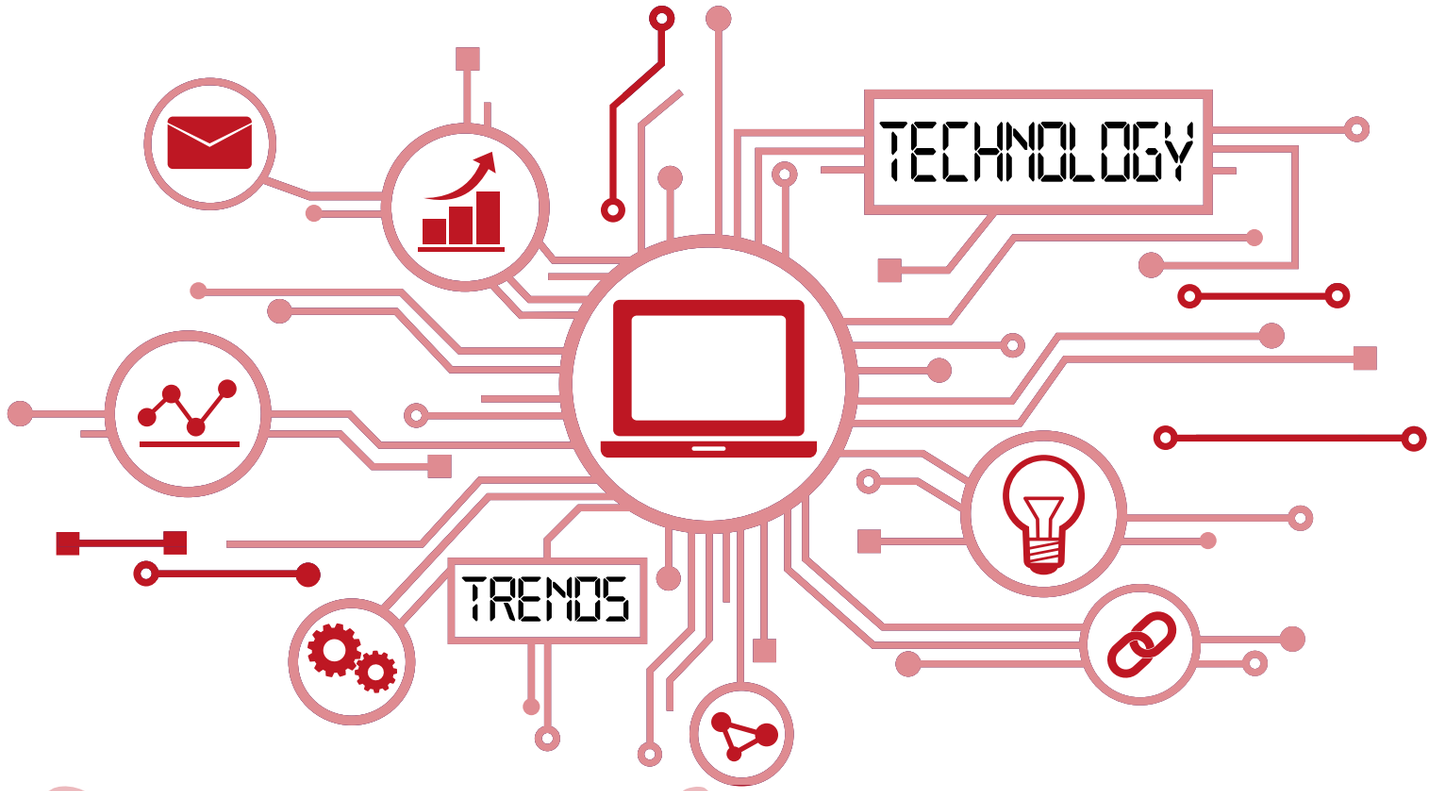
Dice también el gerente de Risk Advisory de Deloitte que la ciberseguridad en IoT implica el análisis de los riesgos más allá del perímetro de la empresa, puesto que en el mundo físico (edge) esta tecnología recibe y captura información que es enviada a través de Internet y que puede ser recogida por nubes, no propietarias de la propia compañía, para finalmente llegar toda esta información al perímetro de la red interna. "Esta nueva visión de entender la ciberseguridad tras la ruptura tradicional del perímetro de la empresa requiere de un nuevo enfoque en las estrategias de defensa de las compañías y estas, aunque muchas medidas no han podido ser aun implantadas, lo contemplan en su estrategia de ciberseguridad de esta forma".

En cuanto a las tecnologías menos utilizadas, menos del 20% de los servicios que son imprescindibles o críticos para la empresa están alojados en la nube, ya que las empresas prefieren mantenerlos 'In House'.

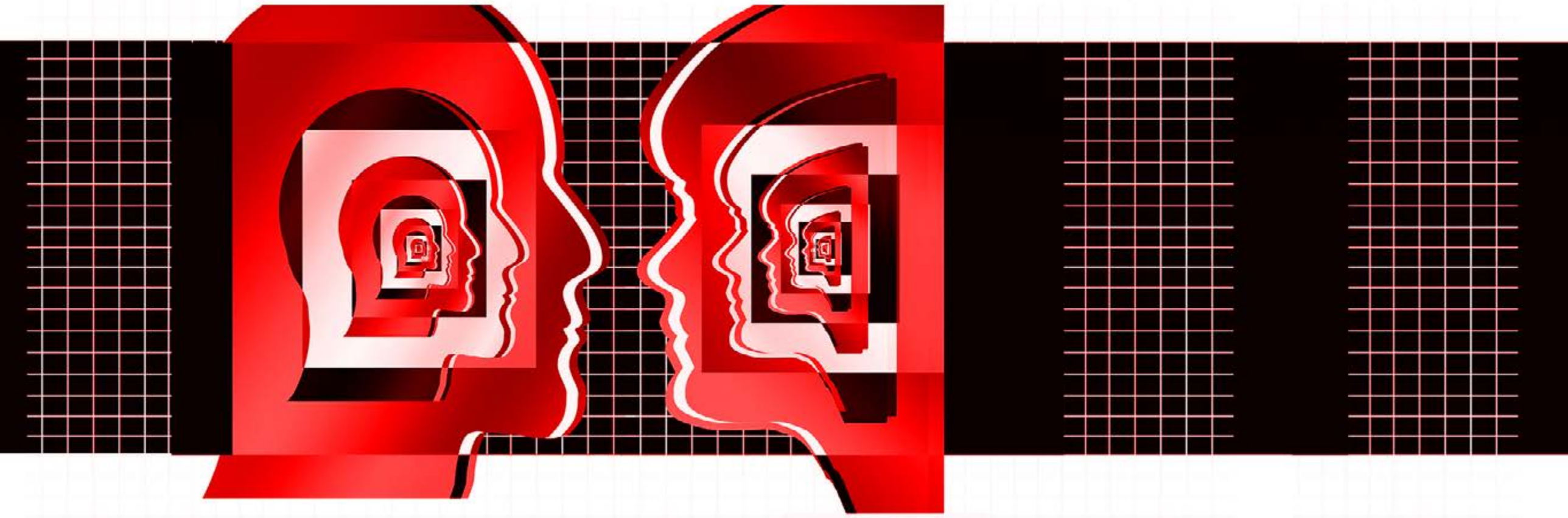
Por último, se ha verificado que el 95% de los sectores tienen poca o ninguna implicación de la tecnología Blockchain en la ciberseguridad de su empresa.

Encuentros it TRENDS

Las tendencias TIC para la empresa digital
de la mano de los líderes del sector



Protección y visibilidad frente al mayor riesgo de ciberseguridad: el usuario



¿Quién puede hacer qué?

Jaime Velázquez

La gestión de acceso delegada y el manejo de identidades se imponen como mecanismos de seguridad básicos para el control de credenciales en redes cada vez más porosas y con multiplicidad de usuarios.

"The House of Wolf', era un simple pub de Islington, en norte de Londres. Otro bar más, totalmente corriente y anónimo. Y así es como a sus propietarios les hubiera gustado que permaneciera; conocido sólo por aquellos que lo frecuentan. La cosa cambió cuando despidieron a uno de sus empleados. El trabajador, enfadado con el establecimiento, utilizó las contraseñas de acceso a las cuentas de redes sociales y la página web del House of Wolf, para vengarse de sus antiguos jefes.

Bloqueó la página web y exigió un rescate para liberarla, y en las cuentas de Facebook y Twitter, pidió a los clientes que no acudieran al pub. "Aguamos la cerveza", escribió en las redes sociales. "Nos encanta tratar bien al cliente. Ah, no, espera… No somos más que unos bastardos que timamos a la gente".

La mayor amenaza no procede de sofisticados ciberataques, sino de un uso indebido de credenciales legítimas

Los daños para 'The House of Wolf' fueron irreparables. Pero estos incidentes no sólo ocurren en pequeños negocios. En 2013, los trabajadores de His Master's Voice (HMV), la cadena de tiendas de música británica, se hicieron con el control de la cuenta de Twitter de la compañía para denunciar los despidos masivos que estaba llevando a cabo la empresa.

Son sólo dos ejemplos de algo que los responsables de seguridad ya saben: la mayor amenaza no procede de sofisticados ciberataques, sino de un uso indebido de credenciales legítimas. Sin ir más lejos, un estudio de la consultora Switchfast revela que uno de cada cinco empleados comparte sus contraseñas de acceso al correo con otros compañeros de trabajo y el 66% de los directores de pymes americanas se conectan a redes públicas para trabajar.

Ya sea para contener los posibles daños de reputación, o impedir el robo de datos sensibles para la compañía, la gestión de identidades y el acceso delegado, se imponen como una exigencia en el nuevo panorama de seguridad. ¿Qué pasaría si esas credenciales caen en manos de criminales, o simplemente quedan a disposición de un empleado despechado?

"Mi presencia en LinkedIn está directamente relacionada con la actividad de nuestra compañía y la relación con nuestros prospectos, clientes y partners. En consecuencia, mi perfil social constituye un importante activo digital que debe ser salvaguardado y utilizado de forma inteligente. Esto es extrapolable a otras redes sociales, así como cualquier perfil profesional cuya actividad en las redes pueda ser percibida como un ejercicio de comunicación corporativa", explica, Ignacio Gilart, CEO de la compañía de seguridad WhiteBearSolutions.

"Por esa razón, el acceso y la gestión de todas estas cuentas debería tener lugar de una forma ágil y, sobre todo, segura. Pero desgraciadamente, en la práctica, son muchas las empresas que exponen

La gestión de acceso delegada permite que los empleados puedan acceder con un solo clic y de forma segura a todos y cada uno de sus perfiles sociales, sin necesidad de exponer sus credenciales

estas credenciales innecesariamente, o bien permiten que los accesos tengan lugar de una forma insegura y poco eficaz".

La gestión de numerosas cuentas hace que los empleados deban recordar un gran número de contraseñas –incluyendo las de los perfiles sociales-, lo que puede dar lugar a errores y ralentización en la realización de las funciones propias de un puesto.

"En caso de que una cuenta se vea comprometida y los datos de acceso terminen en manos de una persona no autorizada, podría tener lugar un abuso en la utilización del perfil social afectado y el consiguiente daño a la reputación e imagen corporativa de la organización" advierte WhiteBearSolutions en su blog corporativo.

La gestión de acceso delegada permite que los empleados puedan acceder con un solo clic y de forma segura a todos y cada uno de sus perfiles sociales, sin necesidad de exponer sus credenciales, y compartir los accesos a los perfiles de las redes sociales con aquellos a los que se atribuya la función de gestionarlas, sin necesidad de que conozcan los detalles de las credenciales, como pudieran ser el nombre de usuario o la contraseña.

"Mediante la utilización de un sistema de gestión de acceso delegado como el de SmartLogin, el responsable de estas tareas, podrá acceder a un portal de control central, desde el que ingresar fácilmente a cada uno de los perfiles corporativos, sin necesidad de conocer las credenciales de acceso de éstos, ni disponer de autorización para modificarlos", explica la compañía sobre su solución de gestión de identidades aplicada al manejo de redes sociales.

La gestión de identidades, más allá de la mera autenticación

La gestión de identidades va más allá de la mera autenticación de los usuarios, sino que permite conocer cuáles son los roles de esos usuarios, y por tanto establecer de forma automática las credenciales de acceso dependiendo de cuál sean sus funciones en cada momento.

Según un informe citado por CA Technologies, el 87 % de las organizaciones consideran que se

les concede a las personas demasiadas posibilidades de acceder a recursos de información que no son pertinentes para las características de su puesto de trabajo. El 61 % de las organizaciones no comprobaban las solicitudes de acceso con las políticas de seguridad antes de autorizar y asignar los accesos.

Gestionar las identidades de usuario y su acceso a la información esencial durante el ciclo de vida de los servicios implica muchos procesos distintos, incluidos la incorporación o integración, la gestión de contraseñas, el autoservicio, las solicitudes de servicios y la certificación de accesos.

"En muchas organizaciones, estos procesos se realizan manualmente o solo están parcialmente automatizados. Gracias a la automatización, la organización puede reducir los costes administrativos y disminuir los riesgos para la seguridad provocados por procesos manuales o incoherentes. Las soluciones de control y gestión de identidades también ofrecen controles de seguridad adicionales, como autorizaciones de flujos de trabajo, políticas de segregación preventiva de funciones o control y auditorías de accesos basados en roles, todos destinados incrementar la seguridad y simplificar los procesos de la organización", explica la compañía americana CA Technologies, que ofrece soluciones de gestión a través de su consola CA Identity Suite.

"La mayoría de las organizaciones abordan los requisitos de seguridad internos y normativos ex-

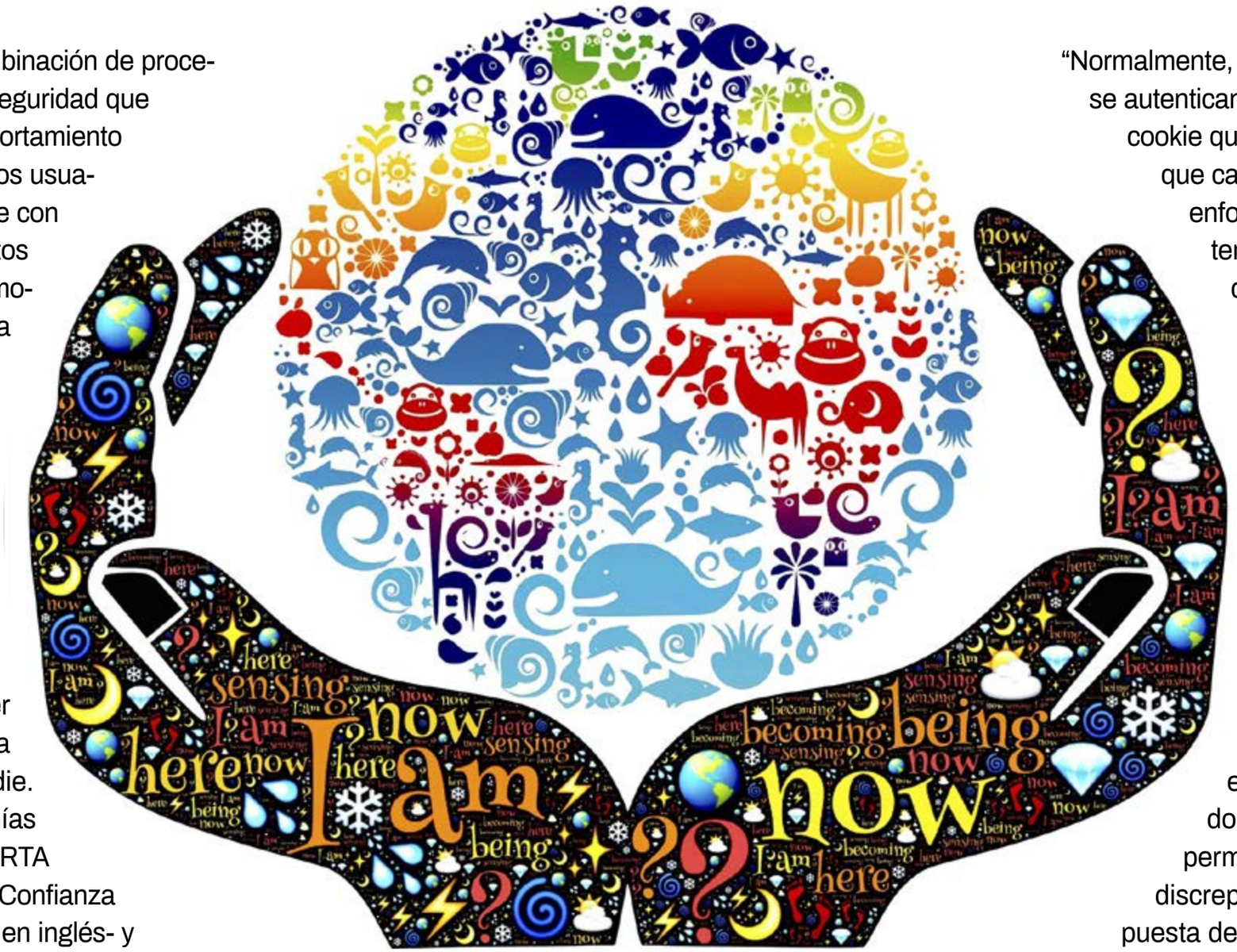
Cada vez más compañías aplican los conceptos CARTA -Evaluación Continua de Confianza y Riesgos, por sus siglas en inglés- y Zero Trust -confianza cero- para garantizar la veracidad de las identidades y el acceso a los datos

ternos mediante una combinación de procedimientos y políticas de seguridad que estipulan cuál es el comportamiento adecuado y validan que los usuarios cuentan regularmente con un acceso apropiado. Estos procesos requieren una monitorización proactiva para detectar accesos o actividades indebidas en los sistemas empresariales".

No se trata sólo de contar con un sistema robusto de autenticación de usuarios, sino de garantice de manera continua su autenticidad, incluso después de haber hecho log-in. La consigna es clara: no fiarse de nadie.

Cada vez, más compañías aplican los conceptos CARTA -Evaluación Continua de Confianza y Riesgos, por sus siglas en inglés- y Zero Trust –confianza cero- para garantizar la veracidad de las identidades y el acceso a los datos. Según Gartner, el 25% de las nuevas iniciativas digitales en 2020 incorporarán una estrategia CARTA, en comparación con el 5% de 2017.

Este tipo de aproximaciones a la seguridad, como Zero Trust, parten de una clara premisa: eliminar la idea de que existe una red fiable dentro de un perímetro corporativo definido, incluso dentro de las propias instalaciones 'on-premises', explica la empresa ForgeRock, especializada en gestión de identidades.



"Normalmente, a medida que los usuarios se autentican, se les otorga un token o cookie que permite el acceso hasta que caduque o sea revocado. Los enfoques modernos para la autenticación incluyen la captura de contexto en el momento del inicio de sesión: ubicación, tipo de navegador, dirección IP y muchos otros factores", explica Simon Moffatt, director de gestión de productos de ForgeRock.

El enfoque de ForgeRock es validar continuamente no solo que el token es válido y activo, sino también que el contexto que daba cuando se emitió el token todavía permanece. "Si se encuentran discrepancias, la tradicional respuesta de denegar el servicio se puede sustituir por otra de acceso limitado a una serie de funciones".

El reto de la movilidad y los servicios en la nube

Las empresas están cada vez más inmersas en procesos de movilidad para ejercicio de las tareas profesionales, también lleva implícito una eficaz

"La utilización del phishing, el baiting u otras técnicas similares permiten a los delincuentes hacerse con las credenciales de acceso de los usuarios de tu organización"

Ignacio Gilart, CEO de WhiteBearSolutions

gestión de la seguridad y del riesgo por parte de las mismas. Para ello, existen sistemas integrados de procesos, políticas y tecnologías que facilitan y controlan el acceso de los usuarios a sus recursos y aplicaciones, además de proteger su información confidencial, tanto personal como profesional, de usuarios no autorizados.

"En este contexto de optimización del flujo de trabajo en diferentes entornos, donde se permite a los empleados trabajar desde cualquier sitio y en cualquier momento con un dispositivo, conceptos como autenticación, cifrado, gestión eficaz de claves o gestión de eventos de seguridad se hacen tan imprescindibles como necesarios para acceder a herramientas y servicios de la empresa", escribe Ignacio Gilart, CEO de WhiteBearSolutions.

La mayoría de los empleados no son conscientes de que sus acciones, aparentemente inocentes, ponen a su organización en un riesgo significativo de una posible violación de datos. Por ejemplo, los empleados que trabajan los fines de semana en una cafetería, son susceptibles de ser víctimas de piratas informáticos que buscan lanzar ataques "man in the middle" o distribuir malware gracias a que acceden a servidores privados a través de redes inalámbricas abiertas. Y las políticas de 'Bring Your Own Device" no hacen más que ampliar las vulnerabilidades.

Según Gartner, el 25% de las nuevas iniciativas digitales en 2020 incorporarán una estrategia CARTA, en comparación con el 5% de 2017

Enlaces de interés...

- La autenticación biométrica en el móvil impulsará la adopción de IAM como servicio
- Consolidación en el mercado de PAM, o de gestión de accesos con privilegios
- Proteger la identidad de las máquinas cada vez más importante
- One Identity se alía con Exclusive Networks para impulsar el mercado de gestión de identidades

"La utilización del phishing, el baiting u otras técnicas similares permiten a los delincuentes hacerse con las credenciales de acceso de los usuarios de tu organización y llevar a cabo una violación de seguridad de una forma mucho más inadvertida. Es entonces cuando lo idóneo es disponer de un sistema de autenticación adaptativa, el cual aplique nuevas capas de seguridad y control de accesos, especialmente, cuando la infraestructura IT se encuentra en la nube", añade Gilart.

"En el momento en que trasladas tus aplicaciones, sistemas de control de accesos y el resto de la infraestructura IT de tu negocio a la nube, tu perímetro de seguridad se abre de forma exponencial. Hasta ese momento, dicho perímetro podía mantenerse relativamente cerrado y bajo control mediante, por ejemplo, el firewall del sistema. Con el traslado a la nube, el panorama cambia por completo" explica el CEO de WhiteBoard-Solutions.

Mediante la autenticación adaptativa que propone WhiteBearSolutions, es posible permitir que, en un momento dado, un empleado acceda a unas determinadas aplicaciones o servicios en la nube y lo haga desde un conjunto de IPs seguras, como puedan ser las correspondientes a la oficina.

"En el caso de que ese usuario utilice los mismos mecanismos de acceso pero, en lugar de la oficina, lo haga desde su casa, el sistema de control de accesos es capaz de detectar que aquel no está operando en una red segura y restringir el acceso o bien aplicar mecanismos de seguridad complementarios como, por ejemplo, un doble factor de autenticación con un código de único uso, etc. Esa es una de las principales fortalezas de SmartLogin, nuestra plataforma de gestión y control de accesos".

Global Phish Report 2019

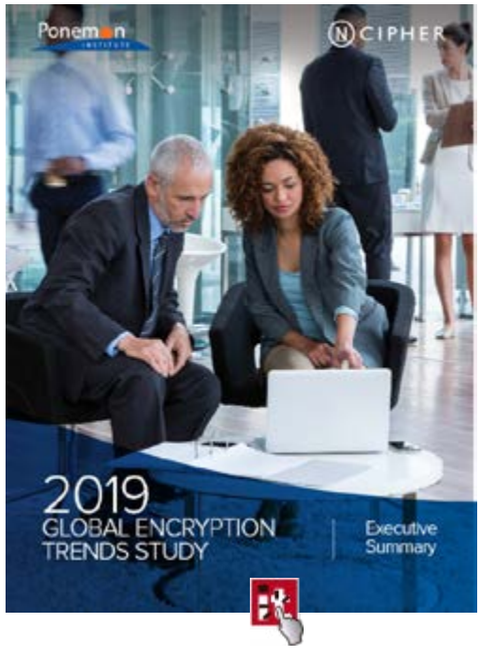
Durante la última década, los ataques de phishing se han convertido en la amenaza de correo electrónico más extendida para las organizaciones de todo el mundo. A medida que las soluciones de seguridad diseñadas para bloquear estos ataques se han vuelto más avanzadas, la sofisticación de estos ataques ha seguido su ritmo, evolucionando para evadir la detección.

La tecnología basada en la nube, con todos sus beneficios, ha dado paso a una nueva era de ataques de phishing. Entre otras cosas, este estudio recoge que más del 30% de los correos electrónicos de phishing enviados a organizaciones que utilizan Office 365 Exchange Online Protection llegaron a la bandeja de entrada.

Tendencias de Cifrado 2019

A medida que las organizaciones adoptan la nube y las nuevas iniciativas digitales, como IoT, blockchain y pagos digitales, el uso del cifrado para proteger sus aplicaciones e información sensible está en su punto más alto.

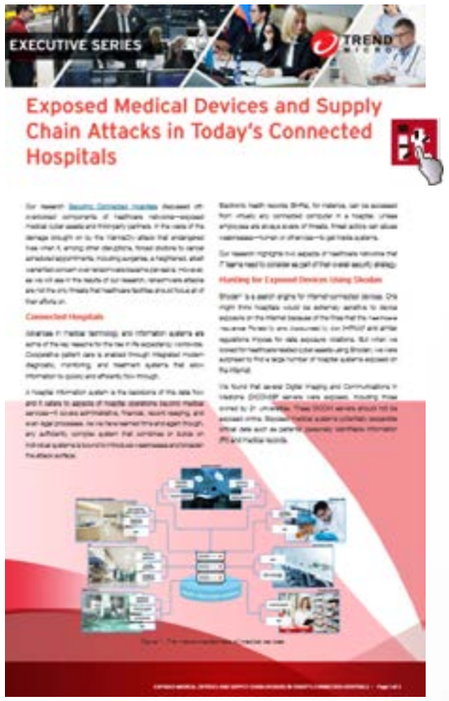
Entre los datos que recoge el informe destaca que el descubrimiento de datos continúa siendo el mayor desafío en la planificación y ejecución de una estrategia de cifrado de datos (69% de los encuestados). Además, la policía de aplicación se considera la característica más importante de las soluciones de cifrado, mientras que para un 60% de empresas ya utilizan HSM para proporcionar cifrado como servicio (hardware security modules).



Dispositivos médicos y ataques a la cadena de suministro

Las amenazas de la cadena de suministro son riesgos potenciales asociados con los proveedores de bienes y servicios para organizaciones de atención médica donde se puede filtrar información confidencial o confidencial, introducir una función o diseño no deseado, interrumpir las operaciones diarias, manipular datos, instalar software malicioso, introducir dispositivos falsificados y afectar la continuidad del negocio.

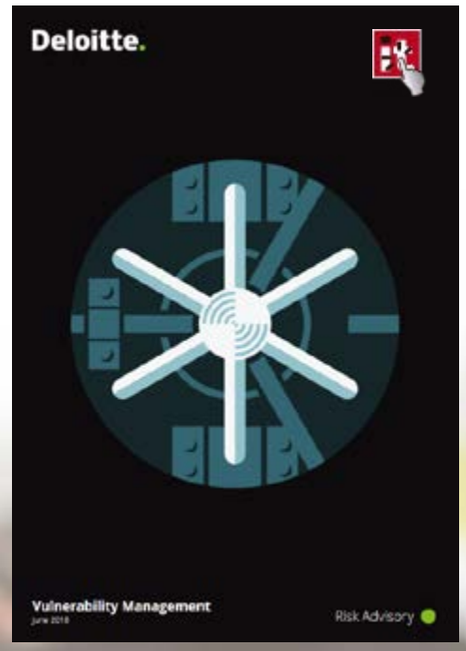
Este documento ofrece una serie de recomendaciones para asegurar la cadena de suministro, como realizar evaluaciones de vulnerabilidades de los nuevos dispositivos médicos, establecer programas de BYOD, desarrollar un plan para el parcheo y actualización del firmware de los dispositivos implantados, etc.



La Gestión de Vulnerabilidades

Es imperativo para cualquier organización implementar una Gestión de Vulnerabilidades efectiva para protegerse contra ataques y amenazas.

La gestión de vulnerabilidades es un resultado maduro de una práctica temprana de evaluación de vulnerabilidad. El panorama de amenazas de hoy es inimaginablemente diferente, con miles de nuevas vulnerabilidades reportadas cada año y la creciente complejidad del entorno de la organización. Diferentes informes sobre brechas de seguridad muestran un claro aumento en el número de vulnerabilidades identificadas y la forma de explotarlas.



La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

Seguridad Web y del eMail

Internet se ha establecido como una herramienta fundamental para romper las barreras geográficas y limitaciones de cualquier proceso de negocio. Una protección eficaz de la navegación web requiere ser capaz de evolucionar y adaptarse a la vez que lo hacen las diferentes amenazas: requiere control a través de un filtrado web dinámico y multicapa; prevención a través de configuración de políticas y, por supuesto, una gestión centralizada.

Desayuno ITDS

SEGURIDAD WEB Y DEL EMAIL — **CLICAR PARA VER EL VÍDEO**

El correo electrónico es uno de los principales vectores de ataque y uno de los primeros recursos de la empresa en haberse ido a la nube. Los famosos ataques BEC o el phishing son algunas de las amenazas que te esperan si no estás protegido. ¿Cómo está evolucionando esta tendencia en España? ¿Cuán protegidas están las empresas frente al phishing o el spam? La empresas española, presta atención suficiente a la seguridad del correo electrónico y la navegación web? Estas y otras preguntas son las que hemos hecho a un grupo de expertos en el marco de un debate en el que han participado Andrés García, Country Manager de Retarus en España; Alberto Rodas, director preventa de Sophos Iberia y Miguel Angel Martos, Country Manager de Symantec Iberia.

Empezamos preguntando a nuestros expertos si, siendo el correo electrónico una de las primera infraestructuras empresariales que se han externalizado y llegado a la nube, ¿se ha hecho con la seguridad adecuada? Para Andrés García, depende de la inversión. Se calcula que el 95% de los ataques entran por el email, y sin embargo sólo se le dedica el 2% del presupuesto en seguridad; “creemos que se debería invertir un poco más”.

Alberto Rodas tiene claro que las empresas terminan añadiendo una capa externa de seguridad cuando deciden llevar su correo electrónico a proveedores externos, aunque a veces tardan en darse cuenta. Miguel Ángel Martos también está de acuerdo en que no se está invirtiendo todo lo que se debiera, asegurando al mismo tiempo que no se trata de invertir más, sino de manera continuada; “nos tenemos que plantear un modelo en el que no

> No se trata de invertir más en seguridad, sino de manera continuada

"Cualquier política de seguridad tiene tres caras: la tecnología, los procesos y las personas, y no hay que descuidar ninguna de las tres"

Miguel Ángel Martos, Country Manager, Symantec

sea una única inversión sino un acompañamiento durante un tiempo".

En relación con las amenazas más críticas que afectan a las páginas web, dice Alberto que lo que se está viendo son procesos de renderización de la web, un ataques que recientemente se ha visto en una conocida cadena de comida rápida en España, infectada desde hace más de un mes. "En cualquier caso hay que abrir dos vías. Una vía es la protección de esos sistemas web, que den esa capa extra de seguridad, pero luego los propios usuarios que hacen click en cualquier cosa. Es necesario contar con un sistema que controle esa navegación, que controle lo que van a descargar, y lo pueda analizar correctamente".

Recuerda el responsable de Symantec en España que la web ha sido tradicionalmente el principal vector de expansión de malware, junto con el correo; "yo creo que el principal problema que nos encontramos a la hora de proteger el correo es que es un entorno tan cambiante, tan sofisticado, que requiere de una vista continua de lo que se está moviendo en Intenet", y explica que la compañía analiza de manera continuada todo el tráfico que se produce dentro de la web , identificando dónde está el mal.

Lo que se ha hecho hasta ahora para proteger la web ha sido identifica lo bueno conocido y lo malo conocido, "y en el medio hay una zona de grises que es lo que utilizan los malos para acceder a nuestros sistemas", dice Martos, añadiendo que han aparecido nuevas técnicas para intentar minimizar esa zona de grises, técnicas que tienen que ver con la defensa en profundidad y otras más novedosas como el despliegue de técnicas de renderización, o isolation que garantizan que puedes navegar en ese entornos de manera 100% segura.

"Los ataques BEC se producen mucho más de lo que parece y además son muy diferenciados desde el punto de vista de tecnología"

Andrés García, Country Manager, Retarus

Evolución

Con el tiempo no sólo ha evolucionado él propio correo electrónicos, sino las técnicas para protegerlo. Recuerda Miguel Angel Martos que no sólo lo utilizamos Para inyectar malware en las organizaciones, o para hacer phishing, "sino que vemos técnicas mucho más sofisticadas en las que, utilizando inteligencia artificial, los malos son capaces de generar correos que son capaces de engañar completamente a un usuario de una organización". Se trata de un tipo de ataque en el que no hay una muestra de malware que se pueda identificar, ni un indicador de compromiso; "lo que estamos haciendo compañías como Symantec es aplicar técnicas mucho más sofisticadas de detección de este tipo de ataques". Técnicas de inteligencia artificial que, combinadas con la información y conocimiento que tenemos del malware en la red hacen ver que un correo es malicioso, y no simplemente porque se identifique una muestra de malware, sino porque el texto del correo, la forma es que se ha generado, determina que es un correo malicioso que está llevando a alguien a hacer una descarga o una transferencia en algún sitio. De forma que, para el directivo de Symantec, uno de los grandes avances tiene que ver con la aplicación de la inteligencia artificial, y por otro lado la integración del correo con el resto de medidas de seguridad que tenemos en la red, en el endpoint, la web y el cloud.

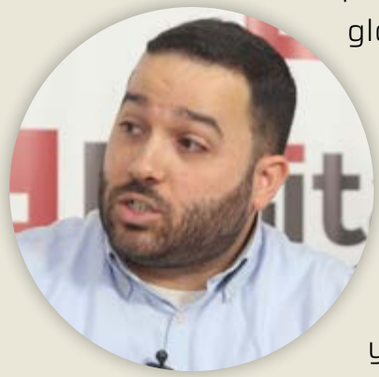
Para Andrés García el cloud ha sido una revolución, "un paradigma completamente distinto" en el

Frente a grandes retos, grandes soluciones

Como es habitual, al finalizar el debate pedimos a nuestros expertos que expongan sus propuestas, en esta ocasión para el email y la navegación web.

Miguel Angel Martos. La aproximación de Symantec es trabajar en dos áreas paralelas pero complementarias; una tiene que ver con la protección antimalware, y otra con la prevención de fuga de información. Identificamos los cuatro termination points dentro de una red, que son aquellos puntos donde realmente pueden ocurrir estas cosas, que se inyecte malware y que se extraiga información, que son el email, la web, el endpoint y los servicios cloud. Para cada uno de estos puntos tenemos servicios diferenciados, cada uno líderes en su segmento, con una cuotas de mercado representativas. Pero la gran aportación de Symantec es la capacidad de hacer funcionar estas diferentes áreas de forma coordinada, tanto para la detección de malware, como para la remediación, como la prevención coordinada de fuga de información.

Alberto Rodas. La piedra angular en Sophos es la seguridad sincronizada. Por ejemplo, cuando detectamos que un usuario está enviando correo malicioso hacia fuera, nuestro sistema lo detecta y enseguida bloqueamos su cuenta, lanzamos análisis en su propio equipo y cuando confirmamos que es correcto se vuelve a liberar su correo quitando los malisiocos. Es decir, trabajar de forma conjunta. Si un usuarios clica en un enlace malicioso de un correo que en tiempo real se evalúa como malicioso, este usuario entra en una lista para el siguiente training, y todo ello de forma automatizada.



Andres García. Nuestro foco y la diferenciación que tenemos se llama Full Stack SMTP. Señalar que, por encima de la parte del correo, estas organizaciones que se pasan a un servicio de email basado en cloud asumen un problema añadido: el estar muy seguro para los correos entrantes, pero tengo aplicaciones que tienen que enviar, que es donde nosotros queremos aportar una solución global alrededor de la parte de correo, que las aplicaciones también pueden enviar exitosamente al exterior en estas situaciones. El segundo diferencial es que la evolución debe ir por la reacción automática ante una amenaza que se ha colado. Creo que debe ser el foco de todos nosotros y para ello se ha diseñado ese módulo de Patient Zero Detection.

que es necesario explotar los datos para generar conocimiento y que “en el siguiente segundo, en el siguiente minuto, siguiente hora, siguiente día… seamos capaces de mejorar el servicio de reconocimiento”. Añade el responsable de Retarus que también ha mejorado mucho la usabilidad hacia el usuario y hacia el administrador, “porque el administrador del servicio tiene que saber lo que está ocurriendo, y lo que ha pasado. Esto ha sido una evolución tremenda”. Y un tercer punto, el siguiente paradigma, está en dar un paso adicional para minimizar un posible impacto, muy relacionado con uno de los módulos que la compañía ha desarrollado recientemente: Patient Zero Detection.

El director preventa de Sophos destaca en su intervención es que los correo maliciosos actuales “están perfectamente diseñados” y que llegados a este nivel es complicado analizarlo todos. “Ahí es

donde nosotros estamos apostamos por técnicas de concienciación del usuario. Tenemos que crear sentido común, con herramientas como que hay que entrenarlo con herramientas como Phish Threat para lanzar ataques controlados y ver quién cae"

Desafíos: implementación y usuario

Respecto al desafío en la implementación de soluciones que protejan la navegación web y el correo electrónico, Andrés García apunta al volumen; "me refiero a la gestión del volumen desde el punto de vista del conocimiento; temas de inteligencia artificial, reconocimiento de patrones, creo que es el reto real". Un reto adicional es que en el proceso de migración de una propuesta on-premise a una cloud, "todo el mundo pone foco en todo menos en seguridad y durante unas semanas, o meses, tienen un modelo híbrido, que es el momento perfecto paras que el malo se cuele"

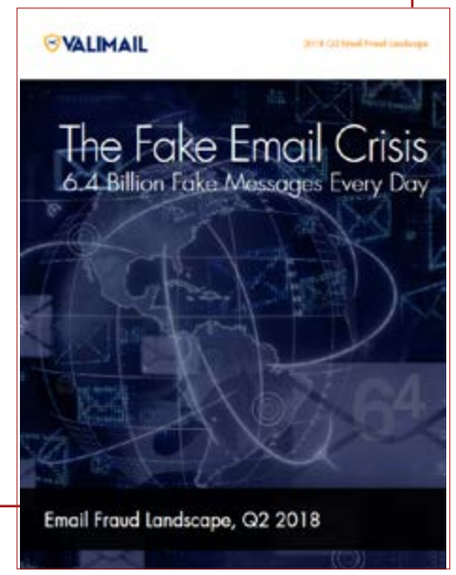
Para Alberto el desafío reside en "confiar ciegamente en las medidas de seguridad que están proporcionando" los proveedores de servicios de correo electrónico en la nube.

"El que se encuentra cualquier empresa que tiene que invertir en seguridad", dice Miguel Ángel Martos cuando le preguntamos por los desafíos de implementar soluciones de seguridad web y del email. Explica el directivo que hay múltiples proveedores, las inversiones son múltiples, los ataques son múltiples, y multivector, y por lo tanto es difícil decir qué tecnología se aplica a cada parte, o contar con una remediación automática. Insiste en que la inversión

LA CRISIS DEL EMAIL FALSO

El correo electrónico sigue siendo un medio eficaz para las comunicaciones en todo el mundo, pero la crisis del correo electrónico falso continúa, con 6.400 millones de email falsos enviados cada día.

Lejos de ser simplemente un problema de "ingeniería social", el correo electrónico falso es el resultado directo de problemas técnicos con la forma en que se implementa el correo electrónico: carece de un mecanismo de autenticación incorporado que hace que sea muy fácil fallar a los remitentes. Sin embargo, este problema también es susceptible de solución técnica, comenzando con los estándares de autenticación de correo electrónico DMARC, SPF y DKIM.



tiene que ser continuada en el tiempo y la apuesta por un modelo de consolidación tecnológica que automatice al máximo la detección y la remediación.

La formación a los empleados se ha convertido en un aspecto fundamental para la seguridad de las empresas. No en vano está recogido en el Esquema Nacional de Seguridad. Asegura el directivo de Sophos que es necesario contar con una herramienta que te permite ver tu nivel de exposición, cómo están tus empleados, quien hace los cursos, quién no, quién reporta… Y así poder atajar ese problema. “De hecho, tras el tercer ataque controlado que hacemos se reduce más de un 30% la incidencia de usuarios”, dice Alberto Rodas.

Explica Miguel Ángel Martos que cualquier política de seguridad tiene tres caras: la tecnología, los procesos y las personas, “y no hay que descuidar ninguna de las tres”. Es cierto que la formación de las personas es un elemento fundamental, pero no olvidemos que los a malos avanzan muy rápido; “hoy no estamos viendo ataques triviales y hay que cuidar los tres aspectos: la formación, para que no caigamos en entornos en los que no debemos caer; los procesos, para que si esto ocurre que sepamos reaccionar y tengamos muy estructurado cómo hacerlo, y la tecnología es muy importante porque, insisto, esto evoluciona de una manera muy compleja y los usuarios no siempre son capaces de tener la formación para detectar los ataques”.

Andrés García coincide en que el papel de los usuarios es clave para el nivelo de seguridad de las

> "La formación a los empleados se ha convertido en un aspecto fundamental para la seguridad de las empresas"
>
> Alberto Rodas,
> Director Preventa, Sophos Iberia

Enlaces de interés...

- Los Yahoo Boys crecen: del spam de las cartas nigerianas a la ingeniería social
- Recomendaciones para blindar las comunicaciones de email
- Los ataques de compromiso del email corporativo crecieron un 28% en 2018

Con el tiempo no sólo ha evolucionado el propio correo electrónico, sino las técnicas para protegerlo

empresas. Pero que no hay que llegar al extremo porque se corre el riesgo de cargarnos el proceso de email.

Ataques BEC

Los fraudes del CEO, los famosos ataques BEC, ¿son tan habituales como sugieren los estudios? ¿están teniendo tanto éxito? Dice El responsable de Symantec en España que se está viendo un incremento enorme de los ataques BEC; se trata de ataques sofisticados que no son fáciles de detectar y que, además, “no son caros de ejecutar”.

El responsable de Retarus en el región e Iberia confirma el crecimiento de este tipo de ataque; “Vemos que son muchos, y cada vez más”. Se refiere Andrés García a los ataques BEC como “Ataques silenciosos porque a las personas no les gusta hablar de ello, evidentemente. Ocurre mucho más de lo que parece y además es un ataque muy diferenciado desde el punto de vista de tecnología”.

Alberto Rodas asegura que este tipo de ataques, también conocidos como el timo del CEO se producen mucho más de lo que se cree. Menciona los 10 millones que una empresa española perdió, mientras Andrés García, apunta los 44 millones perdidos por una empresa alemana.

No significa ello que las empresas no sean conscientes del problema. “Sí que hay una conciencia mayor que antes”, dice Martos, “y esto aplica al correo electrónico o a cualquier otra parte que queramos proteger”. Apunta Rodas que la transformación digital, la adopción del cloud, se está realizando con demasiada confianza sobre el nivel de seguridad que aporta la nube, hasta que, un año después, según García, terminan entendiendo que necesitan algo más, una capa de seguridad adicional”

Compartir en RRSS

¿Es tu empresa una de las organizaciones
que ya ha adoptado tecnologías cloud?
¿Cuántos proveedores de servicios cloud utiliza tu empresa?
¿Eres de nube privada, híbrida o pública?

NUEVA ENCUESTA

it TRENDS

¡AYÚDANOS A CONOCER LA REALIDAD DIGITAL!

PARTICIPA

itTRENDS

Infraestructuras, aplicaciones y datos:

la redefinición del núcleo de las TI

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

JULIO 2019

it TRENDS

Director Pablo García Reales
pablo.garcia@itdmgroup.es
Redacción y colaboradores Hilda Gómez, Arantxa Herranz, Ricardo Gómez, Jaime Domenech
Diseño revistas digitales Eva Herrero
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

Innovación en la tecnología de negocio

Las infraestructuras y el software han sido el objeto de este trimestre en nuestra iniciativa IT Trends, que analiza las principales tendencias tecnológicas que están transformando las TI empresariales, por constituir la base sobre la que se construye la plataforma digital que dirige los negocios.

En nuestros IT Webinars Así son las nuevas infraestructuras tecnológicas y Seguridad de las aplicaciones, cómo mantener tu negocio a salvo, hemos analizado junto a los principales proveedores del mercado, cuales son los nuevos planteamientos que permiten tener unas TI más eficaces y en línea con las demandas de los negocios.

Además, hemos publicado un nuevo informe en base a las respuestas aportadas por nuestros lectores en nuestras encuestas, que titulamos Datos y aplicaciones: soporte de los nuevos modelos de negocio, en el que se refleja cómo la infraestructura híbrida empieza a asentarse en las organizaciones como plataforma de aplicaciones y cargas de trabajo, así como las principales preocupaciones alrededor de estos entornos, entre ellos, la seguridad de las aplicaciones y datos.

Y para continuar con nuestra labor, ya tenemos en marcha una nueva Encuesta IT Trends, ésta con las miras puestas en el estado de las diferentes iniciativas cloud en las empresas. ¿Nos ayudas? ¡Participa!

¡Gracias por acompañarnos en este análisis tecnológico y feliz verano! ■

Arancha Asenjo
Directora de IT Televisión
y Lead Gen Programs

Hewlett Packard
Enterprise

ALMACENAMIENTO HPE 3PAR

Basado en memoria Flash. Hasta un 50 % más rápido*

→ Descubre cómo en

www.hpe.com/es/es/storage/hpe-memory-driven-flash

* Basado en pruebas internas de HPE 3PAR comparado con valores de latencia publicados de Dell PowerMax a 26 de noviembre de 2018.

itTRENDS

El Edge y las oportunidades en el extremo de la red

La penetración de los servidores perimetrales en la infraestructura de las telcos creará una oportunidad de 54.000 millones de dólares para 2024. 5G y “edge” son tecnologías asociadas y, por tanto, no serán rentables una sin la otra.

Existen en la actualidad una amplia variedad de aplicaciones emergentes, incluidos los coches autoconducidos, la Realidad aumentada y virtual, y laInteligencia artificial, que requieren capacidades de procesamiento distribuido que sólo el edge computing puede ofrecer. Por ello, los proveedores de servicios móviles (MSP) actuales, mientras centralizan la infraestructura de telecomunicaciones en sus nubes privadas, tratan de comprender cómo pueden implementar edge computing en sus redes. Un panorama que deja a las claras la oportunidad de negocio que la inminente comercialización del "telco edge" constituye, según la firma de análisis de mercados ABI Research.

Sin embargo, quedan aún muchos cabos sueltos para que el edge computing sea una corriente habitual, ya que no existe un modelo comercial único. Esto representa un desafío

TELCO EDGE: UNA OPORTUNIDAD DE 54.000 MILLONES DE DÓLARES

para la administración de productos "edge", pero también una oportunidad comercial para estas implementaciones y el lanzamiento de 5G. En este sentido, están surgiendo empresas comprometidas con este mercado, como MobiledgeX y ori.co, dos nuevos players disruptivos que tienen como objetivo monetizar las redes 5G y las implementaciones "edge" asociadas en las telecomunicaciones. Mientras tanto, MSP como AT&T y Telefónica, están avanzando en su viaje para desbloquear el poder del "edge computing" y así poder ofrecer nuevos servicios a través de redes 5G.

Por otro lado, resulta vital, tanto para los proveedores como para los MSP, la capacidad de comprender y priorizar la forma de crear infraestructuras "edge" que se alineen con el objetivo empresarial final. El pronóstico de ABI Research indica, en este sentido, que la penetración de los servidores perimetrales en la infraestructura de las telcos creará una oportunidad de 54.000 millones de dólares para 2024. El valor para varios proveedores de telecomunicaciones y de soluciones de software variará de acuerdo con su capacidad para ayudar a los proveedores de servicios móviles a capitalizar el potencial de casos de uso clave, como el almacenamiento en caché de videos, servicios geográficos específicos y servicios personalizados.

ABI Research espera que, a largo plazo, las implementaciones de Telco Edge se conviertan en plataformas de facto para entregar servicios "próximos al extremo". También incide en la idea de que 5G y "edge" son tecnologías asociadas y, por tanto, no serán rentables la una sin la otra. Finalmente, el estudio afirma que será necesario que los operadores identifiquen tanto el mercado vertical al que se quieren dirigir como la posición ideal de sus servidores de "edge". Si no lo hacen de inmediato, Amazon, Google y Facebook apuntarán a las mismas verticales empresariales que los MSP intentan abordar, lo que devaluará seriamente la 5G y el futuro de los proveedores de servicios móviles en general. ■

MÁS INFORMACIÓN

Telco Edge: Enabling Technologies and Commercial Analysis

EQUINIX

DESCÁRGUESE NUESTRA GUÍA DE VANGUARDIA DIGITAL

haga clic aquí

Así son las nuevas infraestructuras tecnológicas

Flexibles, escalables, asequibles, predictivas, inteligentes, seguras, autónomas.... Estas son las capacidades que se demandan a las infraestructuras tecnológicas hoy en día; unas posibilidades en continua evolución, que se enriquecen de manera constante con la injerencia de nuevos planteamientos tanto tecnológicos como de trabajo.

Las infraestructuras de TI subyacen bajo las empresas actuales y, a medida que las primeras evolucionan, las segundas pueden desarrollar nuevas vías para la generación de negocio. Y actualmente, la infraestructura de TI vive un momento apasionante: es un punto de disrupción e innovación en muy diferentes, áreas, desde los servidores, al almacenamiento, desde las redes, al software o la seguridad. En el IT Webinars "Así son las nuevas infraestructuras tecnológicas", abordamos junto a HPE, Veeam, Equinix, Micro Focus, y Kaspersky, algunos aspectos clave de esa transformación de las infraestructuras.

NUEVAS PROPUESTAS PARA EL ALMACENAMIENTO Y LA GESTIÓN DE LA INFORMACIÓN

"Estamos en un momento apasionante de la tecnología por la gran oleada de innovación",

ASÍ SON LAS NUEVAS INFRAESTRUCTURAS TECNOLÓGICAS
Clica para ver este #ITWebinars

comenzó diciendo Jorge Fernández, director de tecnología para Sur de Europa de Hewlett Packard Enterprise. Hablaba en términos generales, pero también de forma particular sobre la transformación que vive el segmento del almacenamiento de datos gracias a la llegada de la inteligencia, que permitirá ser más eficaces. "Herramientas como InfoSight, ponen en manos del cliente información que antes no había tenido. Ahora entendemos las cargas de trabajo, recomendamos la mejor configuración con la información que obtenemos de nuestros propios sistemas". Además, en su intervención, Fernández destacó otros hitos en el campo del almacenamiento, como la irrupción de las cabinas all-flash, "que proporcionan alto rendimiento y tienen técnicas modernas de compactación del dato"; la aparición del protocolo de comunicaciones NVMw, más rápido y eficaz y que "explota la capacidad de los procesadores. Si es over Fabric, permite comunicar de extremo a extremo los datos, y abre un nuevo paraíso para las SAN. Esto nos trae una nueva tecnología de almacenamiento y de comunicaciones que va a cambiar la forma en la que trabajamos en los centros de datos"; las memorias NAND más rápidas; o el almacenamiento secundario, "que es la forma más económica de almacenar sobre servidores estándar y, por encima, una capa de software que me dé la lógica para el acceso al dato".

En esta evolución de las infraestructuras, el dato ha ido pasando por distintos entornos y en todos ellos hay que garantizar su disponibilidad, "en tiempo y forma", matizó Alexis de Pablos, director técnico de Veeam Software. En este camino al cloud híbrido que están haciendo las empresas, se ha pasado por distintas fases de disponibilidad: "desde data centers con cierto nivel de redundancia para poder recuperar la información, pero de forma muy acotada; a entornos de multi datacenter, en los que cloud empezaba a jugar un papel relevante. El hecho de que el dato esté en distintos entornos implica una necesidad adicional de poder gestionar y monitorizar esa información. En estos entornos que empiezan a tener diferentes ubicaciones, "es imprescindible disponer de un modelo de orquestación donde cada organización pueda tener un punto único de gestión para mover los datos en función de la necesidad. Ahora, la tendencia es un modelo basado en comportamiento. Actualmente la gestión del dato está basada en políticas, pero ese salto al comportamiento nos permitirá tratar la información en función de la necesidad de cada momento. Y, por ejem-

"La inteligencia va a transformar la forma en la que vemos el almacenamiento de datos"

JORGE FERNÁNDEZ, DIRECTOR TÉCNICO SUR DE EUROPA, HPE

"La gestión del dato basada en comportamiento nos permitirá tratar la información en función de la necesidad de cada momento"

ALEXIS DE PABLOS, DIRECTOR TÉCNICO, VEEAM

plo, cuando estamos en riesgo, actuar de forma inmediata".

EL FUTURO HÍBRIDO

"Tal y como conocemos hoy las infraestructuras, no pueden dar cabida a la transformación digital. Deben estar adaptadas a la nube híbrida para aprovechar lo mejor de cada infraestructura", señaló Ramón Cano, director de servicios gestionados de Equinix. "En la parte de cloud, tenemos tiempos de despliegue rápidos, mejores posibilidades para la entrega de contenido, escalabilidad..., pero también tenemos que usar infraestructuras privadas, con costes más predecibles, mayor seguridad, y que se adaptan mejor a las cargas críticas de las compañías. "La combinación de ambas nubes debe dar respuesta a las necesidades de agilidad y fiabilidad de las empresas, y deben estar interconectadas formando una única plataforma".

En ese viaje hacia la nube híbrida, el cliente deberá pasar por varias fases, comenzando por el aprendizaje, decidiendo qué aplicaciones pueden ser susceptibles de estar en nube pública o privada, o cuáles en nube híbrida y adaptarlas. "En el paso final se necesita una conexión fiable y segura porque hablamos de cargas críticas de compañías", apuntó Patricia Cuesta, team lead pre-sales engenieer de Equinix.

En términos similares se pronunció Antonio Picazo, consultor preventa de soluciones ITOM de Micro Focus, quien señaló que los clientes deben "estudiar sus cargas y, dependiendo del tipo de aplicación o servicio, apostar por el sitio más adecuado al optar por un modelo de infraestructura híbrida". Después, se tendrán que enfrentar a la gestión de dicha infraestructura, mediante plataformas de gestión cloud que cuenten con portales de autoservicio y herramientas de gestión y control de costes. "Hay que intentar centralizar la gestión en una herramienta para aprovisionar rápido. Que nos dé información para no ponernos en riesgo y que, cuando muevas una aplicación, no se caiga otra".

UNA INFRAESTRUCTURA CON MÚLTIPLES FRENTES A PROTEGER

La infraestructura de TI es uno de los objetivos preferidos de los ciberdelincuentes. Pedro García-Villacañas, director preventa en Kaspersky, detalló cómo ha ido evolucionando la seguridad a medida que la infraestructura tecnológica empresarial se ha ido haciendo más compleja y extendiendo a nuevos entornos como el industrial o los dispositivos IoT, ahora par-

"La combinación de nubes permite dar respuesta a las necesidades de agilidad y fiabilidad de las empresas"

Ramón Cano, director de servicios gestionados, Equinix

"Dependiendo del tipo de servicio o aplicación se debe apostar por el sitio más adecuado al optar por un modelo de infraestructura híbrida"

Antonio Picazo, consultor preventa, Micro Focus

te de la red. “Nuestra recomendación es integrar la ciberseguridad en las infraestructuras de TI; incorporar los procesos de ciberseguridad en los procesos de negocio y que, según se vaya desplegando, se ponga seguridad”. Para evitar este tipo de incidentes, la propuesta es contar con soluciones capaces de predecir, prevenir, detectar y responder y estar así preparados para lo que pueda venir en el futuro, tanto en los entornos de TI empresarial, como de OT industriales e IoT. Además, producto de este planteamiento de embeber la ciberseguridad desde el inicio, existen ya soluciones de seguridad para el sistema operativo de los equipos IoT en el extremo de la red. ■

MÁS INFORMACIÓN

- Así son las nuevas infraestructuras tecnológicas
- Inteligencia Artificial para un centro de datos autónomo
- Cómo dar una mayor rentabilidad a la protección de datos en cloud
- Equinix Cloud Exchange Fabric
- Gestión de nubes híbridas
- Guía sobre el panorama actual de la ciberseguridad

“Incorporar los procesos de ciberseguridad en los procesos de negocio permitirá dar un nuevo nivel de seguridad a las infraestructuras”

PEDRO GARCÍA-VILLACAÑAS,
DIRECTOR PREVENTA, KASPERSKY

Si te ha gustado este artículo, compártelo

LA COMISIÓN EUROPEA RESPALDA A KASPERSKY LAB

LA COMISIÓN EUROPEA REAFIRMA QUE NO HAY INDICACIÓN ALGUNA DE PELIGRO ASOCIADO A ESTE MOTOR ANTI-VIRUS

El pasado 16 de abril de 2019, la comisaria de la UE para la Economía y la Sociedad Digitales, Mariya Gabriel, respondió públicamente a la petición realizada por el eurodiputado Gerolf Annemans sobre la Resolución del Parlamento Europeo adoptada el 13 de junio de 2018 en la que, entre otras cosas, se calificó a los productos de Kaspersky Lab como 'maliciosos'. La respuesta de la Comisión Europea ha sido categórica: **"La Comisión no dispone de ninguna prueba sobre los posibles problemas relacionados con el uso de los productos de Kaspersky Lab". 16 de abril de 2019.**

Es la segunda vez que la Comisión Europea se pronuncia con respecto a Kaspersky Lab, reafirmándose en las dos ocasiones en los mismos términos: **"La Comisión no tiene indicación alguna de peligro asociado a este motor anti-virus". 6 de abril de 2018.**
Con estas dos declaraciones, la Comisión Europea pone fin a las falsas acusaciones difundidas contra la compañía durante los últimos meses; quedando Kaspersky Lab libre de toda sospecha.

KASPERSKY lab

Mejorar la seguridad y la eficiencia son algunas de las ventajas que tiene implementar DevSecOps. Su filosofía es generar conciencia de que "todo el mundo es responsable de la seguridad". Hoy en día, esto está llevando a los líderes de seguridad tradicionales a pelear duramente por un asiento en la mesa ejecutiva de su organización.

DevSecOps, creando software más seguro

El número de aplicaciones y lanzamientos no deja de crecer, como tampoco lo hace el volumen y complejidad de los ataques. Todas las industrias se enfrentan a serias vulnerabilidades y las empresas siguen luchando contra ellas porque incrementan sus niveles de riesgo. Según un informe de WhiteHat Security, más del 60% de las aplicaciones tenían al menos una vulnerabilidad grave y explotable abierta durante todo el año, lo que significa que las puertas a las explotaciones fáciles estaban abiertas.

El estudio presta atención a las tendencias de desarrollo de aplicaciones modernas, de manera concreta, al uso de código abierto y de

arquitecturas de microservicios. “Nuestros hallazgos revelaron que a medida que más empresas aumentan la dependencia de las aplicaciones, tampoco lograron implementar la seguridad de la aplicación en el ciclo de vida del desarrollo del software”, dice la compañía en un post en el que también afirma que los microservicios “generan más inseguridades en promedio que las aplicaciones tradicionales”.

De acuerdo con sus datos, casi el 70% de cada aplicación consta de componentes de software reutilizables (por ejemplo, bibliotecas de terceros, software de código abierto (OSS), etc.), porque este método de desarrollo es rápido y agrega valor a las ofertas. Pero, eso también significa que las aplicaciones “heredan” las vulnerabilidades que se encuentran en los componentes del software. “Sin embargo, cuando DevSecOps se hace de la manera correcta, las tasas de remediación y el tiempo para corregir mejoran las aplicaciones basadas en microservicios”, explica WhiteHat Security.

Por otra parte, cuando las organizaciones incorporan la seguridad en el proceso de DevOps, generalmente consiguen una caída del 50% de las vulnerabilidades de la producción, y su tiempo para solucionarlas mejora en un 25%.

De acuerdo con otro informe, este de Veracode, más del 85% de todas las aplicaciones tienen al menos una vulnerabilidad después del primer análisis, y más del 13% contienen al menos un fallo de severidad muy alta. Además, los últimos resultados de las organizaciones indican que una de cada tres aplicaciones fue vulnerable a ataques por fallos de severidad alta o muy alta. Asimismo, recoge que más del 70% de las vulnerabilidades permanecen un mes después de descubrirse, casi un 55% permanecen más de tres meses y un 25% siguen estando presentes 290 días después de haberse descubierto. En el otro lado, un 25% de los fallos se parchean en 21 días y otro 25% permanece sin parchear un año después.

Los datos de Veracode sobre la persistencia de fallos muestran que las organizaciones con programas y prácticas DevSecOps establecidos superan en gran medida a sus pares en la rapidez con la que abordan las vulnerabilidades. De manera más concreta, los programas DevSecOps más activos corrigen fallos más de 11,5 veces más rápido que la organización típica, debido a las comprobaciones de seguridad en curso durante la entrega continua de compilaciones de software, en gran parte como resultado de un mayor escaneo de código. Los datos muestran una fuerte correlación entre la cantidad de veces al año que una organización escanea y la rapidez con la que abordan sus vulnerabilidades.

En todo caso y a pesar del avance, no hay que confiarse ya que el número de aplicaciones sigue siendo demasiado elevado y los componentes de código abierto “continúan representando un riesgo significativo para los negocios”, dice Veracode. ■

Más del 60% de las aplicaciones tenían al menos una vulnerabilidad grave y explotable abierta durante todo el año

DevSecOps consigue una caída del 50% de las vulnerabilidades

MÁS INFORMACIÓN

- 2018 Application Security Statistics Report: The Evolution of the Secure Software Lifecycle
- Informe de Veracode sobre el estado de la seguridad del software

Si te ha gustado este artículo, compártelo

¿Es tu empresa una de las organizaciones
que ya ha adoptado tecnologías cloud?
¿Cuántos proveedores de servicios cloud utiliza tu empresa?
¿Eres de nube privada, híbrida o pública?

NUEVA ENCUESTA

it TRENDS

¡AYÚDANOS A CONOCER LA REALIDAD DIGITAL!

PARTICIPA

Seguridad de las aplicaciones: cómo mantener tu negocio a salvo

La seguridad de las aplicaciones no sólo se inicia en el proceso de desarrollo, sino que hay que protegerlas una vez que se implementan, incluido el acceso a ellas. Y esto es cada vez más importante a medida que los ciberdelincuentes han fijado su mira en las aplicaciones para lanzar sus ataques.

La seguridad de las aplicaciones recibe cada vez más atención. Esencialmente se trata de prevenir ataques que puedan explotar fallos en cualquier software que utilice una organización. Existen cientos de herramientas disponibles para asegurar las aplicaciones, incluso algunas especializadas en aplicaciones móviles, en aplicaciones basadas en red, incluso firewalls diseñados específicamente para las aplicaciones web.

En un mundo cloud, móvil y distribuido es fácil decir que, en la mayoría de las ocasiones, se accede a las aplicaciones desde fuera del perímetro de la empresa, y desde una diversidad de dispositivos, y por empleados con diferentes perfiles. El IT Webinar Seguridad de las aplicaciones: cómo mantener tu negocio a salvo, celebrado bajo el paraguas de IT Trends y en el que participaron X by Orange, Citrix, Trend Micro, SonicWall, Qualys y nCipher, abordamos cómo llevar el nivel de seguridad de las aplicaciones al siguiente nivel.

"EL 70% DE LOS CIBERATAQUES SE REALIZAN CONTRA LA CAPA DE APLICACIÓN" (X BY ORANGE)

José Fernández, Responsable de producto, en X by Orange, dio comienzo a la sesión diferenciando entre aplicaciones de escritorio, aplicaciones web, los propios sitios web, los servicios en la nube, y las aplicaciones móviles, y aportando algunos datos de diferentes estu-

SEGURIDAD DE LAS APLICACIONES
Clica para ver este #ITWebinars

dios que ponen de manifiesto que las aplicaciones se han convertido en uno de los principales vectores de ataque. Entre los datos aportados, que el 70% de los ciberataques se realizan contra la capa de aplicación, y no contra la red o los sistemas, y que menos del 30% de las empresas tienen soluciones se seguridad a nivel de aplicación.

Fernández detalló cómo se protege a nivel de aplicación, destacando que los ataques a este nivel son los más difíciles de detectar. Se aplican filtrados que determinan el uso de cada aplicación, pudiendo establecer horarios de utilización, o la prohibición de las mismas.

Según una encuesta realizada por X by Orange, los responsables de negocio dicen que la empresa no puede parar por ningún tipo de ataque, mientras que los responsables de TI tienen claro que necesitan estar protegidos todo el tiempo y contra todo tipo de ataque, incluidos los de Día Cero, y necesitan una solución de seguridad completa. La conclusión es que se necesitan sistemas de prevención, detección y respuesta; monitorización y análisis a nivel de aplicación, una mayor protección en los dispositivos, y un marco de gestión global de riesgos para las aplicaciones.

Aseguró el responsable de producto de X by Orange, que existen muchas propuestas en el mercado, de diferentes fabricantes. La propuesta de seguridad como servicio de X by Orange, que no tiene permanencia, se centra en X Privacy, una VPN basada en SD-WAN; X Security, que además añade de servicios de firewalls para analizar el tráfico; y X Protection, una solución completa que incluye un antivirus, un anti ransomware para móviles, que complementa los anteriores. Todos estos servicios incluyen una prueba gratuita de 15 días.

"TENEMOS QUE ENTREGAR LAS APLICACIONES A LOS USUARIOS COMO ELLOS LO DEMANDAN" (CITRIX)

"El mundo de los negocios está cambiando mucho", dijo Nuno Silveiro, Responsable de Networking y Cloud de Citrix. El directivo explicó que ahora tenemos un entorno mucho más abierto, con capacidad para conectarnos en cualquier sitio y a través de cualquier red, a pesar de lo cual "tenemos que entregar las aplicaciones a los usuarios como ellos lo demandan".

La transformación digital tiene como objetivo la agilidad del negocio, pero impacta en diferentes aspectos, como mejorar la experiencia del usuario o la explosión del cloud. También habló Nuno Silveiro de un cambio en la arquitectura que se utiliza para todos estos entornos, porque las aplicaciones están cambiando, al igual que la manera en que accedemos a esas aplicaciones y la manera en

"Más del 70% de ataques son contra la capa de aplicación, y no a nivel de red o de sistemas, que era lo típico en el pasado"

José Fernández, Responsable de producto, X by Orange

"La migración de las aplicaciones tradicionales a las arquitecturas de aplicaciones modernas aumentará en un 85% del tráfico este a oeste"

Nuno Silveiro, Responsable de Networking y Cloud, Citrix

que garantizamos su seguridad, a lo que se añade el reto de pasar de aplicaciones monolíticas a otras con cientos o miles de microservicios que pueden estar dispersos.

Estamos en un entornos híbrido, con parte de aplicaciones legacy y otras cloud, un entorno que durará aún un tiempo, y por eso, según Silveiro, tenemos que trabajar en diferentes capas. Hay que controlar el dispositivo de acceso, garantizar que la conexión es segura, tener controlado el firewall de aplicación, aplicar múltiples factores de autenticación, etc.

Por tanto, hay que trabajar en distintas capas, con distintos contextos y cada uno con sus reglas de protección, algo que se trabaja en Citrix desde hace tiempo.

"HAY QUE TENER UN PLANTEAMIENTO DE DEFENSA MULTICAPA" (TREND MICRO)

"Las aplicaciones no dejan de ser un vector de ataque más", apuntó José de la Cruz, Director Técnico de Trend Micro, destacando la heterogeneidad como uno de sus grandes retos, junto con el malware o las vulnerabilidades. Aseguró respecto a esto último, que no somos lo suficientemente rápidos cuando intentamos mitigarlos, lo que puede generar muchos problemas de seguridad.

Frente a estos retos debe tenerse un planteamiento de defensa multicapa con diferentes tecnologías que se han ido desarrollando a lo largo de los años, y que van desde un antimalware, a la prevención de pérdida de datos, análisis de comportamiento o sandboxing.

De la Cruz incidió en el tema de las vulnerabilidades para hablar de parcheado virtual, una solución que Trend Micro aplica en diferentes puntos para analizar el tráfico en busca del paquete que intenta explotar la vulnerabilidad, siendo capaces de proteger no sólo sistemas operativos sino aplicaciones.

DevOps es una tendencia en el desarrollo de aplicaciones en el que, de nuevo, prevalece la operativa frente a la seguridad. "Hay que ser capaz de implementar la seguridad en la tecnología de contenedores proporcionando información sobre si es vulnerable, tiene malware o no cumple con las mejores prácticas de seguridad". La tecnología Virtual Patching de Trend Micro es capaz de visualizar todo el software que se ejecuta en el contenedor, de la misma manera que se haría con cualquier servidor.

"EN UN MUNDO 'SOFTWARE DEFINED', PUEDE TENER MÁS SENTIDO RABAJAR CON UN FIREWALL VIRTUAL" (SONICWALL)

Cada vez se está poniendo más foco en la seguridad de las aplicaciones, señaló

"La empresa española sí que está concienciada sobre la importancia de seguridad de las aplicaciones, pero quizá nos estemos quedando atrás en cuanto a las medidas a implementar"

José de la Cruz, Director Técnico, Trend Micro

"Los firewalls virtuales pueden tener más sentido a la hora de proteger las aplicaciones en las arquitecturas híbridas actuales, donde cada vez es más todo software defined"

Eduardo Brenes, Territory Manager, SonicWall Iberia

Eduardo Brenes, Territory Manager de SonicWall Iberia, añadiendo que los fabricantes están tratando de securizar y gestionar mejor esas aplicaciones.

La oferta de SonicWall, parte de Dell hasta hace unos años y con quien mantienen acuerdos OEM, es amplia. Desde los NGFW (firewalls de próxima generación), a puntos de acceso Wireless, soluciones de seguridad de correo electrónico, un antimalware basado en un motor de SentinelOne, soluciones de cloud, WAF, CASB, etc. Todo ello con una consola de gestión centralizada que facilita el trabajo de los responsables de seguridad.

Cuatro son las soluciones de SonicWall orientadas a la protección de aplicaciones: Virtual Firewall, WAF, Cloud Application Security y Email Security. Sobre la primera, Brenes explicó que, en un mundo 'software defined' puede tener más sentido trabajar con un firewall virtual, una propuesta que además mejora la seguridad de los contenedores.

Respecto a los WAF (Web Application Firewall), están orientadas a proteger las aplicaciones web, así como los propios portales web, donde el cumplimientos como GDPR es fundamental. SonicWall Cloud App Protection es la propuesta CASB de la compañía para identificar y securizar todas las aplicaciones que están en la nube. Por último, SonicWall Email Security es un servicio de correo limpio para propuestas como office 365 o Google Apps.

"LAS EMPRESAS DEBEN TENER UNA MAYOR VISIBILIDAD DEL ENTORNO EN EL QUE SE VAN A MOVER" (QUALYS)

Raúl Benito, Director General de Qualys Iberia, señaló que las empresas saben que las aplicaciones son un gran vector de ataque, y explicó que, cuando hablamos de aplicaciones, hablamos de aplicaciones web, de APIs, de todos esos servicios que se están construyendo en la transformación digital.

Cada vez tiene más importancia esos aplicativos web y cómo se están construyendo porque los tenemos en cualquier sistema, y eso significa que las vulnerabilidades te pueden llegar de cualquier parte; los ciberdelincuentes están aprovechando esa masificación para lanzar sus amenazas. "Las empresas deben tener una mayor visibilidad del entorno en el que se van a mover", apuntó.

Qualys WAS hace un análisis dinámico de los aplicativos para ver qué vulnerabilidades puede tener ese sistema, añadiendo al mismo tiempo capas para tener más visibilidad o para ver cuán robusto puede ser ese aplicativo, incluido el mundo de los contenedores.

"Necesitamos tener visibilidad de todo lo que está relacionado con los contenedores,

"Tenemos que proveer a los contenedores y los microservicios de la misma seguridad que al resto de aplicaciones"

Raúl Benito, Director General, Qualys Iberia

"Cada vez que nos descarguemos información deberíamos preguntarnos si la fuente de información y si la integración de la información que nos llega es la correcta"

José María Pérez Romero, Ingeniero de Ventas, nCipher

no sólo cuando se están construyendo, sino cuando están funcionando en producción", dijo el directivo, y eso es una de las propuestas de Qualys: tener una visualización constante de los procesos que están corriendo, de qué sistemas se tienen publicados y además qué vulnerabilidades hay para que, con esa información, se sepa si hay que responder de alguna forma a un posible amenaza.

"LA FIRMA DE CÓDIGO RESUELVE LA SEGURIDAD EN LAS APLICACIONES DESDE EL ORIGEN" (NCIPHER)

Para José María Pérez Romero, Ingeniero de Ventas de nCipher, hay dos preguntas que todos debemos hacernos cuando descargamos software: ¿estoy seguro de la fuente? ¿estoy seguro de estar bajando lo que quiero? La firma de código responde ambas al poder verificar la fuente y además la integridad del software que se descarga.

La firma de código trabaja con criptografía simétrica: se firma la aplicación con una clave privada; por otra parte, existen unas entidades certificadoras que van a emitir certificados con la clave pública de los fabricantes de estas aplicaciones para que el consumidor pueda verificar esa autoría. El resultado es una firma electrónica que, en el caso que nos ocup,a se aplica a un código.

Los fabricantes de aplicaciones se enfrentan a dos retos, uno de ellos es la propia operativa derivada de una mayor demanda, y por otra es la seguridad, porque tenemos que tener la clave privada muy segura y bien guardada. Lo que propone nCipher son unos HSM (Hardware Security Modules) para potenciar la operación y para añadir seguridad.

Estos HSM ayudan a guardar las claves y, además, generar claves de forma aleatoria, firma electrónica, cifrado, etc., y todo ello con el rendimiento que se demanda ahora. Los HSM de nCipher son la familia nShield y se ofrecen en distintos formatos dependiendo de lo que el usuario requiera: appliance de red, embebido PCI, o USB. ■

MÁS INFORMACIÓN

- Estableciendo confianza e integridad con la firma digital
- 2019 SonicWall Cyber Threat Report
- Inventariado de activos basados en cloud
- La mayoría de las apps de banca online contienen vulnerabilidades críticas
- El ataque contra las aplicaciones web crece un 56%

PRINCIPALES TENDENCIAS EN LA SEGURIDAD DE LAS APLICACIONES 2019

La seguridad de las aplicaciones recibe cada vez más atención. Esencialmente se trata de prevenir ataques que puedan explotar fallos en cualquier software que utilice una organización. Este informe recoge que más del 85% de todas las aplicaciones tienen al menos una vulnerabilidad; y más del 13% tiene al menos un fallo de seguridad crítico. Dice también que el 70% de las empresas sufren ataques contra sus aplicaciones a través de IPv6, con un tercio de los ataques dirigidos a las interfaces de programación de aplicaciones (API), que el 90% de los responsables de TI confía en que sus organizaciones podrían mantenerse al día con la creciente tasa de ataques de capa de aplicación o que el 86% de los clientes confían en la capacidad de los proveedores de servicios en la nube para proporcionar altos niveles de seguridad de la aplicación.

Si te ha gustado este artículo, compártelo

#ITWebinars

IT TRENDS

Tendencias y oportunidades de la nube

Cloud se ha convertido en LA PLATAFORMA que está alimentando la transformación digital y la modernización de las TI. Prácticamente el 90% de las organizaciones utiliza algún modelo de cloud y la mayor parte, cuenta con dos o más proveedores de servicios de nube, una tendencia que ha ido cogiendo tracción a lo largo de este 2019.

En este IT Webinars que celebraremos bajo el paraguas de IT Trends, descubriremos cuáles son las nuevas tendencias tecnológicas que giran en torno al cloud, así como las oportunidades de innovación que genera para las empresas.

26 SEPTIEMBRE 11.00 h.

¡Regístrate ya!

it TRENDS

El futuro de la protección de datos pasa por la integración flash y la nube

Susana Vila,
Intelligent Storage
Category Manager de HPE

La sincronización del centro de datos all-flash ha sido uno de los mayores cambios en la industria del almacenamiento de los últimos años. A diferencia de la mayoría de transiciones tecnológicas, esto ha sucedido más rápido de lo previsto. Hemos pasado rápidamente de un momento en que el flash era exclusivamente una solución de nicho para un rendimiento extremo a otro en el que el precio del flash ha alcanzado al del disco magnético en almacenamiento neto. Ahora estamos en la cúspide de una tercera ola donde el flash es la solución predeterminada para las aplicaciones comerciales.

A medida que el almacenamiento all-flash pasa a formar parte de la tendencia dominante en los centros de datos empresariales, se plantea una pregunta: ¿pueden los actuales sistemas de protección de datos sostener las exigencias de un entorno de almacenamiento primario all-flash?

Los requisitos del comercio global y de disponibilidad permanente significan que no hay tolerancia para los tiempos de inactividad. Añádele a ello el efecto en cascada de fallos en un mundo virtual en el que un solo fallo de hardware puede hacer caer múltiples servidores y aplicaciones virtuales. El riesgo para tu empresa, así como los costes de funcionamiento para gestionar ese riesgo, pueden ser enormes.

La mayoría de los entornos empresariales disponen de cabinas de almacenamiento primarias y dispositivos de copia de seguridad basados en distintas arquitecturas de almacenamiento sin integración y requieren soluciones de copias de seguridad que resultan costosas y complejas de gestionar, lo que incrementan el riesgo de los servidores de producción que se intenta proteger. Estos son problemas que simplemente no puedes permitirte en un entorno de alto rendimiento.

La alternativa es una solución convergente que integre almacenamiento flash primario y dispositivos de copia de seguridad a través de una solución de software, con una gestión sencilla que dé como resultado servicios

A medida que el almacenamiento all-flash pasa a formar parte de la tendencia dominante en los centros de datos empresariales, se plantea una pregunta: ¿pueden los actuales sistemas de protección de datos sostener las exigencias de un entorno de almacenamiento primario all-flash?

de datos comunes y automatización entre dispositivos para una transferencia de datos perfecta. La protección de datos se convierte en una función del almacenamiento primario, suprimiendo así la necesidad de más infraestructuras de copia de seguridad (servidores de medios) y gestión (aplicaciones de copia de seguridad de terceros). De este modo, la protección de tus datos resulta menos intrusiva en el procesamiento de las aplicaciones, es más sencilla de gestionar y se realiza de forma más rápida.

Al eliminar la complejidad, te queda un proceso de copia de seguridad que permite proteger tus cabinas de almacenamiento primario de forma totalmente automatizada directamente desde la interfaz del hipervisor o la aplicación. Los datos se transfieren de forma nativa desde el almacenamiento primario hasta la copia de seguridad del modo programado por el propietario de la aplicación empresarial, sin necesidad de servidores de medios ni de complicado software de copia de seguridad. ■

TRES COSAS QUE NO TE PUEDES PERMITIR OLVIDAR CUANDO COMPRES ALMACENAMIENTO FLASH

Hoy en día, las empresas se esfuerzan por ser más innovadoras y competitivas, así como por estar preparadas para el futuro.

Para poder alcanzar estos objetivos, muchos están recurriendo a las transformaciones digitales e implementando la TI híbrida. No obstante, si su infraestructura no está a la altura, dar estos pasos hacia la innovación se vuelve una tarea poco menos que imposible. Este documento de la consultora Aberdeen apunta al almacenamiento flash como una forma de dar respuesta a una gestión del almacenamiento que, en los últimos años, ha venido siempre acompañada de frustración, quebraderos de cabeza y pérdidas de tiempo. Con todo, no todas las soluciones de almacenamiento flash son adecuadas para tareas como el análisis predictivo, tan importante para la toma de decisiones actuales.

NUEVO INFORME

DOCUMENTO EJECUTIVO

IT TRENDS 2019:
Datos y aplicaciones, soporte de los nuevos modelos de negocio

ELABORADO POR itRESEARCH

Descarga este **documento ejecutivo** de itRESEARCH

La interconexión, una oportunidad para el mercado global

IGNACIO VELILLA,
Managing Director de Equinix en España

Ciudades de todo el mundo están acometiendo proyectos de transformación digital que requieren de grandes inversiones por parte de los propios Estados, Administraciones locales y, en algunos casos, de entidades privadas. Estas inversiones buscan dotar a los núcleos urbanos de infraestructuras digitales capaces de soportar y gestionar el creciente volumen de datos generados en las denominadas Smart Cities. Los edificios dependientes de los diferentes Gobiernos, el tráfico de vehículos privados, los sistema de transporte públicos, las estaciones medioambientales localizadas en diferentes puntos de las ciudades… son solo alguna fuentes de datos que debemos procesar para administrar debidamente una metrópoli.

En la actualidad, existen algunos ejemplos de ciudades que están haciendo frente a los retos de la era digital. Si miramos al lejano oriente, el Gobierno chino ha anunciado un proyecto de transformación del delta del río Guangdong o de las Perlas – o como se conoce ahora, Gran Bahía de China – para convertir a la región en una red urbana de alta tecnología, que pueda hacer competencia a Silicon Valley o a la bahía de Tokio a partir de 2035. Este proyecto buscará afianzar más la figura de Hong Kong como epicentro financiero mundial y la de Shenzhen como ciudad más innovadora de China.

Mientras tanto en nuestro continente, Londres sigue situándose como un centro tecnológico de importancia mundial. En 2018, la capital de Reino Unido atrajo más de 2.100 millones de euros de financiación destinados a empresas tecnológicas, que suponen un 72% del total de los más de 2.900 millones recaudados por empresas del sector en todo el país. Estas cifras duplican las de Berlín, la segunda capital en cuanto a inversión tecnológica en Europa, y refuerzan la posición de Londres, a pesar del Brexit, como uno de los líderes de la economía digital mundial.

¿QUÉ OCURRE EN ESPAÑA?

En el actual contexto digital mundial, España se encuentra ante una oportunidad única de adoptar una posición de liderazgo en el mapa de conectividad europeo. La región necesita alternativas a rutas altamente demandadas como Marsella, Londres y Ámsterdam para "unir" a Europa con Norteamérica, Brasil y el norte de África y España cuenta con una posición geográfica privilegiada para cumplir ese rol.

La llegada de nuevos cables submarinos a las costas ibéricas y los fuertes lazos lingüísticos y culturales con Iberoamérica son otros alicientes para la llegada de nuevos proveedores de conectividad a Madrid. La llegada de estas empresas favorecerá la llegada de nuevo talento e inversiones que pueden servir de aliciente para la creación de un hub de relevancia mundial. Sin embargo, en cuanto al mercado de infraestructuras digitales y de data centers de última generación, España se encuentra unos peldaños por debajo de grandes centros europeos como París, Ámsterdam, Fráncfort y, por supuesto, Londres. Pero es cierto que España y su capital están pasando de representar un mercado IT que solo atendía a clientes nacionales a convertirse a un nuevo punto de referencia global por su posición geográfica privilegiada y su potencial de interconexión entre diferentes mercados. Para poder llegar al nivel de los mercados punteros continentales, empresas y Administración deben seguir trabajando para adoptar nuevas formas de conectividad más eficientes y productivas que las actuales.

LA INTERCONEXIÓN COMO RESPUESTA AL NUEVO TRÁFICO DE DATOS

La nueva demanda masiva de intercambio de datos despierta una necesidad que la transmisión mediante internet, por motivos principalmente de latencia y seguridad, no puede satisfacer. Por este motivo, la interconexión, entendida como el tráfico directo, privado, ultrarrápido y seguro de datos, juega un papel fundamental en la transformación empresarial y de las ciudades como forma de facto en la que las organizaciones se mantienen conectadas con sus partners, clientes, empleados y proveedores.

Esta afirmación está avalada por la segunda edición del Índice de Interconexión Global (GXI), un estudio de mercado publicado por Equinix que analiza el intercambio de tráfico global. Según el GXI, se prevé que el ancho de banda de interconexión provisto para este propósito crezca en 2021 a más de 8.200 Terabits por segundo (Tbps) de capacidad, representando una tasa de crecimiento anual compuesto (CAGR) del 48%. Este porcentaje representa casi el doble de la tasa del 26% esperada para el tráfico IP global, es decir, del tráfico del internet público.

La concentración de empresas en determinados distritos de grandes áreas metropolitanas ha sido una tendencia natural en el último siglo. Las compañías con negocios similares, que comparten partners o que buscan sinergias con otras compañías han buscado erigir lugares comunes para que el tráfico de información fuera lo más rápido y eficaz posible, como puede ser el ejemplo del distrito financiero de Londres o de compañías tecnológicas afincadas junto a farmacéuticas que han supuesto grandes avances en innovación sanitaria. Esta tendencia a la concentración ha sido fundamental para comprender la configuración actual de los grandes epicentros de negocios, pero ¿es algo necesario en nuestros días? La interconexión se presenta como un elemento democratizador geográfico, que ofrece grandes a oportunidades a regiones como España, y una prueba más del proceso de globalización tecnológica libre de barreras geográficas.

UNA PLATAFORMA GLOBAL PARA EL FUTURO DIGITAL

Equinix, a través de su plataforma global de interconexión formada por más de 200 data centers interconectados en más de 52 áreas metropolitanas, permite a las empresas poder conectarse al mayor ecosistema de partners del mundo a través de una misma plataforma y un mismo proveedor. Esto implica la posibilidad de escalar los procesos de negocio de las empresas a todos los rincones del planeta y en Equinix permitimos a las empresas operar desde Madrid, Barcelona, Sevilla o Lisboa de la misma forma que desde Ámsterdam o Silicon Valley.

En este nuevo contexto en el que la interconexión actúa como el motor de la economía digital, Equinix ha continuado desarrollando y expandiendo su plataforma global de data centers perfectamente interconectado. En 2019, hemos anunciado la apertura de 12 nuevos data centers y el desarrollo de 23 proyectos de expansión en todo el mundo. Como demanda directa de nuestros clientes, hemos continuado creciendo en mercados en los que ya estamos presentes y seguimos buscando nuevos retos que solucionar. ■

Si te ha gustado este artículo, compártelo

INTELIGENCIA ARTIFICIAL PARA UN CENTRO DE DATOS AUTÓNOMO

La gestión de la infraestructura siempre ha provocado frustración, dolores de cabeza y pérdidas de tiempo. Problemas que causan disrupción en las aplicaciones, ajustes manuales de infraestructura, mayor complejidad a medida que aumentan el número de aplicaciones y la dependencia de la infraestructura? HPE InfoSight es una solución basada en inteligencia artificial que predice y previene problemas en la pila de infraestructura y garantiza un rendimiento óptimo y un uso eficiente de los recursos.

DATOS Y APLICACIONES, soporte de los nuevos modelos de negocio

¿Cómo están tratando las empresas sus datos? ¿Qué aspectos son fundamentales para sus estrategias alrededor de los datos? ¿Cómo están gestionando sus aplicaciones? ¿De qué manera están incorporando nuevas tendencias a la administración de datos y desarrollo de apps?

PAGOS Y COMERCIO: estrategias para transformar ventaja digital para el futuro de las transacciones en tiempo real

Esta guía digital para pagos y comercio describe cómo los líderes de la industria están transformando su ventaja digital para aprovechar una cadena de valor basada en el ecosistema y obtener información en tiempo real y una experiencia fluida.

GUÍA SOBRE EL PANORAMA ACTUAL DE LA CIBERSEGURIDAD

A medida que las organizaciones de todo el mundo continúan su transformación digital, aumenta su dependencia de los sistemas de IT. Al mismo tiempo, los responsables de las amenazas globales se esfuerzan por adaptar, refinar, desarrollar y crear nuevas e innovadoras herramientas y enfoques para propagar ciberataques y evadir su detección.

it whitepapers

itTRENDS

it TRENDS

Ciberinmunidad, un paso más en ciberseguridad

ALFONSO RAMÍREZ,
director general
de Kaspersky
España y Portugal

Vivimos una era de cambio constante, en la que la inmediatez y el carácter transitorio de todo es la norma. En el ámbito en el que se mueve Kaspersky, la ciberseguridad, este hecho es todavía más evidente. Cada día surgen numerosas formas de ataque a la seguridad de los individuos y las organizaciones que nos obligan a estar alerta y a modificar nuestro enfoque de negocio, nuestros productos e incluso a nosotros mismos, por no hablar de nuestra visión de futuro.

Hasta ahora nuestra misión se resumía en el lema "salvar el mundo", en lucha constante con la ciberdelincuencia y sus numerosas formas de presencia. Tras el reciente anuncio de nuestro rebranding, damos paso a un concepto más amplio e innovador, que se centra en el hecho de construir un mundo más protegido y seguro. Y en ello estamos trabajando, desarrollando un futuro real y tangible en el que la vida sea más simple, cómoda e interesante.

No podemos obviar que desde hace tiempo los ciberataques han dejado de dirigirse sólo a empresas. Su foco también se centra ahora en autoridades, organismos y administraciones públicas que tienen una gran cantidad de datos sensibles de millones de ciudadanos – y por ende potencialmente lucrativos – para los ciberdelincuentes. Además, muchas instituciones gubernamentales mantienen infraestructuras críticas como la electricidad o el suministro de agua, y para protegerlos utilizan sistemas en ocasiones anticuados y poco efectivos contra ciberataques modernos.

Por este motivo, bajo nuestro punto de vista, resulta esencial cambiar el enfoque actual de la protección de los sistemas de información, integrando la ciberseguridad desde el diseño de la arquitectura del sistema, en lugar de convertirla en un complemento o una capa que se agrega al final del proceso o cuando surge un problema. Para ello, tenemos que dejar de entender la ciberseguridad como algo reactivo; ya no es válido ser el primero y presentar un dispositivo antes que nadie, sino que hay que garantizar igualmente que esté realmente listo en cuanto a seguridad. En este nuevo

No podemos obviar que desde hace tiempo los ciberataques han dejado de dirigirse sólo a empresas.
Su foco también se centra ahora en autoridades, organismos y administraciones públicas que tienen una gran cantidad de datos sensibles de millones de ciudadanos

escenario, lo que tendrá valor será lanzar al mercado productos inmunes, el proceso será quizás más lento, pero será lo que verdaderamente determine el éxito.

Bajo esta premisa, también es esencial que las autoridades y las administraciones integren en su propia estrategia de defensa tres pilares elementales: prevención, detección y reacción. Y esto sólo funciona y es eficiente cuando se combinan los grandes recursos de datos, el control de los dispositivos y la formación y experiencia de los empleados.

Será entonces cuando el concepto de ciberseguridad quedará obsoleto y podrá dar paso a una nueva forma de entender la seguridad, el de la "ciberinmunidad", entendiendo por tal que el coste de un ciber ataque resulte mayor que el daño que pueda causar, de manera que los ciberatacantes tengan que invertir más recursos (dinero, tiempo, etc.) para llevarlo a cabo.

En este mundo ciberinmune que poco a poco va tomando forma, con un entorno más seguro que estamos ayudando a crear, las tecnologías no serán ya una fuente constante de amenaza, sino que serán el facilitador de nuevas posibilidades, oportunidades y descubrimientos para todos. ■

it User
TECH & BUSINESS

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

Zero Trust, la confianza se ha acabado

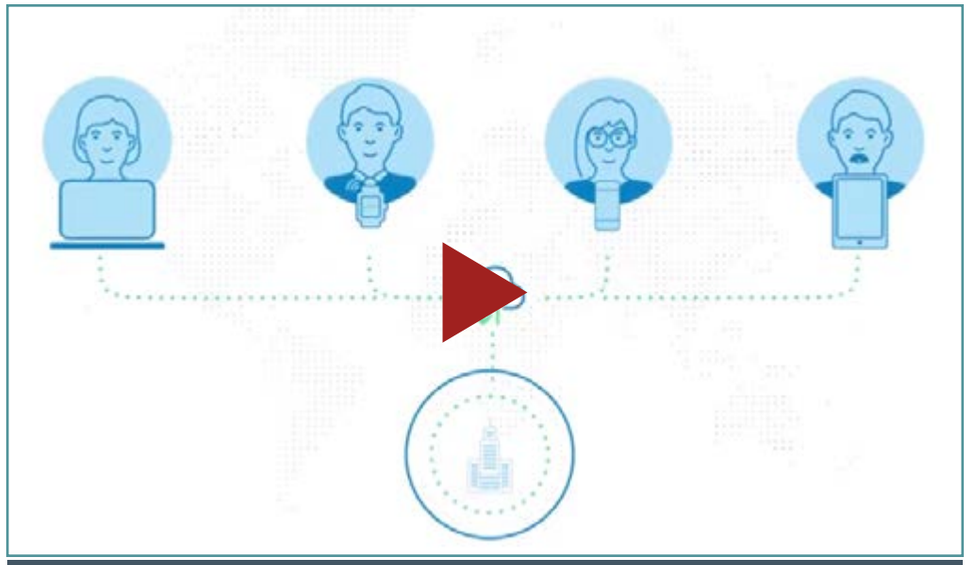
El concepto Zero Trust, o Confianza Cero, no es nuevo. Fue acuñado por John Kindervag, de Forrester, en 2010 y suponía un avance frente al modelo Trust but Verify, en el que todo lo que se encontraba dentro del perímetro era considerado seguro por defecto. El modelo de Kindervag se basa en que las empresas no deben confiar por defecto en nada ni en nadie, y por tanto todo debe ser adecuadamente autenticado en cada momento. Aunque inicialmente el modelo se dirigía principalmente al nivel de aplicación, hoy Zero Trust se promulga como una modelo de seguridad global.

Zero Trust está directamente relacionado con la pérdida de perímetro, un perímetro que saltó por los aires con la movilidad empresarial, con el cloud y que el Internet de las Cosas está llevando al extremo. Al contrario que las redes centradas en el perímetro, el modelo Zero Trust se aplica a usuarios, sistemas y dispositivos. Para acceder a algo la fuente debe ser verificada y autorizada, un proceso en el que entran en juego herramientas como la gestión de identidades y accesos (IAM), la autenticación multifactor o el single-sign-on, o acceso único, que ayude a verificar la identidad del usuario.

La adopción del modelo también está relacionada con un aumento de las amenazas internas. Son muchas las investigaciones que han demostrado que en muchas ocasiones el origen de un ciberataque procede desde dentro de la empresa, y que esto es debido a un fallo a la hora de gestionar las identidades digitales y las conductas de individuos como empleados, partners e incluso los bots o aplicaciones. Y no necesariamente hay que buscar una intención maliciosa, sino que es el resultados de un personal poco entrenado o un bot que adquiere nuevos privilegios.

Según el modelo de seguridad tradicional todo lo que hay dentro del perímetro se considera seguir por defecto, y sólo lo de fuera es no confiable. De forma que cualquier credencial válida puede acceder a la red. Los ciberdelincuentes lo saben y por eso el robo de credenciales en los dos últimos años se ha duplicado. Conforme una investigación de Ponemon Institute desde 2016 la media de incidentes de seguridad a consecuencia de amenazas internas se ha incrementado un 53%. Además, en 2019, las amenazas internas y robo de credenciales se mantienen como el principal factor de riesgo para la ciberseguridad de las empresas

De forma que el reto es hacer que los datos y las aplicaciones sean accesibles a los usuarios adecuados, y de una manera rápida, eficiente y se-



gura. Es un juego entre acceso y control, el no confiar en la estructura interna de la empresas porque el terreno cambia de manera constante, a medida que los empleados van asumiendo nuevos roles que ven modificados sus privilegios de acceso. Y eso sin olvidar que también aparecen nuevas plataformas y aplicaciones… y que la red sigue creciendo.

Sin perímetro tras el que resguardarse y sin poder confiar en nada ni en nadie, las empresas necesitan tener la capacidad de poder autenticar y autorizar a los usuarios, monitorizar políticas y privilegios y detectar cualquier actividad anómala. La adopción de un modelo Zero Trust reduce el número de falsos positivos e incrementa la productividad.

Zero Trust empieza con la garantía de que el usuario adecuado accede el tiempo necesario para realizar una tarea, y conforme a las políticas de la empresa. Para conseguirlo se requiere la implementación de varias políticas, incluida la autenticación multifactor, la puntuación del riesgo, analítica, gestión de permisos, orquestación…

En todo caso, el modelo de confianza cero es más que simplemente usar la tecnología adecuada. Uno de sus beneficios es que ayuda a las organizaciones a superar las limitaciones de la seguridad basada en el perímetro. Al enfatizar la necesidad de verificar las credenciales de los usuarios a intervalos regulares, crea una nueva barrera efectiva para proteger las aplicaciones, los procesos y los datos contra agentes internos maliciosos y actores externos de amenazas.

En el camino hacia la adopción de un modelo Zero Trust se requiere dar una serie de pasos cuyo objetivo final no es otro que ganar visibilidad de toda la red y saber qué usuarios acceden a qué datos y sistemas. De forma que el primer paso sería la identificación de los datos críticos con el fin de

Sin perímetro tras el que resguardarse y sin poder confiar en nada ni en nadie, las empresas necesitan tener la capacidad de poder autenticar y autorizar a los usuarios, monitorizar políticas y privilegios, y detectar cualquier actividad anómala

"Hay que eliminar la creencia generalizada de que el modelo Zero Trust es complejo, costoso y disruptivo"

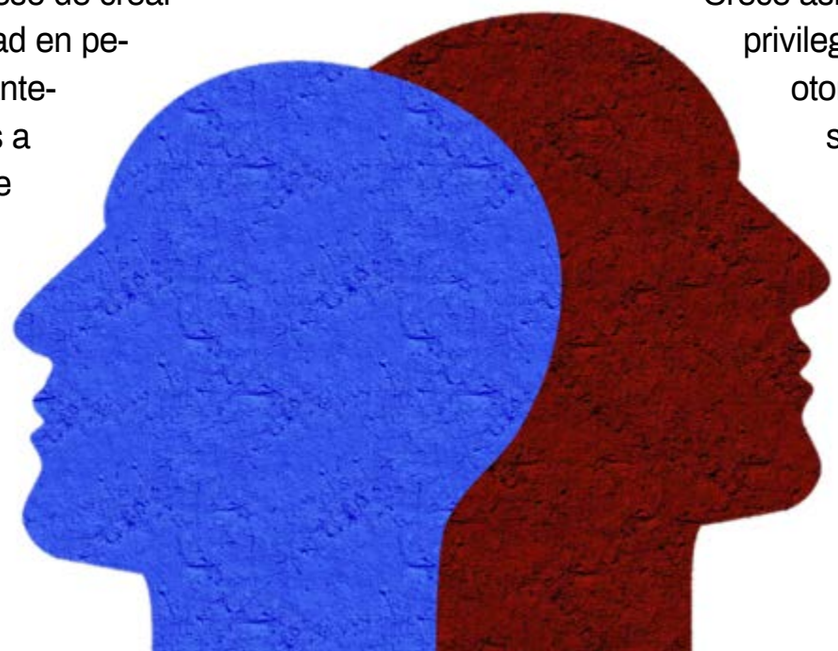
Jesús Díaz Barrero, de Palo Alto

aplicar controles de acceso adicional a los datos y activos que tienen un mayor valor para la organización. Se requiere también evaluar la identidad de la fuente para asignar un nivel apropiado de autorización para cada usuario y dispositivo que intente acceder a la red. Otro paso es determinar la confianza del dispositivo para lo que todos se dividen en gestionados y no gestionados. Los primeros son los que son permitidos por los departamentos de TI y pueden ser fácilmente monitorizados, controlados y actualizados frente a los dispositivos de los empleados de la compañía o subcontratados que tienen acceso a la red corporativa. En una red de confianza cero el sistema debe ser capaz de diferenciar si un dispositivo es gestionado o no y asignar los permisos de acceso más apropiados a cada grupo. Por último, la adopción de un modelo Zero Trust pasa por aplicar control de accesos basado en contexto.

Si traducimos estos pasos a dar en tecnología estaríamos hablando, en primer lugar, de microsegmentación: el proceso de crear perímetros de seguridad en pequeñas áreas para mantener accesos separaros a las diferentes partes de la red. La segmentación permite que los archivos se puedan colocar en zonas seguras separadas de forma que un usuarios o programa no sería capaz de acceder a ninguna otra zona sin una autorización adicional.

Uno de los beneficios de la microsegmentación es que incluye políticas integradas que tienen en cuenta el comportamiento y la protección de manera individual. Tener en cuenta la visibilidad del comportamiento de las aplicaciones en los dispositivos que acceden a ellas también debe tenerse en cuenta para poder detectar una actividad anómala y tomar medidas más rápidamente. Y al hacerse en un entorno aislado, o segmentado del resto de la red, se contendrá cualquier infracción y se evitará la propagación al resto de la red.

Ya hemos mencionado la autenticación multifactor, que permite añadir más piezas que el ciberdelincuente necesita conseguir para acceder a los sistemas. El uso de un doble factor de autenticación, como es el envío de un código a otro dispositivo, ya es algo aceptado por los usuarios. Además, otras formas de autenticación, como las biométricas, están a la orden del día.



Crece asimismo el principio de privilegios mínimos. Es decir, otorgar a un usuario el acceso que necesita sólo para un propósito o función en particular. Es un aspecto clave del demo de confianza cero y una manera de unificar la seguridad del usuario final y del centro de datos. Reduce el ries-

go a un nivel segmentado, a aplicaciones y datos, y es una forma de contener o reducir el perímetro de cada dispositivo individual: un teléfono inteligente o una estación de trabajo, o cualquier otro dispositivo, obtiene acceso solo a lo que el usuario necesita.

Zero Trust y Compliance

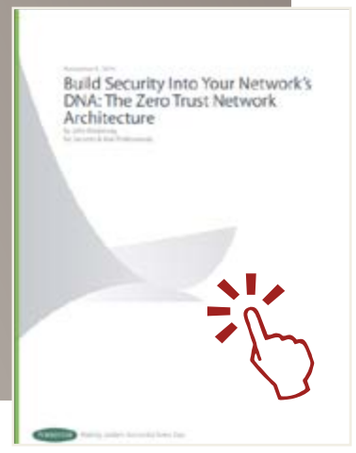
Las regulaciones, no sólo el famoso Reglamento General de Protección de Datos, sino PSD2 o la Directiva NIS. En un momento en que la premisa es proteger los datos y hacer un seguimiento de ellos, cuando la mayoría de la infraestructura de datos de las empresas reside fuera del firewall corporativo, las regulaciones en general han aumentado la carga de trabajo de los equipos de seguridad.

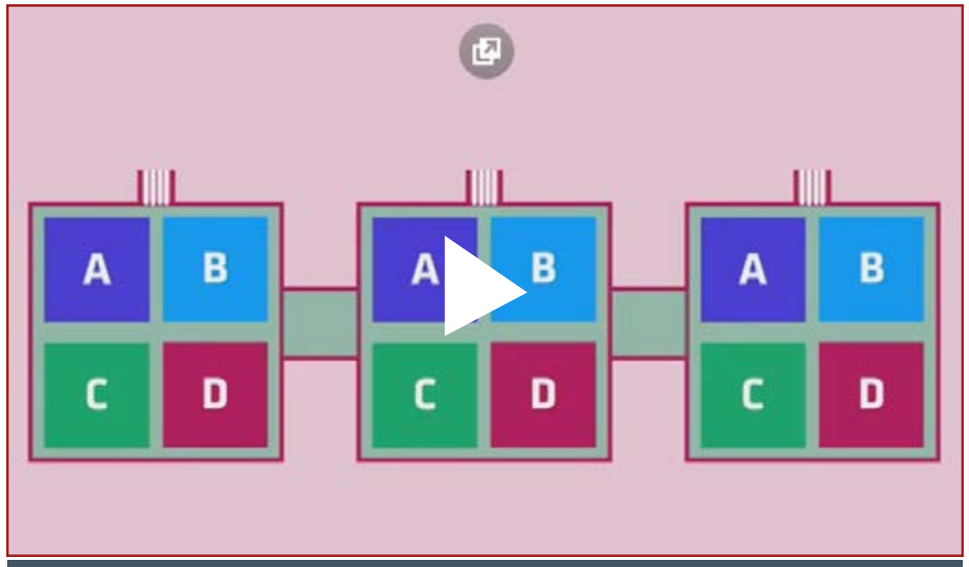
Son muchas las brechas de seguridad que se producen después de que los ciberdelincuentes exploten vulnerabilidades en puntos finales para luego moverse lateralmente dentro de su entorno en busca de datos, lo que está impulsando a las empresas a adoptar el modelo Zero Trust, que verifica la identidad y la carga útil cada vez que se intenta un movimiento de este a oeste, deteniendo el ataque antes de poder llegar a los datos.

Aseguran los expertos que con el modelo de confianza cero, las empresas adoptan una mejor postura de seguridad en dos aspectos clave, tanto en el descubrimiento de todos los activos de la red como en el control de acceso. En el primer caso, como ya hemos ido diciendo, se busca un inventario de aplicaciones, bases de datos y otros activos clave; Zero Trust significa que los activos se descubren automáticamente, y los mandatos de cumplimiento se pueden aplicar a través de la documentación adecuada y el mantenimiento de registros.

SEGURIDAD EN TU RED: THE ZERO TRUST NETWORK ARCHITECTURE

En 2010, Forrester Research publicó un documento que popularizó el concepto de Zero Trust, o Confianza Cero. En su documento, Forrester discutió cómo este modelo de seguridad se basa en la idea de que las empresas no deberían confiar inherentemente en ningún usuario o red, y la creencia de que cualquier intento de acceder a un sistema o aplicación comercial debe verificarse siempre antes de cualquier nivel de se concede acceso.





QUÉ, POR QUÉ Y CÓMO DE LA ZERO TRUST NETWORKING

CLICAR PARA VER EL VÍDEO

En cuanto al acceso con privilegios mínimos, es decir, otorgar acceso solo a los recursos que realmente lo requieren, reduce la superficie de ataque y demuestra a los usuarios, auditores, reguladores e incluso a los tribunales que la organización ha tomado todas las medidas razonables para proteger los datos contra el acceso no autorizado. Como beneficio adicional, esto deja un rastro de auditoría para reconstruir los eventos de seguridad si ocurre una violación.

¿Por qué ahora?

Decíamos al comienzo que este modelo de seguridad se gestó hacia 2010. Es ahora cuando parece que está ganando adeptos. El modelo Zero Trust parte de la constatación de que los perímetros tradicionales son complejos, incrementan el riesgo y ya no son adecuados para los modelos de negocio actuales, dice Enric Mañez, Enterprise Security Sales de Akamai. Los usuarios, los dispositivos, los datos y las aplicaciones se están trasladando fuera del perímetro de la empresa y de la zona de control, y los nuevos procesos empresariales, impulsados por la transformación digital, incrementan el riesgo a la exposición. “Es por ello, que fabricantes de diferentes áreas están empujando el modelo”, dice el ejecutivo, enumerando una serie de razones por las que Zero Trust está siendo más popular:

- **Panorama de amenazas cada vez más hostil**
- **Velocidad y escala del negocio**
- **Ecosistema cada vez más amplio y disperso**
- **Migración a la nube y modelo SaaS de aplicaciones corporativas**
- **Los recursos de TI están cada vez más sobrecargados**

Jesús Díaz Barrero, Manager, Systems Engineering Spain & Portugal de Palo Alto Networks, prefiere diferenciar entre clientes y proveedores de seguridad cuando habla sobre el motivo por el que se está popularizando el modelo. “Para los clientes, el modelo resulta atractivo porque representa un concepto de diseño de seguridad agnóstico y efectivo para prevenir los ciberataques modernos. Por otro lado, los proveedores de seguridad encuentran en el modelo Zero Trust una oportunidad en la que intentar encajar sus productos o soluciones”, asegura.

En el camino hacia la adopción de un modelo Zero Trust se requiere dar una serie de pasos cuyo objetivo final no es otro que ganar visibilidad de toda la red y saber qué usuarios acceden a qué datos y sistemas

"El problema más habitual es que las organizaciones no apliquen el modelo Zero Trust de manera efectiva y se queden en la teoría o solo inicien algunos pasos insuficientes"

José Luis Paletti, Presales Engineer, Cytomic

En resumidas cuentas, y como concluye Samuel Bonete, Director general de Netskope en España y Portugal: "esta transformación digital dentro de las organizaciones también obliga a una transformación de la seguridad que hoy en día es indispensable".

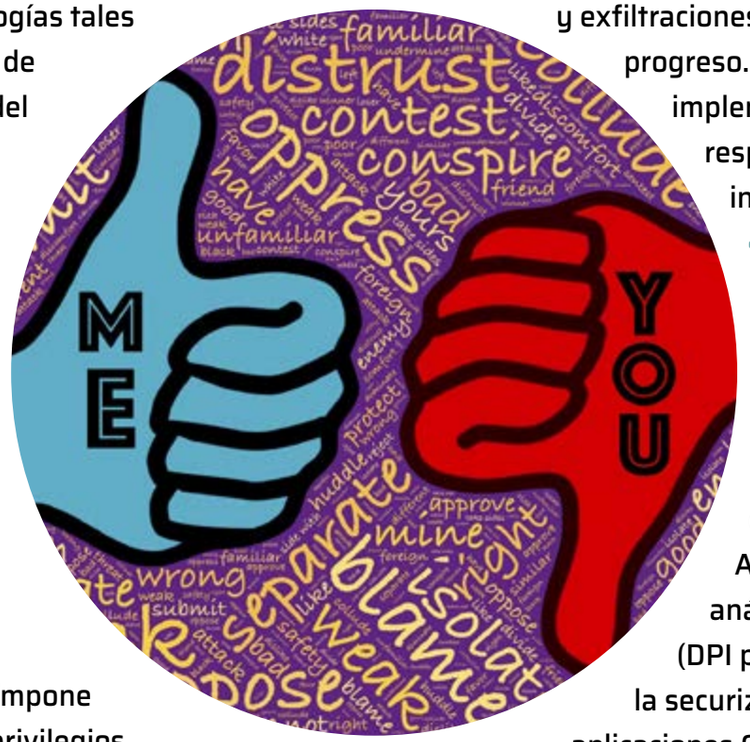
Beneficios del Modelo Zero Trust

"Los beneficios principales de utilizar una arquitectura Zero Trust es la protección desde todos los puntos, incidiendo también desde dentro de las organizaciones", dice Julia Barruso, Channel Account Manager Iberia, explicando que los modelos más tradicionales de seguridad se han focalizado en la protección del perímetro de red, una fórmula "que ha demostrado ser insuficiente ya que muchas de las brechas se producen desde dentro de las organizaciones". Y precisamente por eso, el modelo de confianza cero añade otro beneficio a la seguridad de la empresa: el incremento de protección de los datos que residan fuera de la red corporativa, hoy en día. "La mayoría de las empresas tienen datos residiendo en la nube. Quitando el foco de la protección del perímetro y poniéndolo en la verificación de identidad nos da la habilidad de proteger el dato esté donde esté", dice Julia Barruso.

Rafael Esteban, Responsable de Ventas para el Sur de Europa de LogRhythm, habla de "una me-

Principios de Zero Trust

- AKAMAI. Las empresas que están adoptando un modelo de seguridad Zero Trust aplican una política básica de “verificar y nunca confiar” siguiendo algunos principios básicos: Acceso a nivel de aplicación en lugar de a nivel de red; Funciones de seguridad avanzadas (SSO, MFA, 2FA, etc.); Gestión de TI sencilla; Supervisión y elaboración de informes de forma sencilla, rápida e integrable con SIEM existentes; Experiencia de usuario optima
- CYTOMIC. Zero Trust eXtended (ZTX), una evolución de Zero Trust, aplica los siguientes pilares: La red: ¿cómo funciona la tecnología para permitir los principios de aislamiento, segmentación y, en última instancia, seguridad de la red?; Los datos: ¿cómo se permite la categorización, los esquemas, el aislamiento, el cifrado y el control de los datos?; Los recursos humanos: ¿cómo se protege a las personas que están utilizando la red y la infraestructura de la empresa? ¿Y cómo se reduce la amenaza que crean los usuarios?; La carga de trabajo: ¿de qué manera se aseguran áreas tales como las redes en la nube, las aplicaciones y cualquier otra cosa que una empresa u organización utilice para hacer que opere técnicamente?; La automatización y orquestación; La visibilidad y el análisis.
- FORCEPOINT. Zero Trust se basa en el principio de la “no confianza” y verificación. Para poderlo llevar a cabo se necesitan diferentes tecnologías y mejores prácticas: Menor acceso-privilegios; Microsegmentación; Múltiple Factor de Autentificación; Controles de Seguridad adaptada al riesgo.
- NETSKOPE. Zero Trust generalmente se logra a través de cambios en los procesos de seguridad y la implementación de tecnologías tales como: Identidad y Gestión de Acceso (IAM); Evaluación del dispositivo de un usuario para confirmar si el dispositivo con el que se conecta es seguro, antes de que se le permita acceder a las aplicaciones; Un método seguro de conexión a aplicaciones y servicios, que históricamente ha tenido que ver con la segmentación de la red, o micro-segmentación, que impone un modelo de acceso con privilegios mínimos dentro de una red interna.



- PALO ALTO. Como premisas fundamentales en el desarrollo del modelo han de seguirse las siguientes premisas: Todos los recursos son accedidos de manera segura, independientemente de su localización; El control de acceso es estrictamente forzoso para todos los usuarios; Verificar y no confiar nunca; Inspeccionar y “loguear” todo el tráfico; Diseñar la red desde dentro hacia fuera, acercando la seguridad tanto como sea posible al origen de la comunicación.
- LOGRHYTHM. Proveer a los equipos de seguridad de herramientas que les proporcionen visibilidad de lo que ocurre en sus organizaciones, con un importante componente de análisis en tiempo real que les de capacidad de identificar y abordar vulnerabilidades de alto riesgo en su entorno o de detectar intrusiones y exfiltraciones de datos que ya están en progreso. Siendo importante también implementar soluciones de respuesta rápida ante los citados incidentes.
- SONICWALL: Al desaparecer el perímetro, la única manera de proteger datos, usuarios e infraestructura es construir una defensa en capas, desde el firewall de nueva generación, el Access point WIFI seguro, el análisis del tráfico encriptado (DPI packet inspection SSL-TLS), la securización del email, la de las aplicaciones Cloud (Dropbox, G-Suite, Office365, etc.), el uso de sandboxing avanzado para detección de amenazas avanzadas desconocidas, etc. Hasta el endpoint de nueva generación basado en comportamiento.
- SOPHOS: El sistema se basa en tres principios básicos. En primer lugar, el análisis, descubre usuarios, aplicaciones, dispositivos y datos, tanto on premise como en cloud y los identifica y autentica en tiempo real. El segundo principio es la adaptación, generando políticas de seguridad que se basan en la detección de amenazas, el comportamiento de los usuarios en el sistema y las guías de cumplimiento. Y, por último, la automatización, basada en el control de acceso a la red y al Wi-Fi, el aislamiento automático de cualquier amenaza y la optimización del tráfico del ancho de banda.

nor exposición ante amenazas dirigidas y un mayor control de lo que ocurre dentro de nuestras redes" cuando se mencionan los principales beneficios del modelo Zero Trust.

Para Sergio Martínez, Director general de SonicWall para España y Portugal, el principal beneficio de Zero Trust es que "la desconfianza hacia todo hace evolucionar la defensa hacia algo mucho más sofisticado, orientado a detectar, prevenir y bloquear ataques y malware de todo tipo en tiempo real. Aquí el conocimiento y la evolución de las tecnologías de defensa son claves para conseguir esta estrategia defensiva tan exigente".

Controlan las acciones del dispositivo desde el mismo momento en el que accede a la red para poder detectar un comportamiento inusual es, en opinión de Jose Luis Paletti, Presales Engineer de Cytomic, uno de los beneficios que aporta el modelo Zero Trust. Dice este experto que el control de la información es esencial, ya que desvía la atención del modelo ZT de los puntos más tradicionales y la centra en el objetivo final de cualquier brecha en la seguridad. "Esto da una ventaja esencial y es que ya no hay que preocuparse de fallos según su origen sino su objetivo, por lo que ya no cabe esperar la sorpresa y las compañías pueden prepararse para cualquier cosa, porque controlan la meta del ataque y tienen establecida una respuesta ágil y óptima para que no se produzcan fugas de información", dice Paletti.

"Los beneficios principales de utilizar una arquitectura Zero Trust es la protección desde todos los puntos, incidiendo también desde dentro de las organizaciones"

Julia Barruso, Channel Account Manager Iberia, Forcepoint

Alberto R. Rodas, Sales Engineer Manager Iberia de Sophos apunta a que el principal beneficio de este modelo es estar siempre prevenidos frente a cualquier desafío. La estrategia Zero Trust se anticipa a cualquier amenaza, verificando y registrando todos los elementos conectados al sistema para evitar cualquier posible ataque, tanto desde fuera de una organización como desde dentro y actuando de forma proactiva y no reactiva. Además, garantiza la seguridad en todo el perímetro de la red y no ralentiza las respuestas frente a amenazas al no contemplar las infinitas posibilidades de protección frente a los diferentes ciberataques, algo cada vez más difícil de abarcar.

Además del beneficio obvio asociado a la mejora en la postura de seguridad, es importante destacar otros dos, dice Jesús Díaz Barrero, de Palo Alto: Simplificación en las operaciones de seguridad que realizan los SOC y reducción de errores humanos. En el primer caso, ya que idealmente no ha de existir diferencia en la cantidad de mecanismos de seguridad que se aplican para cualquier tipo de acceso, por lo que la operativa resulta más sencilla. En el segundo explica Díaz Barrero que, al utilizar políticas de seguridad homogéneas, la probabilidad de cometer un error que deje una puerta abierta se reduce.

Cuando se implementa íntegramente, Zero Trust puede mejorar la experiencia del usuario final, proteger los datos de una organización, simplificar las operaciones de seguridad y aumentar la visibilidad del comportamiento del usuario, asegura Samuel Bonete, añadiendo que “Zero Trust también puede facilitar la transformación digital dentro de una organización, permitiendo la adopción segura de la nube y soportando el aumento de la movilidad del usuario”.

Enric Mañez, de Akamai, resumen los beneficios del Modelo Zero Trust de la siguiente manera:

- **Protección frente a fuga de datos**
- **Reducción del tiempo de detección de brechas de seguridad** y tener mayor visibilidad del tráfico hacia aplicaciones corporativas
- **Reducción de la complejidad en la arquitectura de seguridad**
- **Flexibilidad, agilidad y facilidad de uso**
- **Mayor seguridad** y mejor experiencia de usuario
- **Facilita la migración a Cloud** de aplicativos y recursos internos

Adopción del Modelo Zero Trust

Preguntamos a los expertos consultados si los responsables de seguridad de las empresas están

"Siempre es difícil adoptar nuevos modelos que rompen con lo que 'tradicionalmente' se ha hecho, pero el modelo Zero Trust permite la convivencia con las soluciones/arquitecturas anteriores e ir migrando de forma progresiva"

Enric Mañez, Enterprise Security Sales, Akamai

aplicando este modelo. Luis Paletti, de Cytomic dice que la mayor parte de las empresas no cuentan con un modelo Zero Trust como parte de su estrategia en ciberseguridad, “o no lo están implementando de manera efectiva. El por qué es sencillo: las empresas y los responsables de seguridad que están entre sus filas no comprenden por completo la tecnología tras el sistema, al igual que tampoco terminan de entender los cambios organizativos que deben realizar para implantarlo”. Añade el ejecutivo que es importante que las compañías acudan a terceras empresas especialistas en el campo e incorporen las herramientas necesarias para asimilar e implantar el concepto en su estructura de ciberseguridad, y recomienda Panda Adaptive Defense 360, una solución que ha sido especialmente diseñada para monitorizar toda la actividad, exponiendo cualquier actividad sospechosa, centrándonos en la información a la que van dirigidos los ataques antes incluso de que ocurran.

Opinión similar es de la Sergio Martínez, quien asegura que “el modelo de una defensa estática basada en firewall está evolucionando rápidamente gracias a esta visión Zero Trust”. Dice también el directivo de SonicWall que la experiencia de CISOs y Directores de IT es la de amenazas cada vez más inteligentes y dirigidas, al tiempo que menciona un problema cada vez más extendido: lo que llamamos “Shadow IT”, o aplicaciones Cloud utilizadas por los empleados sin conocimiento por parte del departamento de IT, que introducen riesgos insospechados como la descarga de ficheros vía Dropbox en los equipos corporativos vía HTTPS.

"El modelo Zero Trust basa su funcionamiento en controlar y verificar cada dispositivo que se conecte a una red o sistema como si fuera el de un extraño, incluso dentro de una empresa"

Alberto R. Rodas,
Sales Engineer Manager Iberia, Sophos

Julia Barruso, de Forcepoint, recuerda que como parte de la transformación digital los perímetros han dejado de estar acotados y las empresas tienen la necesidad de tener en cuenta las aplicaciones, datos, usuarios y dispositivos donde sea que se encuentren; “esto requiere un nuevo planteamiento, no sólo de negocio sino también de seguridad”. Reconoce que las compañía van paso a paso y que “Zero Trust no se puede acometer de un día para otro, es un camino que hay que recorrer”. Menciona la directiva soluciones como Dynamic Data Protection, con la que Forcepoint ayuda a facilitar este camino y a entender la interacción de datos y usuarios pudiendo incluso prevenir las posibles fugas de información. “De este modo, se requiere menos administración, se dan menos falsos positivos y se ayuda a las compañías a asegurar los nuevos modelos de negocio”, concluye la responsable de canal de Forcepoint.

Jesús Díaz Barrero, de Palo Alto, dice que a pesar de que el modelo Zero Trust ha generado mucho interés en los últimos años “aún estamos lejos de ver una implementación generalizada y que el proceso de adopción va a ser lento. Muchas compañías aún no tienen ni siquiera una estrategia de microsegmentación en el datacenter físico y virtual para la inspección del tráfico este-oeste, lo que constituye uno de los pilares para construir el modelo”.

Rafael Esteban, de LogRhythm, menciona la necesidad de tiempo para “abandonar viejos hábitos pese a que los profesionales del sector en su mayoría son conscientes del escenario actual”.

“Siempre es difícil adoptar nuevos modelos que rompen con lo que ‘tradicionalmente’ se ha hecho,

pero el modelo Zero Trust permite la convivencia con las soluciones/arquitecturas anteriores e ir migrando de forma progresiva", dice Enric Mañez, de Akamai. Explica el directivo que la mayoría de las empresas no puede asumir una transformación completa al modelo de seguridad Zero Trust de la noche a la mañana, que muchas necesitan cierto tiempo para implementar por completo los cambios de red y de seguridad más importantes que dicha transformación supone. "No obstante, sí que vemos que se están dando algunos sencillos pasos para ponerla en marcha, generalmente comenzando por un grupo de usuarios con una exposición mayor a amenazas y hacia aplicaciones que permiten una migración más sencilla", dice Mañez.

De manera más concreta, se observa cómo las empresas trabajan en la categorización de los distintos perfiles de usuarios y aplicaciones, así como el desarrollo de un plan gradual o plan integral de migración del estado actual a un marco Zero Trust para todas las aplicaciones (incluidas las locales heredadas, "legacy").

Para Alberto Rodas, de Sophos, la adopción del modelo Zero Trust entre los responsables de seguridad es menor de lo deseado, "pues muchas veces, optan por un compendio de soluciones que hacen muy complicado el no preestablecer relaciones de confianza entre los diversos productos". Explica Rodas como ejemplo que los firewalls deben "fiarse" de que los endpoints están en un buen estado de salud y, salvo que vean un tráfico realmente malicioso, confiarán por defecto en éstos, sin llevar a cabo ningún tipo de comprobación. "También vemos que preestablecen relaciones de confianza en el tráfico de red, pues cuando sus equipos capa7 no pueden identificar una aplicación en base a firmas,

"El mayor beneficio del modelo Zero Trust es una menor exposición ante amenazas dirigidas y un mayor control de lo que ocurre dentro de nuestras redes"

Rafael Esteban, Responsable de Ventas para el Sur de Europa, LogRhythm

"Al desaparecer el perímetro, la única manera de proteger datos, usuarios e infraestructura es construir una defensa en capas"

Sergio Martínez, Director SonicWall Iberia

confían en que es "Generic TCP" y lo dejan entrar si pasa por algún puerto abierto y no incumple ninguna regla de IPS", añade el experto. Las soluciones de Sophos "no dan por supuesto que los endpoints se encuentran no vulnerados, sino que exigen una prueba para comprobar que así es. También, en caso de haber tráfico de red no reconocido, automáticamente el firewall podrá interrogar al puesto de trabajo para que éste aclare cuál es y, por tanto, si debe ser o no permitido", dice Rodas.

Samue Bonete asegura que la mayoría de los profesionales de la ciberseguridad son conscientes de los principios de Zero Trust; "sin embargo, normalmente no construirán un entorno de TI desde cero. Esto significa que se deberá introducir gradualmente una estrategia de confianza cero en sus entornos y procesos existentes". Pone como ejemplo el directivo que Netskope ve a las organizaciones que buscan reemplazar las VPN de acceso remoto tradicionales con alternativas de Zero Trust Network Access (ZTNA) como Netskope for Private Access. "Es posible que la mayoría de las organizaciones ya tengan algunos elementos de Zero Trust, como la autenticación multifactor o SIEM, que puede ser el punto de partida para una futura implementación", reconoce el directivo de Netskope.

Retos de aplicación del modelo Zero Trust

Sobre los retos a los que se enfrenta la adopción del modelo de confianza cero promulgado por Forrester hace casi diez años, Rafael Esteban, de LogRhythm, lo tiene claro: "Capacidades de adaptación al cambio, concienciar a los clientes de la necesidad de proteger sus mejores activos, los datos y comprender que el perímetro no es suficiente, que no se trata de si los atacantes van a entrar, sino de cuando lo harán".

Menciona Jesús Díaz Barrero, de Palo Alto, que hay que eliminar "la creencia generalizada de que el modelo es complejo, costoso y disruptivo". Expli-

"La transformación digital dentro de las organizaciones también obliga a una transformación de la seguridad que hoy en día es indispensable"

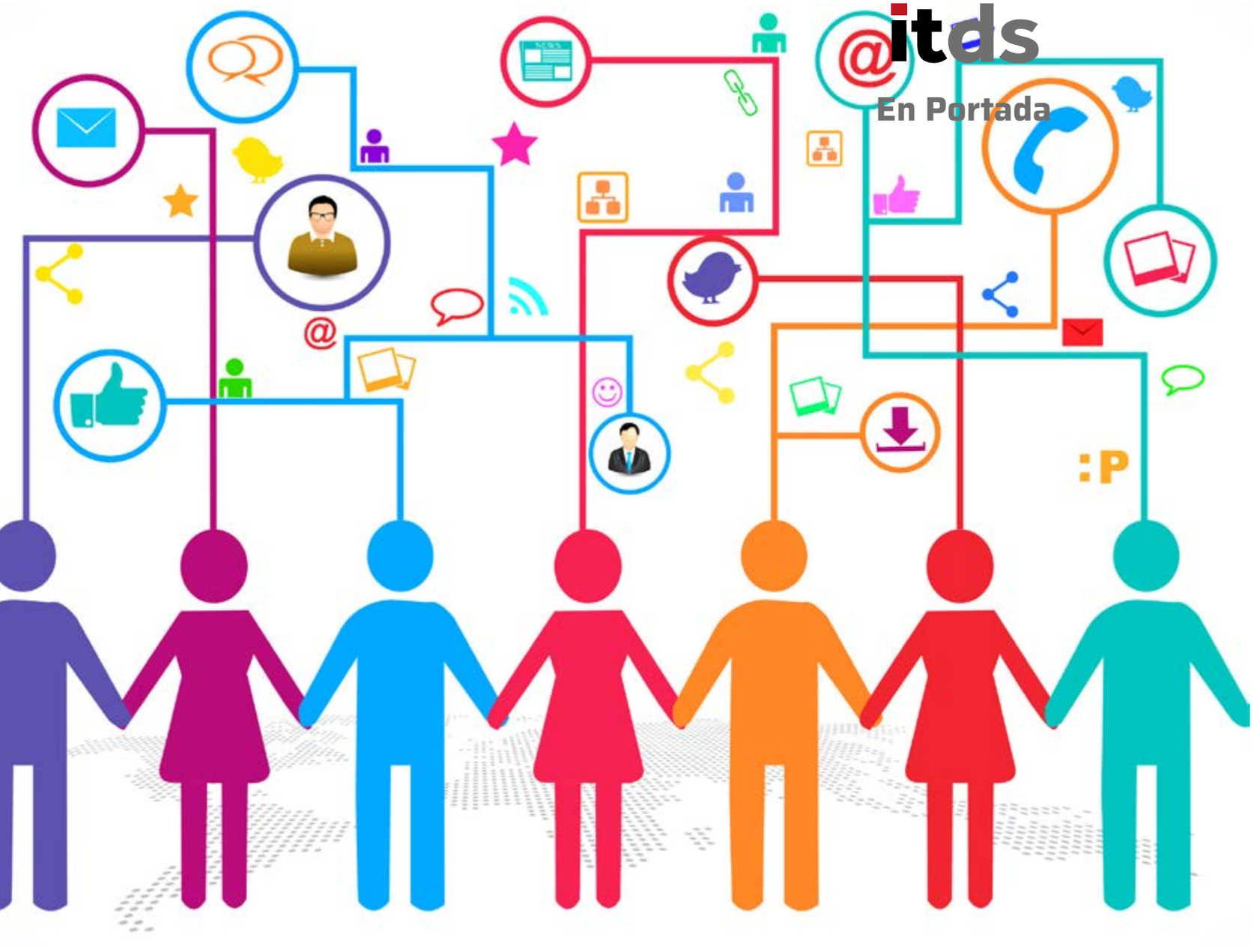
Samuel Bonete, Director general, Netskope en España y Portugal

ca el directivo que el mayor reto es precisamente la comprensión de que Zero Trust implica un cambio en el paradigma de construcción de la seguridad sobre las redes, al que muchos arquitectos están acostumbrados; "es necesario abandonar el modelo clásico, basado en la confianza o desconfianza y que ha demostrado su inefectividad en múltiples ocasiones, y adoptar uno nuevo basado en la "no confianza". De entrada, los humanos somos reactivos al cambio y pensamos que el nuevo modelo va a ser más complejo que el anterior, pero la realidad es que Zero Trust es más sencillo de implementar", asegura el experto.

También habal Díaz Barrero de otro reto importante: explicar y convencer a los responsables de seguridad de que la adopción del modelo Zero Trust no tiene por qué implicar un incremento en los costes, y que no ha de implementarse de un día para otro. "No se trata de tirar a la basura todos los sistemas de seguridad con los que ya cuentan, sino de ir poco a poco adaptándolos y complementándolos para adoptar el modelo paulatinamente. Zero Trust puede convivir perfectamente con los modelos tradicionales para garantizar una transición no disruptiva con los servicios que protege", dice el Manager, Systems Engineering Spain & Portugal de Palo Alto.

Recuerda julia Barruso que los cambios no son fáciles y que "no estamos hablando de implementar una solución sino de un cambio de modelo y gestión". Dice Barruso que la búsqueda de diferentes productos que puedan trabajar conjuntamente es necesaria, y que las soluciones de Forcepoint se integran entre sí y con terceros, dando mayor cobertura a las empresas. "Con la integración de nuestro Next Generation Firewall, Casb, Proxy, DDP conseguimos una mayor visibilidad y una defensa mucho más precisa. La inversión, el aprendizaje y la aceptación del cambio son los mayores retos para poder implementar el modelo Zero Trust, aun así, el camino se hace andando y hay una clara tendencia hacia este nuevo modo de afrontar la seguridad", concluye la directiva.

"La seguridad TI tiene una larga historia que se ha enfocado en el perímetro, y uno de los desafíos de optar por Zero Trust es cambiar la mentalidad de



Enlaces de interés...

- ‘Zero-Trust’: la prevención de intrusiones, cada vez más relevante en las estrategias de seguridad
- Okta hace más accesible el modelo Zero Trust con la compra de ScaleFT
- W Zero Trust Networks
- W Seguridad en tu red: The Zero Trust Network Architecture

los miembros del equipo de seguridad. No porque una red sea interna implica que sea segura”, dice Samuel Bonete, añadiendo que otro reto es simplemente empezar; “implementar Zero Trust no es una tarea trivial, en una organización grande puede ser un proyecto de varios años”.

Menciona Sergio Martínez el “optimismo mediterráneo clásico”, ese “a mí no me va a pasar nunca” como uno de los retos en la adopción de este modelo. Recuerda el directivo “la necesidad de abordar la seguridad de una manera más holística y, sobre todo, incorporar la ciberseguridad en el ADN de las compañías, para proteger a sus empleados, infraestructuras y, sobre todo, datos”.

“El problema más habitual es que las organizaciones no apliquen el modelo Zero Trust de manera efectiva y se queden en la teoría o solo inicien algunos pasos insuficientes”, dice Jose Luis Paletti, Presales Engineer de Cytomic, añadiendo que, en este sentido, el gran reto es que comprendan del todo la tecnología y los cambios organizativos necesarios para ponerlo en práctica.

En todo caso, lo que parece claro es que al adoptar el modelo de confianza cero ahora, las organizaciones pueden comenzar a sentar las bases de todos y cada uno de los desafíos que surjan en el futuro, al mismo tiempo que obtienen una comprensión más completa de las arquitecturas de datos dinámicas en expansión y las vulnerabilidades que contienen.


it Reseller
TECH&CONSULTING
nº 47
JULIO 2019
El partner como motor de la transformación digital de las empresas, a debate
MONOGRÁFICOS
DIGITAL SIGNAGE
GRAN OPORTUNIDAD PARA EL CANAL
La ciberseguridad en 2019 y el papel del canal, a debate
Formación:
potenciando el talento en el canal
it Reseller
TECH&CONSULTING
Cada mes en la revista,
cada día en la web.

it Digital Security

Tribuna IDC

Alineación de la gestión del riesgo con el plan de ciberseguridad

¿Quién no se lleva las manos a la cabeza cuando se habla de gestión del riesgo? Hablar de riesgo en un mundo digital hiperconectado, como en el que vivimos, es sinónimo de complejidad y preocupación.

EMILIO CASTELLOTE

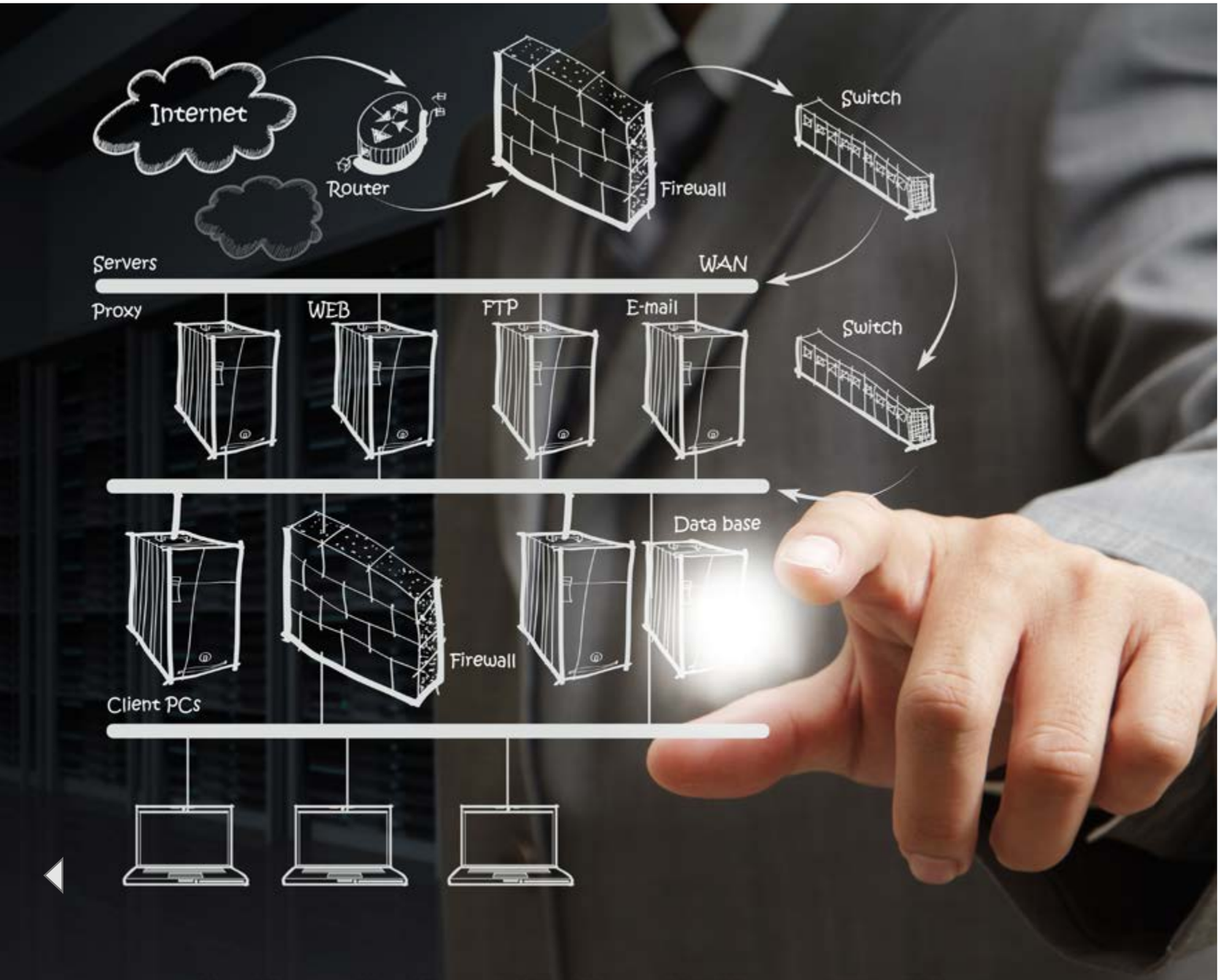
IDC SENIOR RESEARCH ANALYST

Con 20 años de experiencia en las áreas de TI, telecomunicaciones y ciberseguridad, en los últimos dos Emilio Castellote años ha estado trabajando en el desarrollo de Startups, dirigiendo las áreas de estrategia de Marketing y Ventas en compañías como Genetsis Solutions o Hdiv Security.

Anteriormente ocupó cargos como Director de Canal, Director de Marketing de Producto, Director de Pres Venta y Gerente de Producto en Panda Security; Profesor asociado de la Escuela de Ingeniería y Sistemas de Telecomunicación de la Universidad Politécnica de Madrid y Profesor de diversos Masters de Ciberseguridad impartidos por la Universidad Pontificia de Salamanca y la Universidad Europea de Madrid.

Compartir en RRSS

Precisamente esas son las dos premisas básicas que deberemos contemplar a la hora de establecer un plan de gestión del riesgo adecuado a las circunstancias digitales actuales. Deberemos buscar simplificación, facilitando la visibilidad del escenario global, y reducción del nivel de impacto en la preocupación que podemos sufrir.



La tendencia de mercado es clara al respecto, el nuevo escenario digital se posiciona bajo un entorno multicloud, en el que el usuario transita por varias nubes y por varios dispositivos, haciendo uso del dato en la mayor de las ubicuidades posibles.

Las prioridades de inversión en materia de ciberseguridad nos dan la clave para diseñar un plan de gestión del riesgo adaptado al escenario actual. El 50% de la inversión en ciberseguridad que realizarán las organizaciones en España este año será en servicios de ciberseguridad. Estos servicios se reparten a partes iguales entre integración y gestión.

El plan de gestión de riesgo debe estar integrado con la estrategia de ciberseguridad y viceversa. Cualquier nueva estrategia de ciberseguridad, y por consiguiente la adecuación del plan de gestión de riesgo, deberá basarse en un modelo de servicios gestionados. Si queremos tener visibilidad del ciclo de vida del dato en las organizaciones, será imprescindible combinar diferentes servicios ges-

El 50% de la inversión en ciberseguridad que realizarán las organizaciones en España este año será en servicios de ciberseguridad

GESTIÓN DEL RIESGO Y LA SEGURIDAD A LA VELOCIDAD DEL NEGOCIO DIGITAL

La Transformación Digital está cambiando el paisaje tradicional de gobierno y control de TI. Por un lado la autoridad del responsable de TIO se ve a menudo superada a favor de una mayor autonomía en el despliegue de nuevas tecnologías digitales. Por otro, el incremento de nuevos elementos (sistemas, dispositivos e incluso datos) genera problemas de escalabilidad para los que algunas soluciones de seguridad no están preparadas.

¿Cómo hacer frente a esta nueva realidad manteniendo bajo control la gestión del riesgo y la seguridad y siendo facilitadores digitales de negocios en lugar de obstáculos para la innovación?

tionados de ciberseguridad que ayuden a consolidar el plan de gestión de riesgo con una política de ciberseguridad alrededor de este, que permitar ubicar el punto de observación en el escenario multicloud para aportar el mayor nivel de visibilidad disponible.

El escenario multicloud está ligado al servicio, por lo que deberemos buscar aquellos proveedores de servicios especializados que puedan ayudarnos a construir nuevas estrategias de ciberseguridad orientadas a liberar los escasos recursos del área TI. De esta forma, podrán ser dedicados a tareas más productivas y alineadas con el negocio, como la correcta explotación del valor que puede llegar a generar el dato. Para ello será vital que el proveedor de servicios simplifique al máximo el nivel de interacción de sus clientes y aporte la información necesaria de manera sencilla y visual para que estos puedan tener controlado su escenario y una visibilidad del nivel de riesgo al que están expuestos.

Los nuevos planes de gestión de riesgo evolucionan una vez más, tomando al dato como activo más importante para las organizaciones. Será necesario integrar en su diseño nuevas variables de entorno que transformen los tradicionales indicadores de riesgo hacia un modelo de comportamiento. El nuevo marco colaborativo significará compartir información con terceros para intentar cerrar al análisis del círculo de riesgo que permita ejecutar iniciativas proactivas para mitigar cualquier posible incidente.

> Los nuevos planes de gestión de riesgo evolucionan una vez más, tomando al dato como activo más importante para las organizaciones

Enlaces de interés...

- Publicado el listado de tratamientos en los que es obligatorio realizar una evaluación de impacto
- Tendencias en gestión del riesgo y la seguridad
- Análisis de riesgos en tiempo real, el papel de los escáneres de vulnerabilidades

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos IT User

Almacenamiento it

Con la colaboración de: Hewlett Packard Enterprise

MIGUEL OLÍAS DE LIMA

GERENTE DE RISK ADVISORY, DELOITTE

Miguel Olías de Lima es ingeniero en Informática, por la Universidad Carlos III (UC3M). Ha desarrollado su carrera profesional especializada en la ciberseguridad y las tendencias digitales, compatibilizándola con la docencia en universidades como el IE o la UC3M. Además, ha sido fundador de varias empresas de base tecnológica. En 2015 se unió a Deloitte, concretamente al área de Cyber de Risk Advisory. Actualmente, es gerente de ciberseguridad y lidera el área de CyberStrategy, Transformation and Assessment de Risk Advisory de Deloitte, en la que es responsable de proyectos como Planes Estratégicos y Directores de Seguridad, Sistemas de Gestión de Riesgos y perfilados de amenazas y modelos operativos, entre otros.

La figura del CISO, clave para la seguridad de la empresa y el éxito del negocio

La ciberseguridad se ha convertido en una de las mayores amenazas que afrontan las empresas actualmente. No se trata solo del fallo de la red o la "caída" de servidores. Por el contrario, en la actualidad nos estamos enfrentando a un fenómeno mucho más crítico que puede dañar la reputación de una gran empresa e impactar fuertemente en el negocio. Por estos motivos, las organizaciones han incluido políticas de ciberseguridad como un pilar básico en los comités de dirección. En este contexto, la figura del CISO va tomando cada vez mayor relevancia.

Años atrás, el director de Ciberseguridad cumplía con funciones más bien técnicas. Sin embargo, hoy en día debe además interactuar con todos los departamentos de la organización, en una relación que, según el estudio “Las preocupaciones del CISO”, realizado por el área de Cyber Strategy Transformation and Assessment de Risk Advisory de Deloitte, debe continuar avanzando, al igual que su posicionamiento en la estructura de las organizaciones.

En este sentido, la mayoría de los CISOs quiere reportar directamente a la dirección de su empresa, pero en más de la mitad de los casos reporta al CIO. Esto refleja una gran disparidad entre la relación directa actual y la deseada. Asimismo, el comité de dirección sigue estando fuera del alcance competencial de muchos CISOs. Y es que solo 1 de cada 5 empresas encuestadas dispone de un comité específico para dar respuesta a incidentes de ciberseguridad. Otro comité donde la presencia de CISO no está consolidada, es el comité de ries-

Enlaces de interés...

- Cybersecurity Summit
- El CISO es el perfil más cotizado en el sector Teleco, según Spring Professional
- Un 58% de los CISO están preocupados por la expansión sin control de cloud

La seguridad de la información no es un problema que excluya al negocio y permanezca limitada al ámbito tecnológico, sino que es un elemento que afecta a los riesgos de toda la organización.

gos. Resulta difícil entender como una organización puede integrar el ciberriesgo dentro del resto de riesgos de la organización si el CISO no está presente en dicho comité, como ocurre en casi el 40% de los casos. Lo cual es un dato sorprendente si se tiene en cuenta que los ciberincidentes son uno de los riesgos con mayor probabilidad hoy en día y de alto impacto para la organización.

La seguridad de la información no es un problema que excluya al negocio y permanezca limitada al ámbito tecnológico, sino que es un elemento que afecta a los riesgos de toda la organización. Por ello, llama la atención el número tan elevado de compañías que afirman no estar capacitadas para hacer frente a un ciberataque. Los resultados de la encuesta, en donde participaron más de medio centenar de compañías nacionales, indican que el 30% de las empresas considera que está poco preparada para hacer frente a un incidente de seguridad y solo el 42,86% que cree que lo está razonablemente.

Ante esta realidad, el CISO se ha convertido en una figura cada vez más solicitada dentro de las organizaciones y que ha pasado a tener un rol clave dentro de la empresa, en donde sus funciones han tomado un carácter estratégico y están siendo trascendentales para la medición del ciberriesgo y el éxito del negocio.

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 Canon EPSON EXCEED YOUR VISION hp

MARIO VELARDE BLEICHNER

GURÚ EN CYBERSEGURIDAD

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

CiberSeguridad,

la clave del Factor Humano (II): Pertenencia

En este segundo artículo de la serie CiberSeguridad, No sólo tecnología y capacitación técnica, voy a abordar un tema que tiene ver con otro de los elementos que pueden poner en riesgo la integridad de los sistemas de CiberSeguridad y que no provienen de elementos técnicos o de capacitación técnica del elemento humano de dichos sistemas.

En el anterior artículo mencionaba que el Factor Humano en la CiberSeguridad en su mayoría son millenials que llegan con nuevas visiones y/o modos de ver las relaciones laborales, no solo desde la visión tradicional de retribuciones adecuadas y derechos laborales ampliamente consolidados por generaciones anteriores, sino además temas tan debatidos como la conciliación laboral, que ya va avanzando, mayor conciencia ecológica, económica y social.

Llegan también otros elementos muy valorados por los millenials y en esta ocasión voy a tratar uno, la sensación de pertenencia, que además de ser una legítima aspiración de esta generación puede en el caso de no ser debidamente vigilada por los

departamentos de RRHH causa de posibles riesgos internos en un elemento tan importante en las empresas modernas, en gran parte ya digitalizadas, como es los sistemas de CiberSeguridad.

Los millenials cuando han llegado al mundo laboral, y en particular los que han llegado a la CiberSeguridad, se han encontrado con una estructura que en gran medida había sido externalizada, con un pequeño grupo interno que, además de su ocupación principal, la CiberSeguridad de la empresa para la que prestan sus servicios, y con otra tarea cada vez mayor que poco tiene que ver con su cometido prioritario y es la gestión de los externos, a quienes asignar tareas que inicialmente eran muy secundarias, pero que, con la intensificación de los procesos de externalización, han llegado en algunos casos al ridículo de que tareas críticas en los sistemas de CiberSeguridad pasaban a ser responsabilidad de externos.

Y todo esto se intensificó por un mal aplicado criterio de rentabilidad que podría ser justificado en procesos industriales (y no siempre) pero que en algo crítico en las empresas modernas con alto grado de digitalización, como es la CiberSeguridad, es al menos peligroso o en algunos casos podría llegar a ser suicida.

Algunas empresas de servicios que prestaban recursos humanos para la externalización evolucionaron hacia los servicios gestionados, aliviando en el camino este problema al incorporar en sus equipos humanos a externos haciéndoles partícipes de equipos en igualdad de condiciones con sus compañeros y aliviando la sensación de no pertenencia y los riesgos asociados con ello.

No tiene ningún sentido propugnar la desaparición de los externos y pensar que volver a modelos antiguos de gestión de RRHH con grados de externalización muy bajos como en el siglo pasado

Los departamentos de RRHH se enfrentan a un reto nuevo y muy interesante que amplía su ámbito de actuación en el caso de la CiberSeguridad a la totalidad de los equipos humanos

CÓMO UTILIZAR LA DARK WEB PARA LA INTELIGENCIA DE AMENAZAS

Ha habido una tendencia a etiquetar la web oscura como “cualquier sitio web no indexado por Google”, pero esta definición es demasiado amplia. Es mejor pensar en términos de actividad puramente ilegal. En este contexto, la red oscura consiste en unos pocos cientos (tal vez más) comunidades ilícitas, donde los miembros compran y venden de todo, desde herramientas personalizadas para ciberdelincuencia hasta datos robados, drogas, armas y más. No hay duda de que los investigadores pueden usar la web oscura para obtener inteligencia de amenazas muy valiosa, a menudo relevante para un amplio espectro de posibles objetivos, tanto organizaciones como individuos, a los que no se puede acceder a través de la monitorización convencional.

Enlaces de interés...

- Revista Digital Ciberseguridad, el factor humano (I)
- Récord inversiones ciberseguridad en 2018
- Revista Digital Tendencias ciberseguridad

es sensato, más aun cuando, con organizaciones como Agile, el movimiento de las personas en los equipos es constante, la duración en puestos con serias responsabilidades es de duración variable e incluso impredecible, la solidez de los equipos basado en el factor humano y que hacen que estos modelos sean más disruptivos con la implementación de ideas y procesos innovadores.

En este nuevo entorno, donde además los actores, millenials, tienen valores diferentes a las generaciones anteriores, los nuevos externos deben tener condiciones similares a los internos, y no solamente en aspectos salariales, sino además en todas aquellas ventajas sociales que solicita esta nueva generación que es la que tiene una responsabilidad más grande que las anteriores al tener que enfrentarse a amenazas de Seguridad mayores y más complejas.

Los departamentos de RRHH se enfrentan a un reto nuevo y muy interesante que amplía su ámbito de actuación en el caso de la CiberSeguridad a la totalidad de los equipos humanos encargados de esta área crítica en la empresa, independientemente del contrato laboral que tengan las personas que integran estos equipos.

Finalmente, y no por ello menos importante, los departamentos financieros de las empresas deberían incluir en sus cálculos de rentabilidad en la externalización de funciones el factor riesgo por la sensación de no pertenencia, al menos en el área de CiberSeguridad; reducir costes en esta área sin los debidos análisis puede poner en riesgo todos los elementos de la empresa y con el grado de Digitalización que se está alcanzando, es la empresa en su totalidad.

Otros elementos del Factor Humano en la CiberSeguridad no son menos por no haber sido tratados en este artículo, los tiempos y las tecnologías están cambiando que es una barbaridad y a una velocidad de vértigo, pero no olvidemos el Factor Humano, que sin ello nada tiene sentido, ni siquiera la Inteligencia Artificial.

¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el Centro de Recursos IT User

Tecnología para tu Empresa

Con la colaboración de:

CITRIX®

Wolters Kluwer