



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



it Digital Security



Director Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz,
Reyes Alonso, Javier San Juan

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación,
Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Juan Ramón Melara juanramon.melara@itdmgroup.es

Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

Arancha Asenjo arancha.asenjo@itdmgroup.es

Bárbara Madariaga barbara.madariaga@itdmgroup.es

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

¿Te avisamos del próximo IT Digital Security?

Bots, Amigos o enemigos?

Los bots, o pequeñas piezas de código que realizan tareas automáticas y repetitivas, han avanzado mucho y además están cada vez más presentes en nuestro día a día. Para muchos están empezando a dominar el mundo, y aunque quizá sea un poco exagerado, lo cierto es que, sin su bot, capaz de indexar miles de millones de páginas web, Google no sería lo que es, y quizá no serías capaz de reservar una habitación de hotel en la fecha y ciudad que necesitas, ni una mesa en el restaurante que te pilla más mano de dicho hotel.

Eso por la parte buena, porque como ocurre con la mayoría de las tecnologías, su uso puede caer de lado incorrecto o malicioso. De forma que esos pequeños robots que simulan ser un ser humano que está hablando contigo, también pueden unirse para lanzar un ataque de DDoS, puede desvirtuar las métricas como falsos followers o usuarios fantasmas, o incluso tener un impacto que haga que el machine learning no sea tan inteligente como parece. Saber qué es un bot, si las empresas son conscientes de su existencia, si saben detectar el tráfico que generan e incluso identificar qué bot es bueno y cuál está actuando de manera maliciosa es el tema de portada de este mes de julio.

Antes de entrar en el verano hemos vuelto a celebrar uno de nuestros #DesayunosITDS, en el que han participado expertos de Kaspersky Lab, Sophos Iberia, Trend Micro y Panda Security para debatir sobre el Ransomware y otras grandes amenazas, como el cryptojacking o la seguridad del correo electrónico.

Y también hemos querido despedir la primavera con otro de nuestros #ITWebinars, que bajo el título Seguridad y Cloud, ¿qué nos queda por aprender? reunió a expertos de Check Point, Kaspersky, Netskope, Akamai, Citrix, White-BearSolutions, Cisco e Infoblox. Saber lo que ocurre en la nube, dónde y cómo viajan los datos, quién accede a ellos y desde dónde, qué aplicaciones están utilizando tus empleados y cómo las están utilizando son algunas de las cuestiones que se resolvieron durante este maratón de seguridad cloud.

En lo que respecta a la actualidad, hemos dedicado parte de este número al evento Atmosphere EMEA de Aruba Networks, donde la compañía dejó claro que Orquestación y UEBA son claves para su negocio de Seguridad. También dedicamos unas páginas a la seguridad de los contenedores, una tecnología que, si bien facilita el despliegue de aplicaciones, impone una serie de retos desde el punto de vista de la seguridad. Y ahora que tanto se habla de cifrado y privacidad, nos hacemos eco del comunicado de IEEE en relación a su apoyo a favor de una encriptación fuerte para proteger la privacidad y la integridad de los datos y las comunicaciones.

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



Actualidad

Revista especial IT User

No solo IT

Índice de anunciantes



Ingecom

Trabajamos para Ti

Si te gusta la CiberSeguridad y quieres unirme a un equipo de profesionales de la misma, ponte en contacto con nosotros

www.ingecom.net

info@ingecom.net

MADRID C/ Infanta Mercedes, 90 - 8ª Planta - 28020 Madrid - Tel.: +34 91 571 51 96 Fax: +34 94 441 05 39

BILBAO C/ Máximo Aguirre, 18 Bis - 8ª Pl. - 48011 Bilbao (Bizkaia) - Tel.: +34 94 439 56 78 Fax: +34 94 441 05 39

LISBOA Edificio Infante, Avenida D. João II, 35, 11ªA - 1990-083 Lisboa - Tel.: +351 21 012 65 65





Orquestación y UEBA, claves del negocio de seguridad de Aruba

Seguras por diseño. Así son las redes de Aruba. Nos lo contaron Félix Martos y Pablo Collantes, director de canal seguridad -el único de europa, y director de canal de Aruba respectivamente. Nos lo contaron en Sibenik, localidad croata en la que Aruba ha celebrado este año su evento Aruba Atmosphere EMEA, y en la que reunió varios cientos de partners y clientes que durante varios días pudieron ver en detalle algunos productos y hablar con grandes ejecutivos, incluido Keerti Melkote, uno de los fundadores de la empresa.

Entre los cientos de asistentes al Aruba Atmosphere EMEA Pablo Collantes y Félix Martos, que nos contaron que la seguridad forma parte de los inicios de Aruba, un fabricante con 16 años de vida. Aruba se hace famosa como fabricante de redes inalámbricas, pero es la primera que tiene un

firewall integrado dentro de la propia controladora, así como un sistema de prevención y detección de intrusiones, nos explica Félix Martos.

Empezar vendiendo redes securizadas por diseño les valió adentrarse en el mundo de la banca, o ser los proveedores de red inalámbrica de las fuerzas aéreas americanas o todos los hospitales navales

Compartir en RRSS



Aruba SD-Branch

Celebrado a primeros de junio en Croacia, el Aruba Atmosphere contó con pocos anuncios de novedades, que se reservaron para el HPE Discover, el evento que, a mediados del mismo mes se celebraba en Las Vegas.

Entre las grandes novedades Aruba SD Branch, una nueva oferta que integra WAN, LAN, WiFi y Seguridad para las Sucursales Definidas por Software. El nuevo producto está diseñado para que los responsables de sucursales puedan gestionar redes y seguridad a medida que adoptan arquitecturas de nubes múltiples



del mundo -incluido el de Rota. “Desde el principio Aruba y la Seguridad van intrínsecamente unidas”, asegura Félix Martos, añadiendo que el controlador de Aruba es también un terminador de túneles VPN; “los puntos de acceso remoto establecen conexiones seguras con el controlador y encapsulan. De forma que la arquitectura distribuida de Aruba es

¿Te avisamos del próximo IT Digital Security?

y supervisan un número creciente de dispositivos móviles e IoT. La idea que hay detrás de la propuesta es imponer cierta disciplina de seguridad sin incrementar la dificultad desde el punto de vista de la red.

La arquitectura Aruba SD-Branch integra los nuevos gateways de la serie 7000 para proporcionar un único punto para la política de redes SD-WAN, cableadas e inalámbricas y la aplicación de la seguridad. Las capacidades de tener en cuenta el contexto están incorporadas en los nuevos controladores además de otras características como el enrutamiento basado en políticas.

Esto significa que los gateways pueden usar esta información contextual para dirigir el tráfico de manera dinámica a través de la WAN según el usuario, dispositivo o grupo de afiliación.

Para la administración de políticas la solución SD-Branch cuenta con la plataforma cloud Aruba Central ofreciendo una gestión de la seguridad y conectividad capaces de escalar de forma sencilla. El producto de control de acceso a la red de Aruba, ClearPass, automatiza la administración de políticas en diferentes capas de acceso a redes y aplicaciones.

intrínsecamente segura porque siempre va a través de túneles seguros”.

Lo llamativo es que la seguridad añadida llega como consecuencia de la propia inseguridad de la red inalámbrica. Es decir, es una onda que viaja por el aire, que cualquiera puede monitorizar, una comunicación abierta y son precisamente estas caracte-

terísticas las que llevan a Aruba a convertir la seguridad en una obsesión, a “intentar que el aire sea como mínimo tan seguro como el cable, y a lo que se llega es que el aire termina siendo más seguro que el propio cable”, reflexiona Martos.

El futuro pasa por Orquestación y UEBA, por IntroSpect y ClearPass. El primero es el cerebro y el segundo el brazo armado, el ejecutor de políticas

De forma que en Aruba el negocio de seguridad es una evolución del propio negocio de red. La explosión de las redes inalámbricas se produce en 2008 “gracias al iPad”, dice Pablo Collantes. Gracias en realidad a todo el mercado de tabletas y de ultrabooks, muchos de los cuales no incorporan puerto ethernet. Es decir, que el número de dispositivos móviles crece, el puerto ethernet desaparece... “y la red primaria pivota a la red inalámbrica”. Y ahí, justo con la explosión de dispositivos, lo que aparece es la necesidad de securizar esos dispositivos”. Es el momento de crecer y Aruba cuenta con ClearPass, el NAC (sistema de control de acceso a la red) de la compañía.

ClearPass es, en opinión de Félix Martos, “un NAC en el sentido más amplio del término. Em-



pezamos securizando el acceso de invitados con AmigoPod en su momento y luego con ClearPass Guest; el siguiente paso fue securizar el acceso a las redes empresariales introduciendo seguridad dentro de los dispositivos, dentro de los PCs, con ClearPass Onboard, y el ClearPass OnGuard, que sería el agente que va en el PC y verifica que tiene actualizaciones de seguridad que tiene antivirus...". Y este es el primer gran salto al mundo de la seguridad fuera de la red inalámbrica que da Aruba, porque ClearPass se aplica también a los puertos de red.

Al final todo pivota hacia lo inalámbrico, incluida la misma concepción de los puertos de red, un concepto bautizado como Colorless, que consiste en dejar de preocuparse por dichos puertos "porque cuando conectas algo a la red se identifica qué es lo que se conecta a la red, qué dispositivos es, a

quién pertenece, si ha sido provisionado antes o no..., y en función de eso se le aplica una política de seguridad al puerto". Es decir que los switches no están configurados previamente, sino que se configuran de forma dinámica cuando se conecten a ese puerto.

El de la seguridad es un mercado muy fragmentado en el que la consolidación avanza despacio. Le preguntamos a los ejecutivos de Aruba cuán cómodos se sienten es este mercado, sobre todo comparado con el de redes, y teniendo en cuenta que son cada vez más los fabricantes de seguridad que se animan a adentrarse en el mundo de las red Wifi, como puede ser un WatchGuard, un Fortinet o un Sophos. "Nos da mucha satisfacción porque es lo que estamos haciendo desde el inicio y que los demás lo estén siguiendo confirma que nuestra estrategia era la buena".

¿Te avisamos del próximo IT Digital Security?



INFORME GLOBAL DE SEGURIDAD DE APLICACIONES Y REDES DE RADWARE

A lo largo de 2017, los principales titulares destacaron los ciberataques y las amenazas de seguridad que incluyeron una posible interferencia en las elecciones presidenciales de EE. UU., brotes de malware en todo el mundo y la brecha de seguridad de Equifax. Estos y otros eventos de alto perfil estimularon una mayor inversión en ciberdefensa por parte de todos, desde estados nación y corporaciones globales hasta individuos que compran soluciones antimulware para dispositivos personales.





Pablo Collantes, director de canal de HPE Aruba Iberia

En Aruba el negocio de seguridad es una evolución del propio negocio de red, de intentar que el aire sea como mínimo tan seguro como el cable

ClearPass es el motor que va a securizar la red inalámbrica, la red cableada, la VPN, es un overlay que puede ir con lo que sea. Nace en 2012 para facilitar a los departamentos de TI la gestión de los dispositivos móviles, permitiéndoles acceder de manera segura a cualquier red empresarial. Y su evolución no ha hecho más que empezar. ¿Cuál es el porcentaje del negocio de seguridad? “Estamos empezando y ya representa el 10%” ¿El objetivo? “El infinito, porque hay mucho recorrido”, dice Collantes, explicando que ClearPass no sólo habla con la infraestructura de red de Aruba, sino con soluciones de otros fabricantes, incluidos un SIEM, un firewall, un MDM... capaz además de interrelacionar y pasar información entre ellos. Es decir, un orquestador, un elemento cada vez más importante porque un elemento de la red que siempre han sido silos.

Explica Martos que el MDM era un silo, los firewalls otros... y que las API y los estándares han sido muy beneficiosos para el mercado. Por cierto, que “en nuestro caso siempre hemos estado definiendo los estándares. En casi todos los estándares de WiFi ha participado alguien de Aruba y utilizándolos de forma amplia”.

No se para Aruba en orquestar toda la información, sino que da un paso más para analizarla, añadiendo al análisis el comportamiento de los diferentes individuos y de las cosas. ¿Es decir que el futuro pasa por Orquestación y UEBA? “Si, y para nosotros es IntroSpect y ClearPass. El primero es el cerebro y el segundo el brazo armado, el ejecutor de políticas”. Se van identificando posibles riesgos de seguridad en función de los cuales ClearPass

decide desviar el tráfico de un usuario, pedirle que se instale un agente, si se detecta una exfiltración se habilita una red especial para controlarlo, etc”.

IntroSpect es el resultado de la compra de Niara, un experto en tecnologías UEBA (user and entity behavioral), que analizan la conducta de entidades y usuarios para la detección de amenazas de seguridad. La compra se realizó a primeros de 2017 y ya desde el principio se habló de combinar la solución de Niara con Aruba ClearPass con el objetivo de llevar al mercado “el sistema de detección de ataques y visibilidad más completo”, dijo la compañía en su momento. Tan sólo unos meses después, en septiembre del año pasado Aruba anunciaba el lanzamiento de Aruba 360 Secure Fabric, un marco analítico para la detección y respuesta de ataques; el software ya combinaba machine learning con productos existentes y la tecnología de Niara. El paquete se ampliaba para incluir una versión básica



Aruba preparada para el IoT: los puntos de acceso securizan las conexiones del IoT, ClearPass identifica todos los dispositivos que hay en la red, e Instrospect los analiza y ve si están haciendo algo que no deben

de Aruba IntroSpect y un producto de análisis del comportamiento de la entidad, que utiliza detección de comportamiento basada para detectar cambios en el comportamiento del usuario que pueden indicar ataques internos.

Empresa española y seguridad

Lo fácil o difícil de hacer negocio es que los clientes estén por la labor. Si bien es cierto que después de cada gran incidente de seguridad aumenta la concienciación y se cierran algunos acuerdos, también lo es que se tiene mala memoria, que los incidentes quedan pronto olvidados.

La empresa española, ¿está concienciada en cuanto a la seguridad? Que entre 2012 y 2018 la

facturación del negocio de seguridad de Aruba se haya multiplicado por diez es una buena noticia. Concreta Pablo Collantes que “antes de la compra de HP ya llevábamos un 5x, y luego hemos seguido creciendo. Desde la compra de HP en 2015 se ha crecido un 50%”.

Sobre el IoT dicen que es como todo, que primero es hablar y hablar para después empezar a hacer negocio, y si algo aportará el Internet de las cosas es negocio inalámbrico que deberá tener cierto grado de seguridad; “con el BYOD pasó lo mismo. Hace dos años sólo se hablaba de eso, pero proyectos había pocos, pero ahora hay muchos más proyectos y ya no se habla de ello”, dice Félix Martos.


Aruba ya está preparada para ello; “nuestros puntos de acceso securizan las conexiones del IoT, nuestro ClearPass identifica todos los dispositivos que hay en la red, e Instrospect los analiza y ve si están haciendo algo que no deben. Si una webcam lo que debe de tener es tráfico HTTP y lo que tiene res trafico FTP es un problema y puede indicar un fallo masivo de seguridad. Ya se han utilizado cámaras para lanzar ataque DDoS, por ejemplo. De lo que se trata es de que la red a la que se conecten

sea segura, que se securicen los dispositivos que se conectan a la red; y es fundamental que haya un elemento que sea lo suficientemente inteligente como para monitorizar esos 50.000 millones de dispositivos IoT”, explica el responsable de canal de seguridad de Aruba Iberia.

Monitorizar 50.000 millones de dispositivos... “no hay ser humano que haga eso. Eso lo hacen muy



Félix Martos, Channel Security Manager para HPE Aruba Iberia.

bien las máquinas”, añade Martos. La gran ventaja es que Aruba ya cuenta con su orquestador y cuando se incorporen nuevos dispositivos “seguiremos haciendo lo mismo. Lo único que tenemos que saber es que la red va a crecer y poner los medios para que se gestione lo mejor posible”. 

Enlaces de interés...

- [Atmosphere 2018 EMEA](#)
- [HPE Aruba trae a España sus soluciones de análisis de comportamiento de red](#)

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.



Inteligencia de amenazas líder del sector



Las claves de la seguridad de los contenedores

Los contenedores se expanden porque permiten empaquetar una aplicación y todo lo que esta necesita en una sola imagen, facilitando la coherencia entre entornos y múltiples objetivos de implementación, como servidores físicos, máquinas virtuales (VM) y nubes privadas o públicas. Pero aplicar la capa de seguridad es un reto para el que deben tenerse en cuenta varias áreas, desde el propio sistema operativo a la seguridad de la capa de orquestación o el entorno de desarrollo.



Una de las características del mercado de TI es lo rápido que ocurren las cosas. Lo rápido que se suceden las tecnologías, lo rápido que evolucionan y la tecnología de contenedores no es ajena a ello. Empecemos por el principio, por definir lo que es un contenedor, que no es otra cosa que el último grado de virtualización, una forma de encapsular una aplicación en su propio espacio aislado. Una vez que la aplicación esté en su contenedor, no tendrá

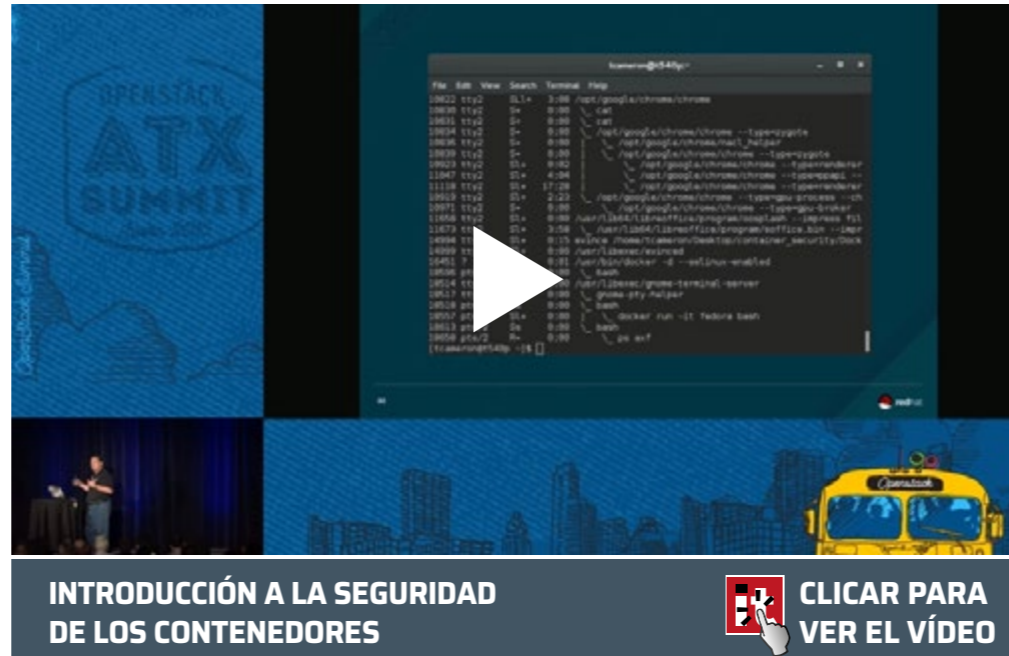
conocimiento de otras aplicaciones o procesos que existan fuera de su espacio. Todo lo que necesita la aplicación para ejecutarse correctamente también se encuentra dentro de este contenedor.

Buceando en Internet se puede averiguar casi de todo, como la historia de los contenedores, que comienza en los años 2000. En 2001, la tecnología de contenedores llegó al mundo Linux a través de Jacques Gelinas y el proyecto VServer, que permitió "ejecutar varios servidores Linux de propósito

Compartir en RRSS



general en una sola caja con un alto grado de independencia y seguridad”, según decía el propio proyecto. De forma que la solución Linux-VServer fue el primer esfuerzo en Linux para “separar el entorno de espacio de usuario en distintas unidades (Servidores privados virtuales-VPS) de tal manera que cada VPS se ve y se siente como un servidor real para los procesos contenidos dentro”. Google se adentró en el negocio de contenedores en 2006 con sus Process Containers que un año después renombró como Control Groups y se agregaron al kernel de Linux. A lo largo de la década de 2010, aparecieron algunas empresas de contenedores, pero su popularidad no comenzó hasta la llegada de Docker en 2013.

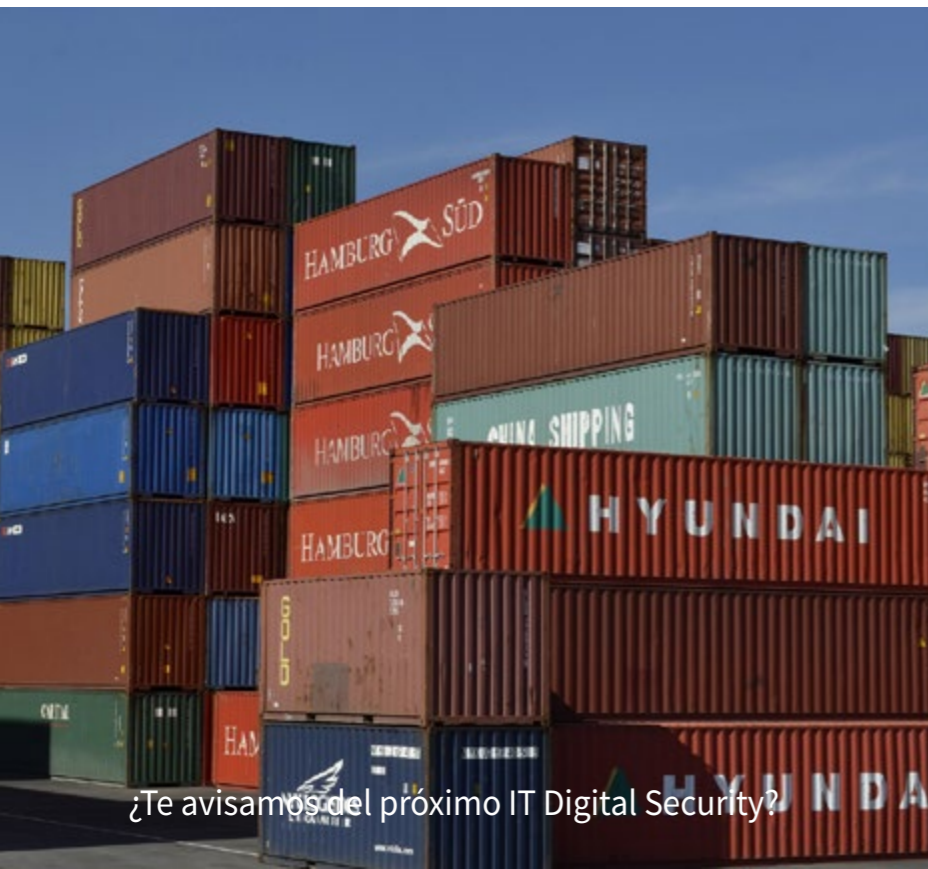


La creciente adopción de aplicaciones basadas en contenedores llevó a que los sistemas se vuelvan más complejos y aumentaran los riesgos, ha-

objetivo es construir contenedores seguros desde cero sin reducir el tiempo de comercialización.

Qué opinan los responsables de TI
Actualmente, y según un estudio de EGS, los contenedores son responsables del 19% de las cargas de producción de cloud híbrida, porcentaje que en dos años se convertirá en un tercio de dichas cargas. Además, un estudio de Global Market Insight asegura que el mercado de contenedores superará los 2.400 millones de dólares para 2024 en la región de EMEA.

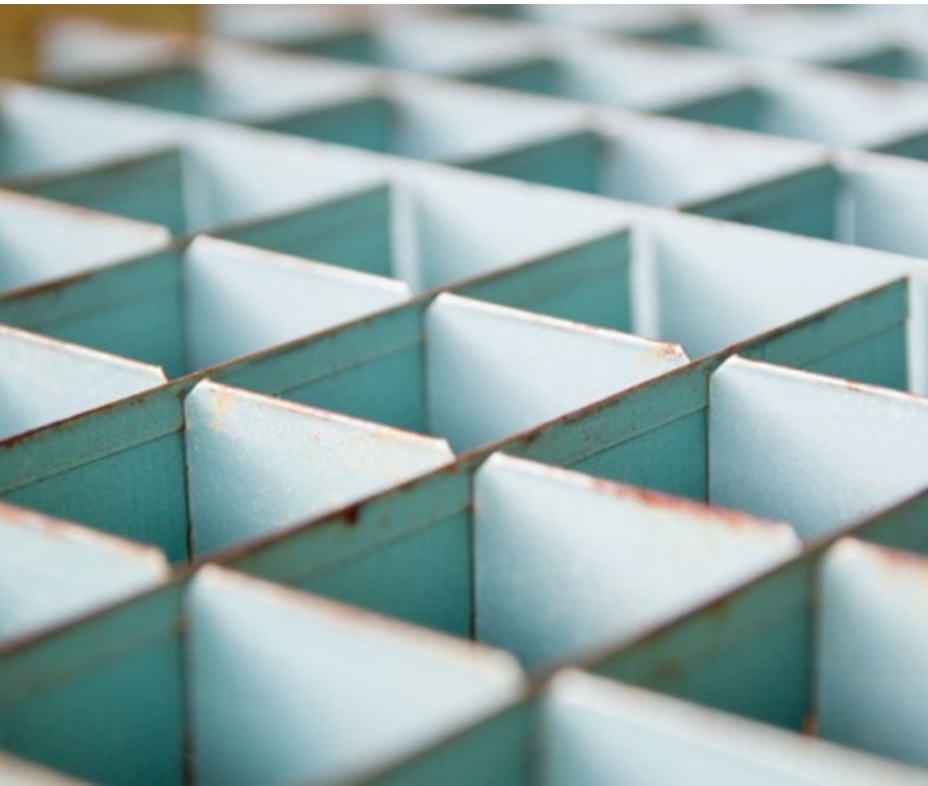
Con estos datos en mente y advirtiendo del rápido crecimiento y proliferación de los contenedores de aplicaciones, los profesionales de ciberseguridad



Bajo la premisa de entender mejor qué amenazas deben abordarse y qué áreas afectan más a los contenedores Adrian Lane, analista y CTO de Securosis, enumera cinco puntos de peligro

ciendo que la seguridad de los contenedores cobrara protagonismo. Vulnerabilidades como Dirty Cow despertaron las conciencias y a un cambio en la seguridad a lo largo del ciclo de vida del desarrollo de software, convirtiéndolo en una parte clave de cada etapa en el desarrollo de aplicaciones de contenedores, también conocido como DevSecOps. El

aseguran que se han generado varios problemas de seguridad. Entre otras cosas, un 35% dice que las soluciones de seguridad para las cargas de trabajo en el servidor no admiten la misma funcionalidad para los contenedores, lo que requiere del uso de tecnologías de seguridad de contenedor separadas, lo que agrega costes y complejidad



para salvaguardar los activos de TI; otro 34% está preocupado porque las imágenes almacenadas en los registros del contenedor coincidan con los requerimientos de seguridad y cumplimiento de la organización.

Un dato en el que coincide un tercio de los encuestados es sobre la falta de soluciones de seguridad maduras para la seguridad de los contenedores. Al respecto señalarla cobertura de empresas de seguridad asentadas, como Trend Micro o VMware.

Además, para un 27% la portabilidad hace que los contenedores sean más susceptibles a los compromisos de “in motion”. Un riesgo cuando no se cuentan con herramientas capaces de monitorizar los contenedores y microservicios en tránsito a medida que aparecen y desaparecen.

Áreas de peligro

Pequeños y algo volátiles, dos características de los contenedores, hacen que el vector de ataque que pueda comprometerlos sea reducido. [Dice Gartner](#) sobre ellos que los contenedores “no son inherentemente inseguros, pero que están siendo desplegados de manera insegura por los desarrolladores”. Teniendo en cuenta que los contenedores comparten el sistema operativo, un ataque o una vulnerabilidad en el SO que los aloja puede comprometerlos a todos; “las redes tradicionales y las soluciones de seguridad basadas en host son ciegos a los contenedores”, dice la consultora, añadiendo que las soluciones de seguridad de los contenedores deben proteger todo el ciclo de vida de los mismos, desde la creación a la producción, y que la mayoría ofrecen además escaneo de preproducción combinado con monitorización y protección en tiempo de ejecución.

Bajo la premisa de entender mejor qué amenazas deben abordarse y qué áreas afectan más a los contenedores Adrian Lane, analista y CTO de Securosis, enumera cinco puntos de peligro generales dentro de un entorno de contenedor que son vulnerables a los ataques. “Algunas amenazas y problemas son bien conocidos, algunos son puramente pruebas de concepto de laboratorio, y otros son vectores de amenazas que los atacantes aún no han explotado”, [dice el experto](#).

■ Amenazas para el entorno de construcción

Asegura Adrian Lane que la primera área que necesita protección es el entorno de desarrollo “porque es la menos segura y donde más fácil es



LAS DIEZ CAPAS DE SEGURIDAD DE LOS CONTENEDORES



Los contenedores tienen un gran atractivo porque permiten a los usuarios empaquetar fácilmente una aplicación, y todas sus dependencias, en una sola imagen que puede promocionarse desde el desarrollo, la prueba y la producción, sin cambios. Los contenedores facilitan la coherencia entre entornos y múltiples objetivos de implementación, como servidores físicos, máquinas virtuales (VM) y nubes privadas o públicas. Esto ayuda a los equipos a desarrollar y administrar con mayor facilidad las aplicaciones que brindan valor comercial.

Las empresas requieren una seguridad sólida y cualquiera que ejecute servicios esenciales en contenedores preguntará: “¿Están seguros los contenedores?” Y “¿Podemos confiar en los contenedores con nuestras aplicaciones?” Este documento describe 10 elementos clave de seguridad para diferentes capas de la pila de soluciones de contenedores y diferentes etapas del ciclo de vida del contenedor.





Dentro de los contenedores no se pueden insertar identidades y control de acceso ni administrar certificados en instancias variables

insertar código malicioso”. Hay toda una industria dedicada a testearla gestión y petición de datos porque los desarrolladores tienden a obviar la seguridad, dice el experto, enumerando algunas de las amenazas que pueden producirse en esta área: cambios en el código fuente, modificaciones maliciosas o erróneas en los controladores de compilación automatizados, Scripts de configuración con errores o que exponen credenciales, la incorporación de bibliotecas inseguras o versiones de versiones anteriores / inseguras del código existente.

■ **Contenido y carga de trabajo del contenedor**

Cuando se trabaja con contenedores es habitual preguntarse qué hay en el contenedor, qué hace e incluso qué versión. A menudo los responsables de operaciones no saben si los desarrolladores han incluido herramientas como ssh en un conte-

nedor o pueden alterar su contenido. Y todo esto es un problema cuando se trata de mapear los derechos de acceso al sistema operativo y los recursos de host por un contenedor. Las personas de seguridad generalmente desconocen qué tipo de refuerzo se ha realizado, en caso de haberse hecho.

■ **Conducta Runtime**

Existe la preocupación de que un contenedor ataque o infecte otro contenedor; que un contenedor pueda estar exfiltrando datos o tenga una conducta sospechosa. “Hemos visto ataques para extraer código fuente, y otros para añadir nuevas imágenes a los registros, y en ambos casos las plataformas no estaban protegidas por una gestión de accesos e identidades”, dice Adrian Lane, añadiendo que las organizaciones deben confirmar que el acceso al cliente de

Docker está suficientemente controlado a través de los controles de acceso para limitar quién controla el entorno de tiempo de ejecución. Otras preocupaciones a tener en cuenta es que los contenedores se ejecuten durante mucho tiempo, sin rotación a las versiones más nuevas parcheadas, que la red se haya configurado correctamente para limitar el daño de compromiso y que los atacantes estén probando contenedores, buscando vulnerabilidades.

■ **Seguridad del sistema operativo**

La seguridad del sistema operativo subyacente es una preocupación. La pregunta clave es si está configurado correctamente para restringir el acceso de cada contenedor al subconjunto de recursos que necesita, y para bloquear de manera efectiva todo lo demás. A los responsables de TI les preocupa que el motor del contenedor

Según Gartner, los contenedores no son inherentemente inseguros, pero están siendo desplegados de manera insegura por los desarrolladores

no proteja suficientemente el sistema operativo subyacente, dice el CTO de Securosis. Y es que, si un ataque en la plataforma de host tiene éxito, poco se puede hacer para ese grupo de contenedores, y además podría dar acceso suficiente al código malicioso para pivotar y atacar a otros sistemas.

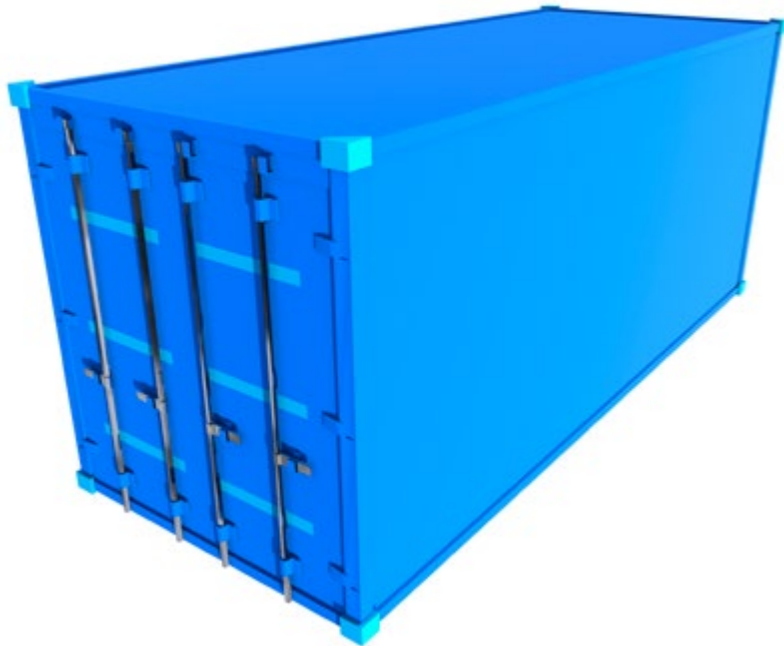
■ **Seguridad para el administrador de orquestación**

“A medida que los contenedores se han convertido en una unidad de entrega de aplicaciones, las organizaciones han comenzado a sentir que entienden los contenedores y la atención se ha desplazado a la administración de contenedores. La atención y la innovación han cambiado para centrarse en la orquestación de clusters, con Kubernetes como el niño mimado para optimizar el valor y el uso de contenedores”, dice Adrian Lane, añadiendo que al igual que muchos productos de software, el enfoque de las herramientas de orquestación es la escalabilidad y la facilidad de administración, no la seguridad. De forma que las herramientas de orquestación brindan un nuevo conjunto de problemas de seguridad y vulnerabilidades.

Confusión en torno a los contenedores

Habla Lori MacVittie, Principal Technical Evangelist de F5 Networks, de la confusión en torno a los contenedores. “Las arquitecturas de entrega tradicionales no funcionan dentro del entorno de contenedores. La comunicación es errática, dinámica e impredecible. Las comunicaciones se multiplican y el entorno es altamente volátil. Lo que aparece ahora no es lo que se verá en dos minutos, y mucho menos en diez”, dice la ejecutiva, para terminar asegurando que una arquitectura de dos niveles proporciona la fiabilidad y la seguridad necesarias al tiempo que admite la velocidad y la escala que exigen las aplicaciones en contenedores.

Dice también MacVittie no se pueden insertar identidades y control de acceso en el interior ni administrar certificados en instancias variables. “Utilizar terminaciones SSL en la aplicación se convierte en una pesadilla... Incluso la seguridad de la aplicación, como la defensa de bot o las protecciones contempladas en el OWASP Top Ten, se vuelven problemáticas”, explica la experta de F5 Networks. Afortunadamente las aplicaciones implementadas como varios microservicios dentro de un entorno de



Un 34% de responsables de TI está preocupado porque las imágenes almacenadas en los registros del contenedor coincidan con los requerimientos de seguridad y cumplimiento de la organización

contenedor siguen siendo aplicaciones (incluso API) y tienen un punto final “específico de la aplicación” que brinda la oportunidad de establecer una ruta segura de entrada sin perder el entorno del contenedor. Esto permite una arquitectura de red bifurcada basada en los principios tradicionales de estabilidad y escala, explica Lori MacVittie, al tiempo que adopta enfoques modernos de escalas basadas en software para contenedores.

Esta arquitectura de dos niveles es lo que permite un punto final confiable y seguro a través del cual se puede pasar de la ruta troncal norte-sur a las rutas este-oeste dentro de un entorno de contenedor. De forma que una arquitectura de dos niveles “limita el caos de los contenedores, mantiene la cordura y aísla la infraestructura compartida de la entropía inherente a las aplicaciones en contenedores”.

¿Te avisamos del próximo IT Digital Security?

Finalmente [explica en su post](#) que el punto de ingreso puede administrar las políticas específicas de la aplicación (rendimiento y algo de seguridad) mientras que el resto de la red entrante segura maneja el resto. “Esto hace que la inclusión de contenedores en entornos de producción que ofrecen aplicaciones heredadas sea un proceso más suave y menos doloroso, ya que es lo menos disruptivo posible”.

Soluciones

Como decíamos al comienzo existen soluciones de seguridad para contenedores de empresas de seguridad tradicionales, como la anunciada recientemente por Trend Micro: Deep Security Smart Check, un componente que ofrece análisis continuo de imágenes de contenedores para complementar la protección existente que aporta Deep Security al tiempo de ejecución del contenedor.

Según Trend Micro, Deep Security Smart Check escanea las imágenes del contenedor antes de que se lleve a cabo el despliegue. Con esta solución los problemas de seguridad se resuelven en el ciclo de

desarrollo y no después del lanzamiento de la aplicación.

Además, Trend Micro lanzaba un nuevo y amplio conjunto de API y un centro de automatización con recursos para ayudar a permitir la automatización de la seguridad a través de mejores integraciones. Los clientes de Trend Micro Deep Security utilizan las API de producto para permitir la entrega continua, la monitorización del estado, la gestión de servicios de TI y la integración de herramientas de





orquestración, como el recién lanzado Amazon Elastic Container Service for Kubernetes.


Del lado de VMWare, la compañía, que ha jugado un papel fundamental en ayudar a transformar el centro de datos gracias a la virtualización, lanzó hace unos años NSX, su plataforma para la virtualización de la red con la que se pueden crear servicios de red como balanceo de cargas, firewall,

routing, etc. La familia NSX tiene dos productos, NSX for vSphere, o NSX-V, que lleva cuatro años en el mercado y está muy ligado a la infraestructura vSphere y VMware.

La compañía cuenta también con NSX-T, una plataforma de red única que se implementa en software para conectar cualquier tipo de aplicación. Podría ser una máquina virtual, contenedores o bare-me-

Enlaces de interés...

- I [Trend Micro extiende su solución de seguridad para contenedores](#)
- I [Los contenedores no están preparados para proteger las aplicaciones mágicamente](#)
- W [Las diez capas de seguridad de los contenedores](#)
- W [El cloud híbrido cambia las reglas de la seguridad](#)

tal. NSX-T hace que sea más fácil administrar contenedores a escala e integrarlos con otros servicios de red, como firewalls y balanceadores de carga. El gestor de reglas de aplicaciones proporciona una visibilidad única de la actividad, desde el sistema operativo hasta los flujos de red, lo que facilita la actualización automática de políticas y reglas, y mejora la microsegmentación. 

Un 35% de los responsables de TI dicen que las soluciones de seguridad para las cargas de trabajo en el servidor no admiten la misma funcionalidad para los contenedores

Trabajamos para hacer de la tecnología un bien más accesible, democratizando su uso

Soluciones globales para la seguridad del dato esté donde esté


WBSAirback

Storage &
Backup
Appliance

**WBSVision &
SmartLogin**

Identity and
Access
Management
Appliance

Tecnología basada en open source y estándares



IEEE se posiciona a favor del cifrado y contra las puertas traseras

En oposición a los esfuerzos de algunos gobiernos que exigen puertas traseras, o backdoors, el Institute of Electrical and Electronics Engineers, o IEEE, ha publicado una declaración en apoyo para un cifrado fuerte.

El Institute of Electrical and Electronics Engineers (IEEE), la organización profesional técnica más grande del mundo dedicada al avance de la tecnología ha sumado su voz a los expertos de seguridad, abogados y otros grupos que están en contra de la idea de establecer puertas traseras.

Dice la organización que, comprometida con el desarrollo de la confianza en las tecnologías a través de la transparencia, la creación de comunidades técnicas y asociaciones en todo el mundo, IEEE respalda el uso de encriptación fuerte para proteger la privacidad y la integridad de los datos y las comunicaciones.



HACIENDO FÁCIL EL CIFRADO Y LA ROTACIÓN DE CLAVES



El cifrado de datos es fundamental para la seguridad de las empresas modernas. Y una buena práctica relacionada con el cifrado es el llamado rekeying, que no es otra cosa que la rotación

de las claves de cifrado de forma periódica y que evita, entre otras cosas, reduce el riesgo de que alguien use una clave antigua para acceder a los sistemas. Teniendo en cuenta que el rekeying es tan importante, surgen algunas preguntas que este Whitepaper analiza: ¿cuáles son las mejores prácticas de rekeying?, ¿Por qué las organizaciones no rotan las claves de cifrado de manera consistente?, ¿Por qué es el proceso tan difícil?



A continuación, parte de la declaración, a la que puede accederse desde este enlace.

IEEE APOYA EL USO DE CIFRADO FUERTE SIN RESTRICCIONES PARA PROTEGER LA CONFIDENCIALIDAD E INTEGRIDAD DE LOS DATOS Y LAS COMUNICACIONES. NOS OPONEMOS A LOS ESFUERZOS DE LOS GOBIERNOS PARA RESTRINGIR EL USO DE CIFRADO FUERTE Y/O PARA EXIGIR MECANISMOS DE ACCESO EXCEPCIONALES TALES COMO “PUERTAS TRASERAS” O “ESQUEMAS DE CUSTODIA DE CLAVES” PARA FACILITAR EL ACCESO DEL GOBIERNO A DATOS CIFRADOS. LOS GOBIERNOS TIENEN INTERESES LEGÍTIMOS EN EL CUMPLIMIENTO DE LA LEY Y LA SEGURIDAD NACIONAL. IEEE CREE QUE ORDENAR LA CREACIÓN INTENCIONAL DE PUERTAS TRASERAS O ESQUEMAS

El cifrado es una herramienta esencial para garantizar la privacidad y la integridad de los datos y sistemas

DE DEPÓSITO EN GARANTÍA, SIN IMPORTAR CUÁN BIEN INTENCIONADAS SEAN, NO RESPONDE BIEN A ESOS INTERESES Y CONDUCIRÁ A LA CREACIÓN DE VULNERABILIDADES QUE PRODUCIRÍAN EFECTOS IMPREVISTOS Y ALGUNAS CONSECUENCIAS NEGATIVAS PREDECIBLES”.

El chip Clipper, o déjame entrar

Anunciado en 1993, el proyecto del chip Clipper sólo vivió tres años. Fue desarrollado y promocionado por la NSA, la Agencia Nacional de Seguridad de Estados Unidos, como un dispositivo de cifrado que aseguraba los mensajes de voz y de datos. Incorporaba de serie una puerta trasera y el objetivo era que fuera adoptado por las empresas de telecomunicaciones para la retransmisión de voz.

Capaz de cifrar y descifrar mensajes, Clipper fue parte del programa de la Administración Clinton para “permitir a los agentes del orden público federal, estatal y local decodificar las transmisiones interceptadas de voz y datos”.

Cada chip Clipper tenía un número de serie único y secreto, y utilizaba un algoritmo de cifrado de datos llama-

do Skipjack para transmitir información, y el algoritmo de intercambio de claves Diffie-Hellman para distribuir las cryptokeys entre los pares.

Skipjack fue inventado por la Agencia de Seguridad Nacional del gobierno de los Estados Unidos; este algoritmo se clasificó inicialmente como Secreto, lo que evitó que fuera sometido a una revisión por parte de la comunidad de investigación de cifrado. La información que proporcionó el gobierno fue que utilizaba una clave de 80 bits, que el algoritmo era simétrico y que era similar al algoritmo DES.

Finalmente, según recoge Wikipedia, el chip no fue adoptado ni por consumidores ni por fabricantes y dejó de ser relevante en 1996.

Algunos gobiernos buscan establecer puertas traseras en los productos tecnológicos para revisar la información privada cifrada de empresas y usuarios

Para James Jefferies, presidente y CEO de IEEE, el cifrado fuerte de la información electrónica “es una herramienta esencial para garantizar la privacidad y la integridad de nuestros datos y sistemas”.

Hace un tiempo que en Estados Unidos se intenta forzar el establecimiento de puertas traseras en los productos tecnológicos, lo que permitiría a las enti-

dades gubernamentales, revisar la información privada cifrada de empresas y usuarios. Recordemos el chip Clipper, un intento del gobierno americano por desplegar un sistema de cifrado que incluía de forma explícita una puerta trasera para dar acceso a las fuerzas del orden y la seguridad nacional. El chip no tuvo éxito.



Aseguraba hace unos meses The Register que dos años después de que su esfuerzo por introducir una nueva legislación muriera, la senadora Diane Feinstein (D-CA) inició un nuevo esfuerzo para hacer posible que las fuerzas de seguridad puedan acceder a cualquier información enviada o almacenada electrónicamente. En todo caso, los expertos en criptografía siguen advirtiendo que una puerta trasera de este tipo podría ser explotada por malhechores expertos para que también lean los archivos y las comunicaciones de las personas.

El fiscal del distrito de Nueva York y defensor del establecimiento de las puertas traseras, Cyrus Vance (D-NY), también está a favor de una nueva legislación. Lleva varios años argumentando a favor de las leyes en contra del cifrado, sobre el que ha dicho que es la inhabilidad para rastrear a través de las comunicaciones personales de las personas, lo que hacía su trabajo más difícil.

Qué es un Backdoor

Un backdoor, o puerta trasera, es un método, a menudo secreto, de superar la autenticación o cifrado normal de un sistema, producto o dispositivos, para acceder de forma remota a los mismos. En términos de funcionalidad, las “puertas traseras” son similares a muchos sistemas de administración diseñados y distribuidos por desarrolladores de programas legítimos.

Enlaces de interés...

- ▮ [Declaración IEEE: In Support of Strong Encryption](#)
- ▮ [Comunicado de La casa Blanca sobre el chip Clipper](#)
- ▮ [Tres arcaicos Backdoors que sigue estando de plena actualidad](#)
- ▮ [Listado de Backdoors y cómo eliminarlos](#)
- ▮ [Backdoors vs troyanos](#)

Skipjack fue un algoritmo de cifrado inventado por la Agencia de Seguridad Nacional del gobierno de los Estados Unidos

Compartir en RRSS



SOPHOS

INTERCEPT

VER EL FUTURO ES EL FUTURO DE LA CIBERSEGURIDAD.

- ▶ Protección Anti-Ransomware
- ▶ Protección Anti-Exploit
- ▶ Protección Predictiva Deep Learning
- ▶ Remediación y Limpieza Avanzados

Más información y pruebas gratuitas en:

www.sophos.com/es-es

El reto del ransomware y otras grandes amenazas

El ransomware se ha convertido en una de las principales ciberamenazas a las que deben hacer frente las organizaciones, que puede tener un gran impacto en sus resultados finales, desde pérdidas financieras, interrupciones y daños a la reputación. Los ataques donde se infectan docenas o incluso cientos de ordenadores pueden dejar a las empresas con enormes demandas de rescate que nunca deberían satisfacerse.

¿Te avisamos del próximo IT Digital Security?



El ransomware avanza sin freno. Pese a no ser una amenaza de última generación, está generando enormes problemas a empresas de todos los tamaños. ¿Por qué tiene tanto éxito? ¿Cómo podemos hacerle frente? ¿Cuál es su evolución? La principal vía de entrada del ransomware es a través del correo electrónico, un vector de ataque que también está de plena actualidad y sobre el que también hemos hablado en uno de nuestros #DesayunosITDS, un encuen-



ILUMINANDO EL SHADOW IT

Más del 70% de las organizaciones saben o sospechan que los empleados están usando cuentas personales para compartir archivos. Este documento técnico explora cómo hacer frente al Shadow IT y el uso de aplicaciones personales de intercambio de archivos que ponen en riesgo los datos confidenciales al colocarlos fuera del control y la visibilidad de TI.



"El ransomware y todas sus variantes es la amenaza que más está impactando hoy en día en usuarios y empresas"

José de la Cruz,

Director Técnico de Trend Micro

tro que también ha tenido como protagonista otra gran amenaza: el cryptojacking.

Una reciente encuesta de Logicalis mostraba que la extorsión y el ransomware son consideradas las mayores amenazas de seguridad para las empresas, según un 72% de responsables de TI.

Para hablar de grandes amenazas hemos reunido un grupo de expertos con los que poder debatir sobre la situación del mercado y las grandes amenazas a las que se enfrentan las empresas: Bosco Espinosa de los Monteros, European Presales de Kaspersky Lab; Iván Mateos, Ingeniero de Sophos Iberia; José de la Cruz, Director Técnico de Trend Micro y Vicente Martín, Director Preventa Iberia Panda Security.

"El ransomware y todas sus variantes es la amenaza que más está impactando hoy en día en

usuarios y empresas", dice José de la Cruz, indicando que las nuevas variantes y modalidades de pago no hacen sino agravar la situación. De acuerdo se mostraba Bosco Espinosa de los Monteros, que mencionó cómo el ransomware se está profesionalizado. En opinión de Iván Mateos la importancia que tiene el ransomware se demuestra en que tiene nombre propio y se ha hecho un hueco; "es una amenaza por sí sola y por eso tenemos soluciones dedicadas. Es un gran negocio para la ciberdelincuencia". Vicente Martín destacó que ahora está de moda utilizar el propio equipo de la víctima para cifrarlo, "lo que ya de por sí es una nueva variante".

El dinero es la piedra angular del ransomware. Es lo que mueve a quienes lo diseñan y propagan, que los usuarios y empresas paguen el rescate para

recuperar sus archivos. El ransomware es una gran amenaza que sigue teniendo mucho éxito. El secreto está, según el director técnico de Trend Micro, en su gran rentabilidad económica; “con poca inversión se consigue una gran rentabilidad. Los ciberdelincuentes avanzan y mezclan tecnologías modernas y más antiguas “para conseguir más efectividad”, asegura José de la Cruz.

En ransomware sigue teniendo mucho éxito porque a pesar de que se diga que no se debe pagar, lo cierto es que se paga; “si no fuera así se acabaría el ransomware”, asegura Bosco Espinosa de los Monteros. Añade el ejecutivo que “además nadie te asegura que vayas a recuperar tus datos”. Al



EL RETO DEL RANSOMWARE Y OTRAS GRANDES AMENAZAS

CLICAR PARA VER EL VÍDEO

respecto señalar que no incluso existen algunos ransomware que ni siquiera tienen la capacidad para descifrar los archivos y que, según estudios de Kaspersky, el 20% de los usuarios que han pagado un rescate no han recuperado sus archivos.

Hay que tener en cuenta además que pagando se les está demostrando que se es un blanco, y además vulnerable, de los que pagan de forma que una empresa o usuarios que pague tienen más posibili-

dades de volver a pasar por lo mismo.

En opinión del ingeniero de Sophos el impacto de ransomware se ha infravalorado, “la gente pensaba que era un malware más, pero ha generado toda una industria detrás, con mucha fuerza además”.

Vicente Martín pone el dedo en la yaga al asegurar que realmente se paga porque no se tienen las medidas necesarias para recuperar los datos. “Los cifrados son muy avanzados y es complicado recuperar los archivos”, asegura el directivo de Panda Security, añadiendo que los cibercriminales no son tontos y saben que si la víctima consigue recuperar sus datos “podrá volver a ser víctima. Esto es un negocio y la satisfacción del cliente se tiene en cuenta”, asegura Martín.

El avance del Crytojacking

El cryptojacking es una actividad maliciosa por la que se roban recursos de computación para poder minar criptomonedas. A pequeña escala puede no tener importancia, pero lo cierto es que algunas empresas están viendo cómo su factura de la luz

"En ransomware sigue teniendo mucho éxito porque a pesar de que se diga que no se debe pagar, lo cierto es que se paga"

Bosco Espinosa de los Monteros, European Preventa de Kaspersky Lab

"La gente pensaba del ransomware que era un malware más, pero ha generado toda una industria detrás, con mucha fuerza además"

Iván Mateos, Ingeniero de Sophos Iberia



se incrementa, los empleados pierden productividad y los ordenadores no funcionan como deberían.

Para José de la Cruz el cryptojacking es interesante porque mientras que el ransomware tiene un daño claro y evidente, "el valor que aporta el cryptojacking es que efectivamente es muy rentable, pero el impacto al usuario no es tan grande. Está consumiendo recursos, incrementado el recibo de la luz, pero para una compañía detectar ese tipo de ataque es complicado, y como no se ve afectado no se va a preocupar tanto por protegerse o evitar ese tipo de ataques, lo que le hace más rentable".

Es más, si el ciberdelincuente es listo "no va a consumir todos los recursos disponibles de la máquina, sino unos pocos para permanecer el mayor

tiempo posible, generando dinero sin levantar sospechas", dice Bosco Espinosa de los Monteros. La ventaja del cryptojacking, dice también el ejecutivo de Kaspersky es la cantidad de tiempo que puede estar funcionando, y que no es tan perseguible.

Para Iván Mateos los ciberdelincuentes han visto que pedir un rescate es violento y han decidido hacerlo más suave: "no te pido dinero, te pongo a fabricarlo". Y lo que se busca es permanecer el mayor tiempo posible en una máquina para generar más beneficios. Es seguro, dice el ejecutivo de Sophos, que "termine siendo más productivo que el ransomware, y sin embargo los usuarios no son tan conscientes de que también tienen que protegerse".

Vicente Díaz está de acuerdo en que cuando se habla de cryptojacking hay un tema de percepción

importante porque "cuando un usuario tiene un ransomware lo sabe, pero con el cryptojacking un usuario puede percibir que algo pasa, que su máquina va más lenta, se queja... Pero no aparece una pantalla con una alerta. El cryptojacking hace caja continuamente, mientras que el ransomware la hace una vez, si la hace".

Añadimos el elemento del IoT al tema del cryptojacking, porque ya se han detectado conversaciones en la Dark Web sobre la posibilidad de utilizar dispositivos conectados para minar monedas, algo para lo que se requiere de capacidad de cómputo. Para José de la Cruz, es complicado porque "un dispositivo de IoT no tiene esa capacidad, es cierto que lo mismo millones de dispositivos procesando un cachito cada uno... a lo mejor sí es factible. Habría que hacer un business case, pero es significativo", asegura el directivo de Trend Micro.

Y además añade José de la Cruz el hecho de que haya empresas que se están planteando realizar minado de monedas de sistemas ajenos de manera legítima y legal. Es decir, que mientras que el usuario esté utilizando determinados servicios permita utilizar los recursos de su CPU en compensación "para hacer este tipo de actividad de manera totalmente consentida. Es decir que se está poniendo en paralelo la actividad ilícita con la legítima de este tipo de actividades".

Para Vicente Martín es "interesante pensar que la legalización pueda acabar con esta parte del negocio. Y es posible que esta sea una iniciativa que pueda acabar con esa parte del negocio oscuro que

Frente a grandes amenazas, grandes soluciones

Al finalizar el debate, pedimos a nuestros invitados que nos hablen sobre sus propuestas más avanzadas para hacer frente a las amenazas de seguridad.

Trend Micro. José de la Cruz. El ransomware es una amenaza que ataca múltiples vectores, que está en constante evolución, y Trend Micro entiende que el mejor planteamiento son dos: Tecnología multicapa, que es combinar todas las tecnologías que hemos desarrollado, partiendo de un motor de firmas a tecnologías más avanzadas, como el machine learning, el sandboxing de manera coordinada y conjunta para proporcionar la mejor protección a nuestros usuarios. La segunda sería lo que llamamos Seguridad Conectada, que es proteger todos los vectores de entrada (correo electrónico, navegación, puesto de trabajo...) compartiendo la inteligencia con todos los elementos de componen la oferta de seguridad de nuestra compañía.

Kaspersky. Bosco Espinosa de los Monteros. Por nuestra parte pensamos que por supuesto hay que proteger el endpoint, que es la primera barrera de entrada, y proteger todos los vectores de ataque, y además tener una visibilidad de lo que ocurre, analizar todos los archivos, el poder hacer sandboxing, comprobar qué está haciendo y utilizar múltiples motores y múltiples tecnologías que nos ayuden a saber lo que está ocurriendo. Hay que combinar todas las tecnologías, unificar todo. Y añadiría una capa más que sería la formación y concienciación al usuario, que puede elevar mucho el nivel de seguridad con una inversión muy pequeña.

Sophos. Iván Mateos. El primer punto en la estrategia de Sophos es mantener el nivel de protección en el endpoint y el firewall UTM, donde invertimos cada día para añadir mejoras. Y el segundo punto es que debemos tomarnos la seguridad como un ecosistema y no como un Frankenstein de soluciones. Al final lo que propone Sophos es que todas las soluciones se hablen entre ellas, que la capacidad de respuesta te haga sumar más; que la seguridad sincronizada de la que hablamos te aporte un poco más de lo que tenías hasta ahora. Y tercer punto que muchas veces se pasa por alto: ya no es sólo mantener la seguridad, sino mantener la sencillez. Las plataformas tienen que ser fáciles de administrar.

Panda Security. Vicente Martín. Nosotros queremos aislar al usuario del malware, que todo sea fácil y la catalogación del 100% de los procesos de corren en el equipo. Nosotros esa catalogación la hacemos desde el punto de vista del goodwill; catalogamos todo lo que es confiable, y todo lo que no lo es lo bloqueamos por defecto hasta que se analice. Es una catalogación para la que utilizamos diferentes técnicas, todas en cloud y que al final están apoyadas en una persona que cubre ese gap. También hacemos una labor de threat hunting, que es un paso más allá del malware y que es hacia donde todos vamos evolucionando.

hay detrás y que deje de ser rentable para según qué empresas u organizaciones”.

La rentabilidad está sobre la mesa, dice Bosco Espinosa de los monteros, porque al final de manera legítima o no, consumo los recursos de otro.

“El problema es que abres la puerta...”, dice Iván Mateos, quien asegura que puede que al final cada



web, cada servicio, se convierta en un minero de criptomonedas.

“Es que la gratuidad es algo que tenemos que empezar a pensar que tiene sus consecuencias. No te creas que todo lo que hay por detrás es tan bonito porque no es así, no todo es tan maravilloso”, añade Vicente Martín.

"El cryptojacking hace caja continuamente, mientras que el ransomware la hace una vez, si la hace"

Vicente Martín,

Director Preventa Panda Security Iberia



Correo electrónico, el mayor vector de ataque

El email no es una gran amenaza, pero sí que es el principal vector de ataque, la puerta por donde llegan la mayoría de las grandes amenazas. Y a pesar de que su trayectoria está asociada a Internet, sigue siendo una asignatura pendiente.

Para José de la Cruz es sin duda el principal vector de ataque. Algo que tiene que ver con la manera que está diseñado el protocolo SMTP, que funciona de una manera que puedes fácilmente ocultar el remitente. Y es que si bien es cierto que hay muchos mecanismos de protección avanzada (SPF, DKIM) para mejorar el nivel de protección, "puede ser muy sencillo suplantar la identidad del remitente y que un documento parezca legítimo".

Y no hay que olvidarse, dice el ejecutivo de Kaspersky, la ingeniería social. Proteger adecuadamen-

te el correo electrónico no es tarea fácil porque si se protege al máximo ese pierde usabilidad y el usuario se queja, "o permito que el usuario tome acciones, y entonces puede hacer algo que no debe. Y siempre estamos en esa lucha".

"Además, el correo y el phishing tienen una ventaja, y es que llegan a todos los usuarios, desde el que sabe al que no", dice Iván Mateos, quien añade que "da igual hablar del eslabón débil", porque si un usuario pincha y abre todo lo que le llega, por mucha conciencia que se tenga, se está abriendo la puerta al atacante, "y el phishing ha evolucionado mucho precisamente porque es muy efectivo. Es el principal vector de ataque de ransomware, del cryptojacking, del robo de credenciales, precisamente por la efectividad que tiene. La gente no lo sabe identificar y además los ciberdelincuentes lo hacen cada vez mejor".

Habla Vicente Martín de debilidades humanas; "todo el mundo es curioso y si lo que tienes delante es atractivo vas a caer. Siempre que esté bien hecho, siempre que esté bien escrito, la gente pincha porque es curiosidad, es innato".

En este punto la formación y concienciación a los empleados se convierte en un elemento de lo más recomendable. Para el directivo de Panda Security se está empezando a hacer, pero es lento porque hay que esperar que todo lo que le has enseñado lo asimile. "No es como colocar una pieza de software, un appliance que te proteja y es inmediato, sino que hay que darles formación y eso lleva tiempo", dice Bosco Espinosa de los Monteros, añadiendo que la nueva regulación europea está ayudando a impulsar esa formación y concienciación, aunque sea un poco tarde.

Iván Mateos lo tiene claro: "Plataformas de entrenamiento para que el usuario aprenda a distinguir el phishing son casi tan importantes como lo bueno que sea tu protección endpoint". Y añade que, aunque muchos empleados creen que esto de la seguridad no va con ellos, "no es verdad, a ellos también les afecta, en ello va su reputación, y tienen que participar y que la inversión que hace una empresa en seguridad también implique a los usuarios".

Machine Learning contra las grandes amenazas

En los últimos años parece que el machine learning se ha convertido en la bala de plata de la seguridad. Anunciado a bombo y platillo en campañas de marketing la tecnología tiene, en realidad, solera. Un



El cryptojacking es una actividad maliciosa por la que se roban recursos de computación para poder minar criptomonedas

informe de Radware indica que para finales de este año la mitad de las empresas habrán incorporado Machine learning/IA en sus soluciones de seguridad.

La estrategia de Trend Micro, dice el director técnico de esta firma de seguridad, “es incorporar múltiples barreras de protección y el machine learning es una capa más que nos ayuda a protegernos, que en el caso de ransomware es particularmente efectiva porque nos ayuda a protegernos sin necesidad

de patrones, analizando tendencias de cómo el tipo de código se está ejecutando”.

A Bosco Espinosa de los Monteros, le sorprende “que digan que lo van a implementar, porque llevamos bastantes años utilizándolo en el endpoint. Lo que pasa es que quizá no lo llamábamos next generation, ni machine learning, pero es una capa más es importante y llevamos años”. E incide el ejecutivo que se trata de una capa más, y que no se puede proteger sólo con firmas, pero sólo con machine learning tampoco; “tienes que tener análisis de comportamiento, listas de reputación, firmas... yo desecharía ninguna tecnología”.

En Sophos la variante de machine learning que se utiliza es Deep Learning, y para Iván Mateos “la

Enlaces de interés...

- ! [La extorsión y el ransomware son las mayores amenazas para los CIO](#)
- ! [Crece la amenaza del cryptojacking en los entornos cloud](#)
- ! [Los dispositivos conectados también sirven para minar criptomonedas](#)
- ! [Atlanta, la ciudad devastada por un ransomware](#)
- ! [Evite que el ransomware llegue a su puerta](#)

gente también se está dando cuenta que no todo es machine learning. Estoy de acuerdo en que es una capa más, pero que te mantiene en competición con los ciberdelincuentes, porque ellos también lo utilizan”.

Vicente Martín asegura que el machine learning ha cogido más peso, pero que la clave es cómo se utilice o complemente. En el caso de Panda desde hace unos años se utiliza el machine learning “desde una perspectiva de catalogar lo bueno en vez de lo malo, pero siempre lo tienes que complementar con algo, porque el machine learning, y todas las tecnologías automáticas, tienen un gap de detección. Lo importa es que utilicemos la mejor tecnología posible”.

Compartir en RRSS



BE SURE TO BE FREE

BLINDA TUS "SUPERCONFIDENCIAL"



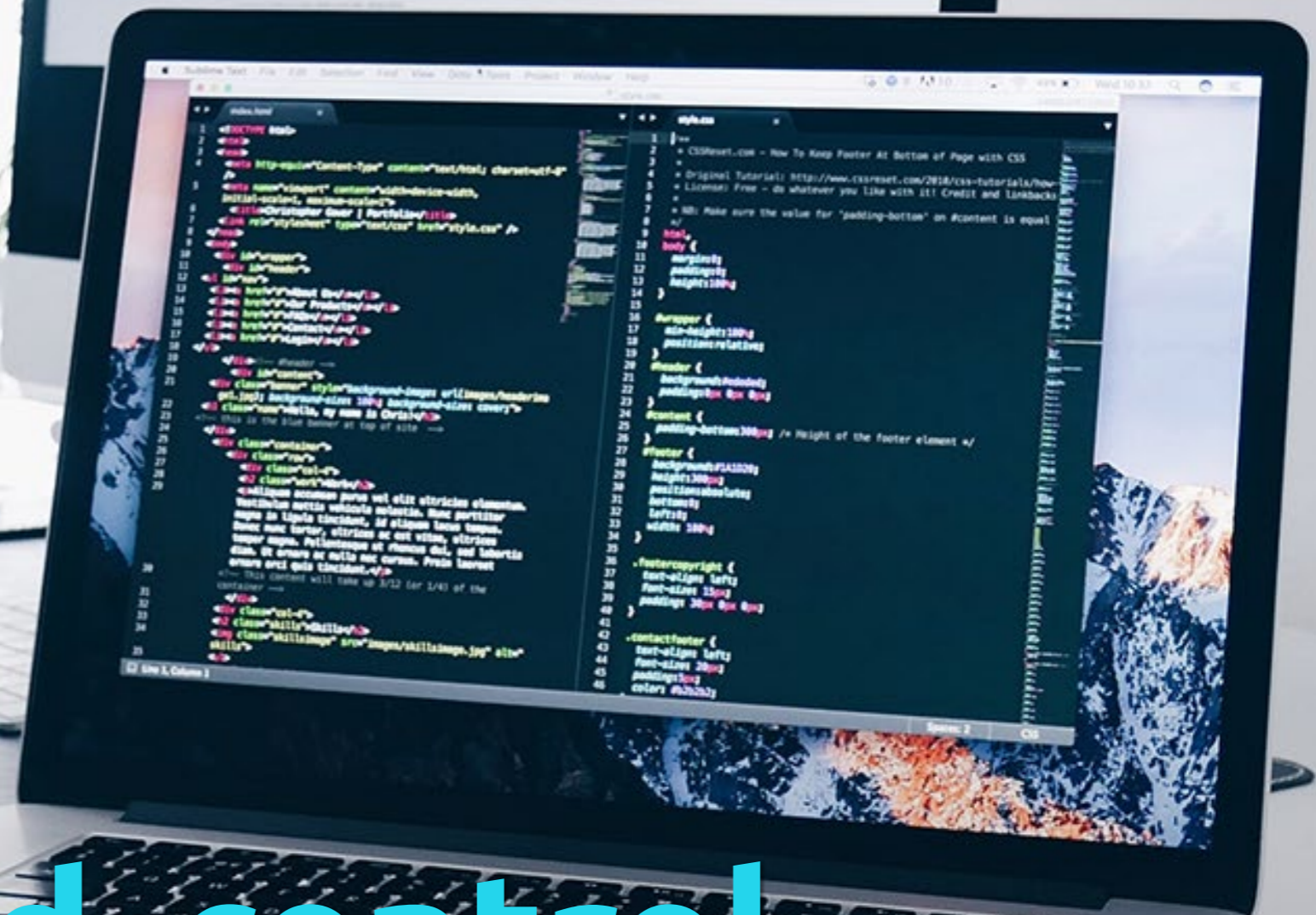
#BlindaTuLibertad

Garantiza que lo que pasa en tu empresa se queda en la empresa.
Descubre lo último en ciberseguridad empresarial.

www.eset.es



ENJOY SAFER
TECHNOLOGY™



Visibilidad, control y modularidad: seguridad de nueva generación



Visibilidad y modularidad: seguridad de nueva generación

La red es un ente cada día más complejo, tanto dentro del perímetro, con un número incremental de dispositivos, conocidos o no, conectados a la misma, como fuera de él, donde se multiplican las conexiones con un sinfín de dispositivos móviles de empleados, proveedores y clientes, además de una cantidad ingente de dispositivos que todavía no ha llegado a su límite, o que, mejor dicho, todavía está por explotar, como es IoT.

Esto supone uno de los retos a los que las empresas deben enfrentarse cuando de seguridad hablamos, que se une a la necesidad imperiosa de cumplir con todas las normativas que afectan a las compañías, sus datos y sus sistemas de TI.

Y es que los CISO y los CSO tienen ante sí dos grandes retos que ninguna empresa puede eludir, porque son la base sobre la que edificar su futuro. En otras palabras, no asumir ambos retos podría suponer la desaparición de una empresa, bien porque cualquier ataque pueda acabar con sus datos o con su reputación, y sin ninguno de los dos elementos se puede vivir, o porque se incumplan las normativas, lo que arriesga a las empresas a multas, en algunos casos,





millonarias, que pueden poner en riesgo su porvenir.

Pero vayamos por partes. El primero de los retos a los que tienen que hacer frente las empresas es el de la explosión de tecnología en las redes corporativas, con más dispositivos, diferentes formatos, diferentes sistemas operativos, diferentes formas de conexión, diferentes lugares, diferentes objetivos... y eso sin tener en cuenta la que se le viene encima a los administradores de las redes con el despliegue masivo de dispositivos con IoT, donde convivirán dispositivos muy inteligentes y autónomos con otros “tontos” que no tengan ni la posibilidad de securizarse a sí mismos.

Las empresas tienen que cambiar su forma de entender y de enfrentarse a la seguridad, porque lo que ha funcionado durante muchos años, como ha sido la seguridad perimetral, ha dejado de tener sentido. Durante años, la propuesta más efectiva para la seguridad era defender el perímetro, y muchos proveedores conectaban esta idea con la imagen de un castillo y un foso. No es que se haya quedado tan anticuado con la imagen, pero el acercamiento a la seguridad desde esta idea ha dejado de ser efectivo, entre otras cosas porque el perímetro, como tal, ha desaparecido. Porque, ¿dónde acaba ahora la red de la empresa? Antes, los usuarios se conectaban por cable a los recursos de red de las compañías. Ahora lo hacen en movilidad mediante 4G, WiFi o VPN desde cualquier

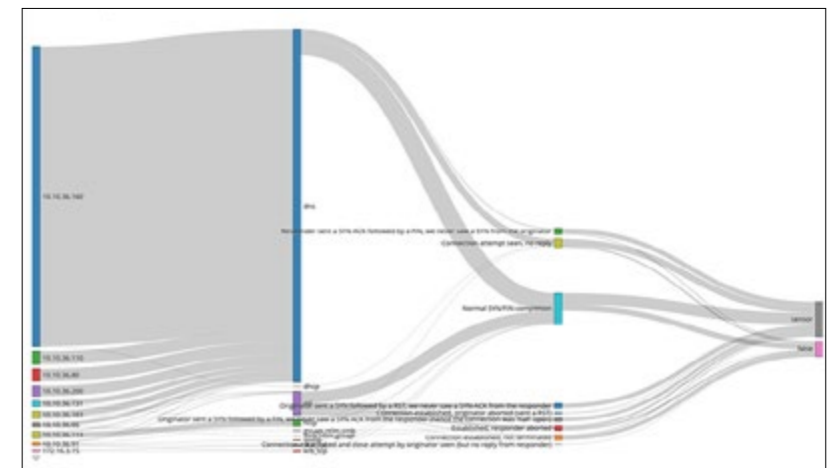
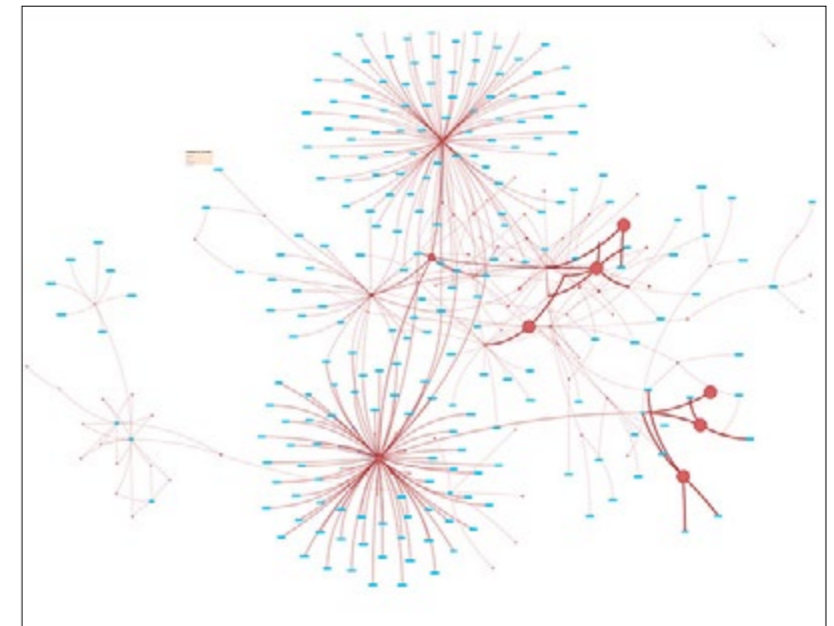


La visibilidad, desde diversos puntos de vista, es fundamental para la seguridad de nueva generación que necesitan las empresas

lugar, con dispositivos que no siempre han sido proporcionados por la propia compañía ni, en algunos casos, aprobados por el departamento de TI. Además, la empresa está conectada con sus proveedores, y, sobre todo, sus clientes, que quieren que la empresa les atienda siempre y desde donde ellos lo precisen, accediendo en muchos casos a datos muy sensibles para la propia empresa.

Por tanto, el perímetro conocido es una ilusión que no permite servir de base sobre la que desarrollar la red, de ahí que sea necesario buscar otra alternativa.

El segundo gran reto a los que tiene que enfrentarse la empresa, en lo que a la seguridad se refiere, es el cumplimiento de normativas y leyes, tanto internacionales, como pueda ser el caso de GDPR, como por la legislación nacional.



El cumplimiento de normativas es algo que no se puede ignorar, y las empresas deben asegurarse de que se cumplen todas y cada una de las normativas de aplicación en la empresa.

NUEVA APROXIMACIÓN A LA SEGURIDAD

Como ya hemos comentado, las empresas deben pensar en cómo diseñar e implemen-

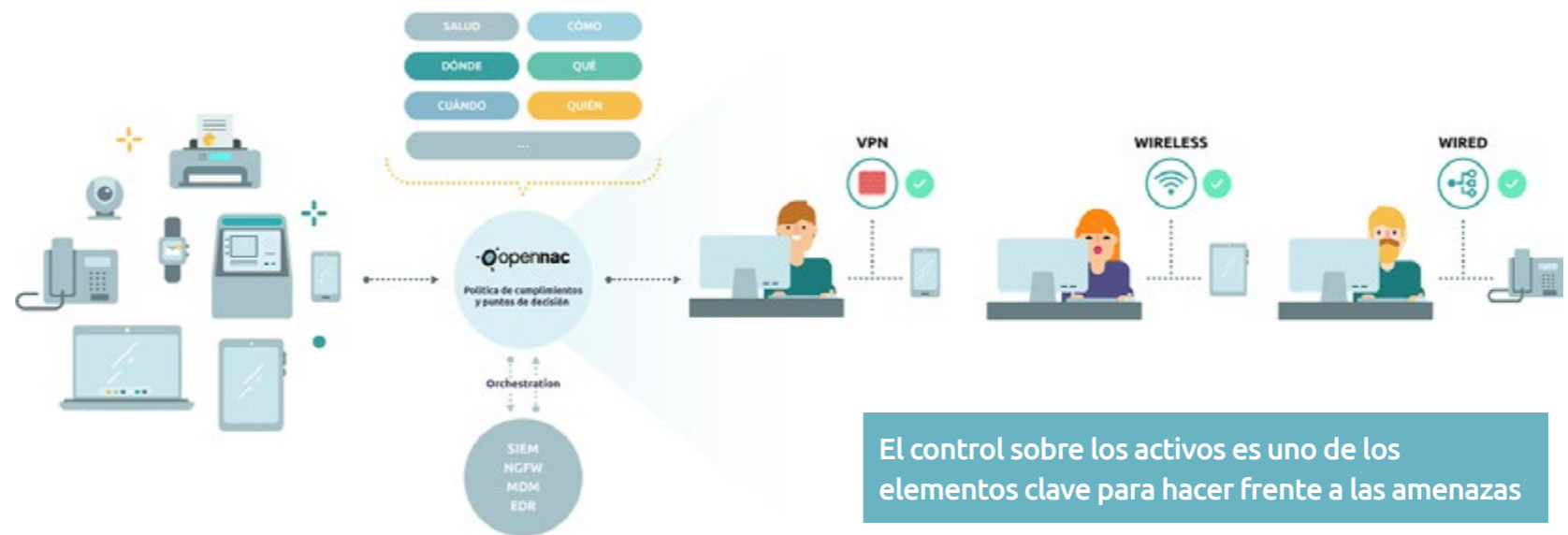


tar la seguridad, de forma que den respuesta a los retos que se les imponen en este momento. Y si algo es necesario tanto para securizar esta red creciente como para el cumplimiento de normativas es la visibilidad de todo lo que está conectado a la red, lo que permite a los responsables de esta seguridad establecer la trazabilidad de todos los accesos a la red.

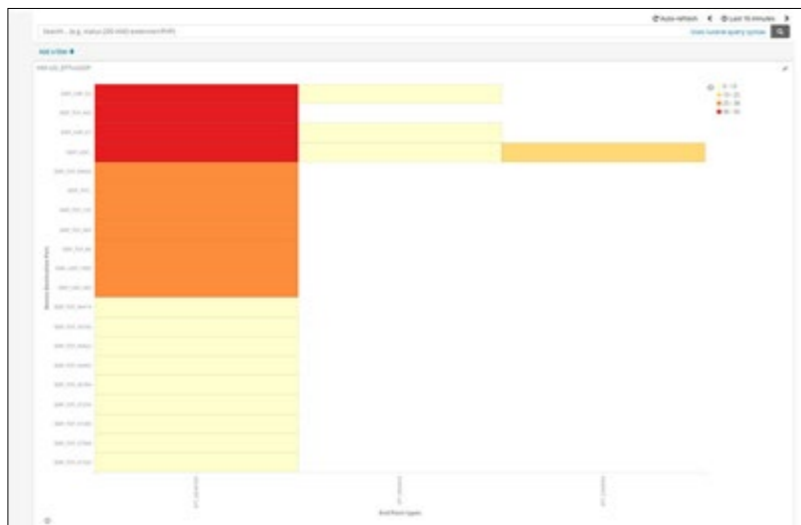
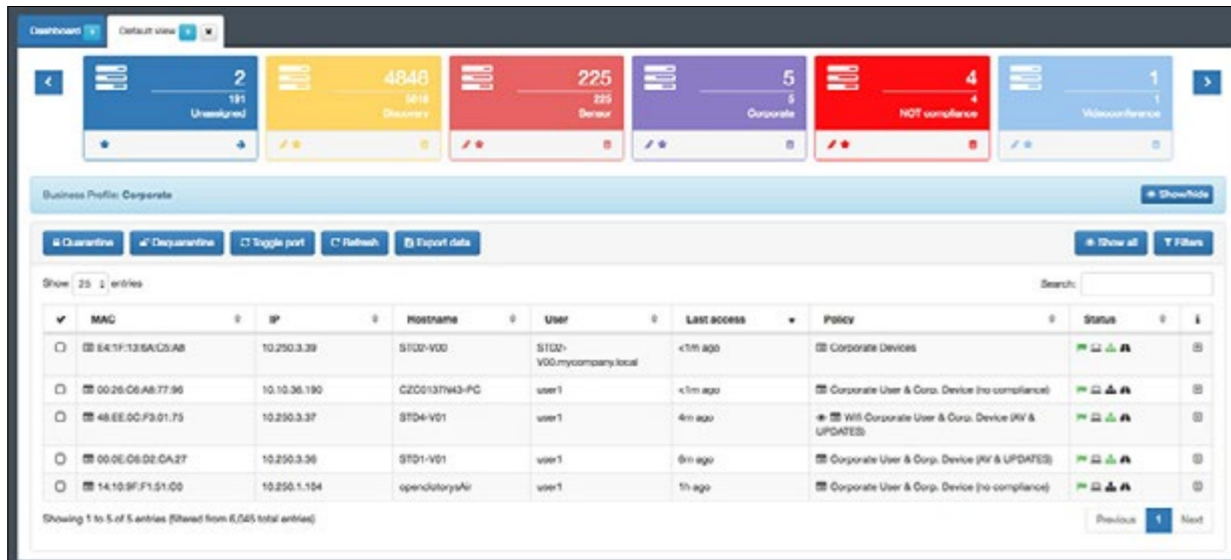
Por tanto, esta visibilidad puede verse como un primer paso de la seguridad, porque hay que empezar por conocer y entender todo lo que está conectado, tener el máximo información para, sobre esto, ir desarrollando otras capas de la seguridad, como las políticas de control.

Porque, como indicábamos, el paradigma de seguridad perimetral ha cambiado, y encontramos muchas cosas conectadas dentro y fuera del perímetro. Hay que cambiar la forma de entender la seguridad, que debe verse desde cualquier dispositivo que se conecta a la red.

Y si ahora son muchos los dispositivos en la red, ¿qué pasará con el despliegue real de Internet de las Cosas? En el desarrollo de IoT hay dispositivos de todo tipo, y muchos de ellos no tienen capacidad para incorporar una solución de seguridad tradicional, como un antivirus o un antimalware,, con lo que hay que pensar en otras formas de asegurar IoT, y una de las propuestas está precisamente ahí, en la conexión. Cuando un dispositivo intenta conectar hay que analizar el dispositivo y la



LA SEGURIDAD SEGÚN OPENCLOUD FACTORY



Control sobre todos los elementos de la red, clave en la seguridad



conexión y determinar el nivel de seguridad adecuada o el área de red a la que pueden conectarse, en función del propio dispositivo y su naturaleza.

TODO LO QUE ESTÁ CONECTADO CUENTA

Las empresas han estado en jaque durante años; el trabajo a distancia, el número cada vez mayor de proveedores/ colaboradores de

servicios, BYOD, la implementación de tecnologías de vanguardia y el mantenimiento de soluciones heredadas en productos electrónicos heterogéneos han sido parte de la experiencia cotidiana en la lucha contra incendios para garantizar un panorama de amenazas cada vez mayor. Sin embargo, en 2018 IoT ha empujado a los equipos de operaciones de red y seguridad más allá de un punto sin retorno.

Este 2018 ha marcado un punto de inflexión para IoT dentro de un contexto empresarial. Las organizaciones han pasado de una fase de conceptualización/descubrimiento de IoT, que duró algunos años, a una fase de implementación/ejecución para aprovechar las ganancias

prometidas de eficiencias de IoT. La mayoría de las empresas que adoptan IoT hoy utilizan métricas e indicadores clave de rendimiento (KPI) que reflejan las mejoras operacionales, la experiencia del cliente, la logística y las ganancias de la cadena de suministro.

Hasta 2018, los principales problemas para las empresas han sido el volumen de dispositivos que se deben proteger y la naturaleza heterogénea/dispersa de las redes, donde cada dispositivo conectado es un punto potencial de ataque o reconocimiento. IoT, además de agregar volumen al problema también ha agregado capas adicionales de complejidad al mismo.



El gasto de la empresa en IoT crecerá inicialmente un 30,7% anual en los próximos 3 años. Todo ese gasto deber ser administrado por una red y un equipo de operaciones de seguridad que no crece al mismo ritmo. Por sorprendente que parezca este crecimiento, no tiene en cuenta que otras cosas, los empleados, invitados y contratistas adoptarán a la red para hacer que

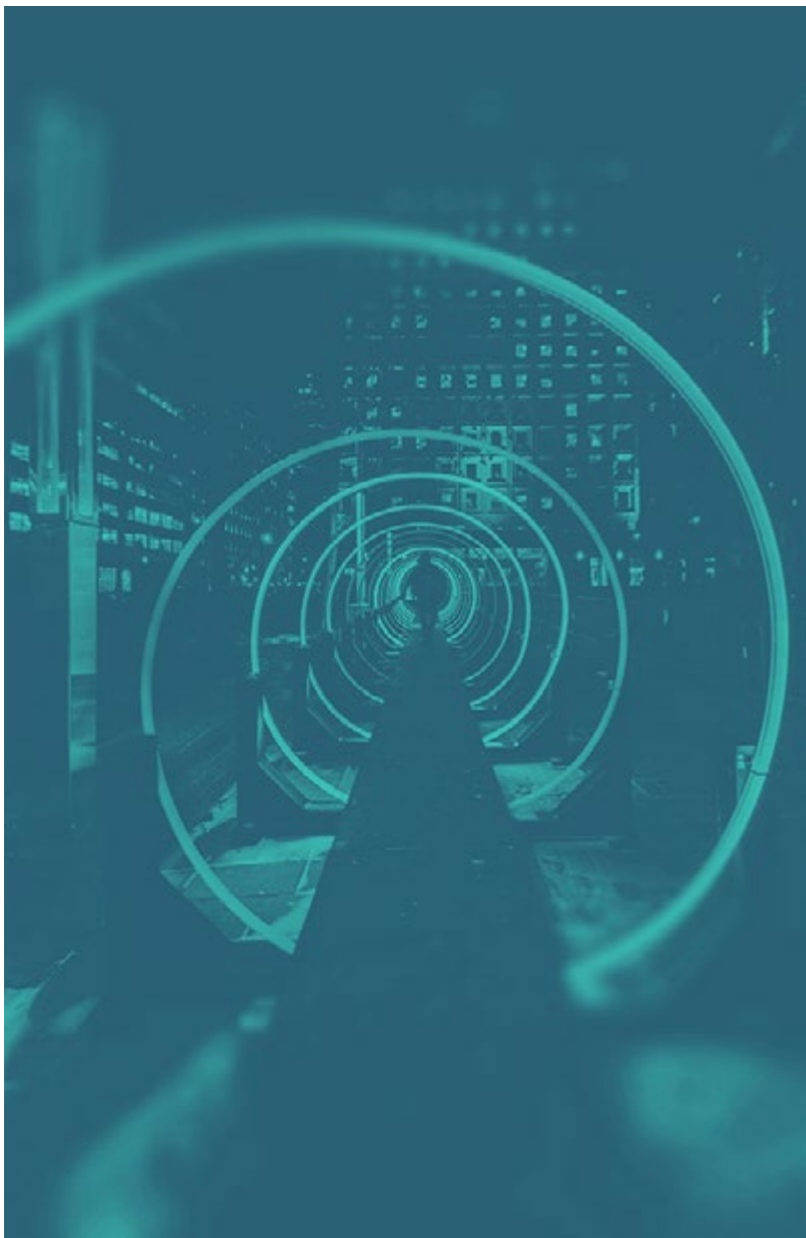
su día a día sea más eficiente. Por lo tanto, el total de dispositivos conocidos que se gestionarán no tiene precedentes, pero aún debemos agregar los dispositivos desconocidos (no corporativos).

La mayoría de los dispositivos de IoT son económicos, diseñados especialmente, y de conexión plug and play, todos aspectos positivos desde el punto de vista de la empresa. Sin embargo, esto "faculta" a las unidades/departamentos de negocios para que compren las cosas que necesitan y las conecten directamente a la red para obtener resultados rápidos sin aprovisionarlas primero a través de redes u operaciones de seguridad. Esta falta de "descubrimiento y visibilidad" da como resultado una planificación inadecuada que no está alineada con los objetivos comerciales, lo que genera tiempo perdido, recursos, brechas de seguridad y un mayor riesgo.

¿INSEGUROS POR DISEÑO?

Aunque el artículo 25 del Reglamento General de Protección de Datos establece que toda la protección de datos deber ser por diseño y de manera predeterminada, la realidad es que hasta que se cumplan las regulaciones, la métrica clave del éxito para los proveedores de IoT no será la confianza del mercado, sino el tiempo de comercialización. En estos casos, la seguridad es un segundo pensamiento en la mayoría de los casos.

Incluso si los fabricantes cuentan con cierta conciencia de seguridad, la mayoría de los dispositivos IoT son livianos y no tienen la capacidad de instalar y mantener controles de seguridad estándar, como soluciones antimalware, o no pueden escanearse de forma remota, convirtiéndolos en un objetivo fácil para los agentes de malware, abriendo



nuevas rutas de ataque en los entornos de red/IoT.

NO TODAS LAS COSAS SON IGUALES EN IOT

Algunos dispositivos IoT son “terminales brutos” en el sentido de que no procesan datos importantes y, por lo general, están limitados por los recursos. La mayoría tiene un procesamiento y memoria limitados para ayudar a los agentes. En el otro extremo del espectro, algunos dispositivos IoT tienen una increíble potencia de procesamiento que puede aprovecharse malignamente y, lo que es más preocupante, es que procesan datos confidenciales (información de identificación personal, datos de categorías especiales), además de poder cambiar los estados físicos de sus entornos. Esto se ve claramente en el sector de la Salud, donde los datos procesados son fundamentales y la posibilidad de cambiar los estados físicos es literalmente mortal.

EL PRECIO DE LA GLOBALIZACIÓN

Junto con todo lo anterior, el tsunami de IoT, los nuevos colaboradores y los módulos de trabajo, los entornos heterogéneos se combinan con el efecto global, y es que debido a los objetivos de eficiencias corporativas, las organizaciones necesitan administrar oficinas más remotas a través de divisiones geográficas mayores, integrar nuevas compañías mediante adquisiciones/fusiones lo más rápido posible, todo con una debida diligencia y seguridad.

INCREMENTO DE LA VISIBILIDAD

En general, los tiempos de detección, según el Trustwave Global Security Report, han disminuido, debido a la tecnología de seguridad de vanguardia. Sin embargo, los tiempos de respuesta a los ataques aumentan debido, en parte, a los falsos positivos y la complejidad de este nuevo paisaje en expansión conocido y desconocido. Para agravar el problema, el impacto de los ataques, tanto desde un punto de vista económico como de reputación, aumenta a medida que los ataques se han convertido en “ataques a gran escala, multi vector y mega ataques” (informe de ataques de la Generación V, Checkpoint).

Los siguientes controladores para aumentar la visibilidad de las soluciones de IoT también se aplican a todos los activos de la empresa en la mayoría de los casos. El problema de base es común: no se puede controlar, administrar o asegurar lo que no puede ver. La visibilidad es el pre-requisito para la seguridad.

❖ **Presión de regulación y auditoría:** algunos auditores requieren que una organización brinde visibilidad y control sobre todos los dispositivos que están conectados a la red corporativa principal.

En Gartner’s Guide to Network Access and Control 2017, Gartner señaló que las consultas de los clientes mostraron una gran demanda de respuesta a los comentarios de los auditores sobre la falta de visibilidad de los dispositivos



❖ **Respuesta y recuperación (Regulaciones):** cuando responden a violaciones de seguridad, las organizaciones necesitan responder y recuperarse rápidamente, tanto desde un punto de vista técnico como desde un punto de vista reputacional. Por la misma razón, cuanto mayor sea la información disponible sobre todos los activos, mejor (por ejemplo, nombre del dispositivo, tipo, ubicación, es un activo crítico...).

El Artículo 33 de la GDPR establece claramente: “medidas tomadas o propuestas a tomar por el controlador para abordar la violación de datos personales, incluidas, cuando corresponda, medidas para mitigar sus posibles efectos adversos”.

❖ **Programas BYOD:** BYOD requieren visibilidad y cumplimiento de políticas para garantizar que el empleado no quiera o quiera exponer a las corporaciones a un riesgo mayor.

❖ **Autenticación:** para permitir que la autenticación basada en la red administre qué dispositivos pueden obtener acceso a la red, primero se debe lograr una visibilidad del 100% en todas las capas de acceso (cable, Wi-Fi y VPN).

FRENTE AL PROBLEMA... LA SOLUCIÓN

Portátiles, smartphones, tablets, proveedores, usuarios externos, y una gran oleada de dispositivos (IoT) se conectan diariamente a unas redes que son cada vez más heterogéneas, dispersas y complejas de gestionar,

cada activo es un riesgo a gestionar. Frente a esto, Opencloud Factory pone sobre la mesa la solución openNAC Enterprise, que, sin importar el tipo de dispositivo y cómo se conecta, automáticamente descubrirá y categorizará todos los activos de su red corporativa.

A través de la visibilidad y control centralizado que aporta openNAC Enterprise, la empresa podrá disminuir el riesgo y el im-

pacto de los ataques disruptivos y responder ante requisitos de regulaciones. openNAC Enterprise, sin importar el tipo de dispositivo y cómo se conecta, automáticamente descubrirá y categorizará todos los activos. Las organizaciones puedan aplicar la categorización al contexto del negocio y sus riesgos para priorizar sus esfuerzos y responder ante auditorias.



CASO DE ÉXITO:
OPECLOUD FACTORY UNIVERSIDAD DE BARCELONA



Una vez conseguida la visibilidad e información sobre cada conexión (usuario / dispositivo), la solución le proporciona un punto único y central donde puede definir y aplicar políticas de acceso, adaptadas a las necesidades de la organización, y los accesos correspondientes para todos los activos conectados y que intenten conectar. La organización puede, de manera automática, permitir, denegar y limitar todos los accesos (cable, wi-fi y VPN) basándose en la lógica del negocio con una trazabilidad 100% de lo conectado; desde qué dispositivo, con qué credenciales, a que segmento de la red, durante cuánto tiempo ..etc.

Con la misma facilidad la organización puede aplicar una política nueva sobre dispositivos ya conectados para dar respuesta en tiempo real a una incidencia; por ejemplo, ante una brecha de

seguridad una organización podrá querer aislar todos los dispositivos afectados que tengan datos personales para responder ante el Artículo 33 del GDPR. La política se aplicará en tiempo real y podrá segmentar los equipos en cuestión y hacerlos un seguimiento desde un *dashboard*.

UNA SOLUCIÓN MODULAR QUE RESPONDE A TUS NECESIDADES HOY Y MAÑANA

openNAC Enterprise es una solución software se puede implementar desde la nube, on-premise o en un modelo híbrido reduciendo así el impacto en tu infraestructura, y que ofrece visibilidad y control total sobre las redes corporativas. Con openNAC Enterprise descubrirá todos los dispositivos (siendo del tamaño que sean) que están conectados a sus infraestructuras, ofreciendo diferentes

¿Te gusta este reportaje?

Compártelo en redes



mecanismos de descubrimiento, perfilado y control acceso a su red.

Además, OpenNAC Enterprise es una solución que ofrece la seguridad por módulos, proporcionando una seguridad que se adapta a la situación actual, aportando resultados en menos tiempo y con menos esfuerzo. La modularidad de la solución podría incrementarse a medida que crece la complejidad de la propia empresa. ■

MAC	IP	Hostname	User	Last access	Policy	Status
00:21:B7:55:A4:75	180.235.193.244			<1m ago	Printer	🟢🟡🔴
00:21:B7:E6:DF:7D	180.236.229.188			<1m ago	Printer	🟢🟡🔴



MÁS INFORMACIÓN



[Opencloud Factory](#)



[El CISO ante la problemática de la seguridad en su empresa](#)



[Opencloud Factory](#)



[Casos de éxito](#)



[Construcción de un entorno seguro](#)



Principales beneficios de openNAC Enterprise

❖ VISIBILIDAD

- Inventario 100% de dispositivos / things, infraestructura y usuarios.
- Visibilidad continua automática en la conexión.
- Etiquetar activos críticos (GDPR...) por contexto del negocio y los riesgos de ciberseguridad relacionados para priorizar los esfuerzos.
- Permite responder ante auditorías y ataques.

❖ CONTROL DE ACCESO UNIVERSAL

- Simplifique el control de acceso de los activos en redes cableadas, Wi-fi y redes privadas virtuales (VPN)
- Punto único de decisión y aplicación de las políticas de acceso.
- Integración /adaptación con otras soluciones de seguridad NGFW / SIEM etc.

❖ SEGMENTACION DE RED

- Segmentar redes y funciones para contener el daño cuando ocurre una intrusión.
- Reducir la superficie de ataque.
- Proteger / asilar activos críticos.
- Segmentación simple de IoT.

❖ COMPLIANCE

- Cumplimiento de seguridad del EP con las políticas corporativas / mandatos regulatorios.
- Definir y aplicar políticas de seguridad para EP.
- Descubrir EP y garantizar el cumplimiento con la política de manera automática.

❖ BOYD SEGURA

- Única identidad corporativa
- Controlar y rastrear accesos a la red

❖ CONTROL DE ACCESOS DE INVITADOS

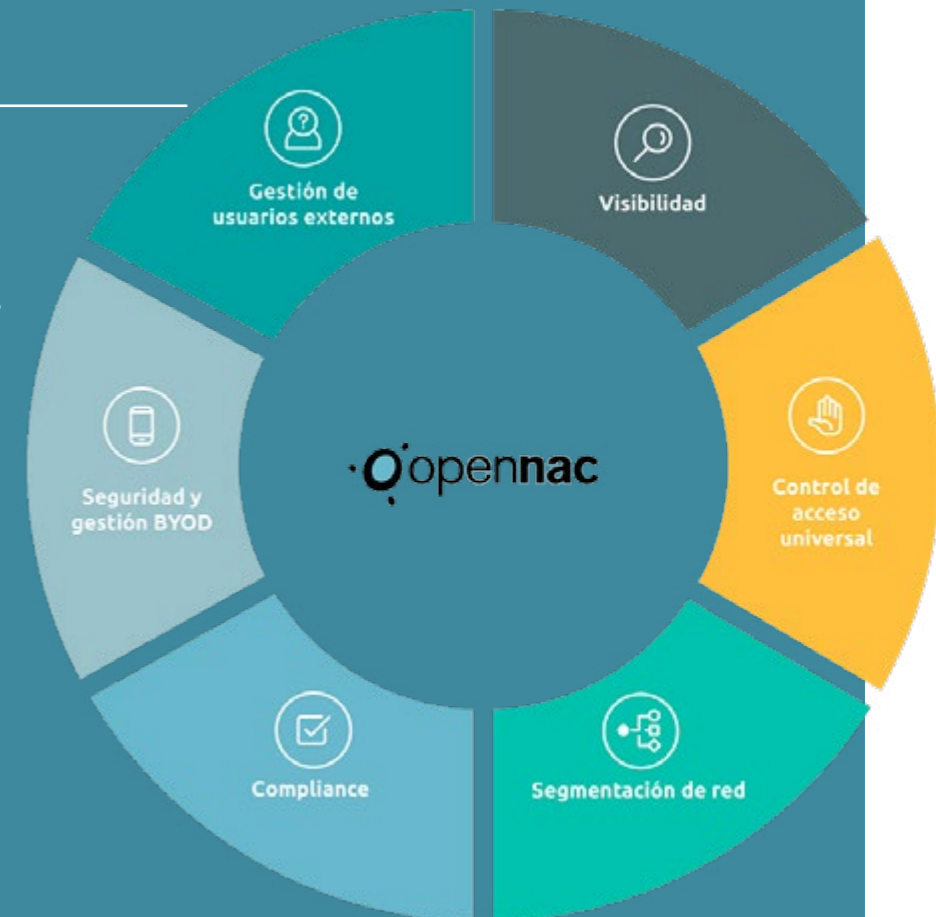
- Aislamiento automático de la red
- Reconfiguración de accesos.

❖ DIFERENTES DESPLIEGUES

- Desde la nube:
- La implementación en la nube no requiere infraestructura o mantenimiento
- On premise: VM son premise no requiere HW

❖ OTROS VALORES

- Escalado horizontal
- Entorno multivendedor amigable
- Adaptable a la infraestructura de red de la empresa



Control y visibilidad de tus datos personales

Simplifica el cumplimiento del GDPR

Con la entrada en vigor del GDPR (General Data Protection Regulation), las empresas deberán, no solo proteger su privacidad, sino también controlar cómo se procesan, almacenan y utilizan sus datos. **Panda Adaptive Defense** y su módulo adicional **Data Control**, te ayudarán en el cumplimiento del GDPR.



Descubre y audita

Identifica a los usuarios, equipos o servidores con acceso a Información de Identificación Personal (PII) de tu empresa.



Monitoriza y detecta

Implementa medidas de acceso y operación sobre PII con la ayuda de los informes y las alertas en tiempo real.



Simplifica la gestión

Su activación es inmediata y se gestiona directamente desde la misma plataforma cloud.



Control de datos

Tu empresa tendrá un control exhaustivo de la PII ubicada en sus equipos.

Contacta con tu distribuidor habitual o llamando al 900 90 70 80

Seguridad y Cloud, ¿qué nos queda por aprender?

Con las aplicaciones y los datos distribuidos entre nubes y plataformas, el control de los mismos se hace cada vez más necesario. Se requiere tener visibilidad sobre dónde viajan tus datos, quién accede a ellos y desde dónde, así como qué aplicaciones están utilizando tus empleados.

Si bien no puede obviarse el avance en la seguridad cloud, aún hay muchos responsables de seguridad que se dan cuenta de que las herramientas y procesos de seguridad heredados no son suficientes para asegurar un nuevo ecosistema sin perímetro y en constante cambio.

Menos de la mitad tienen visibilidad sobre el intercambio externo y las infracciones de la política DLP, y aunque un 78% aseguran tener visibilidad de los inicios de sesión de los usuarios, solo el 58% tiene visibilidad de las descargas de archivos. Además, un 11% no tiene una solución de control de acceso desde el móvil a los recursos alojados en la nube, lo que le permite el acceso a cualquier teléfono inteligente o tableta, con el consiguiente riesgo de seguridad.

¿Sabes lo que ocurre en la nube?, ¿sabes dónde y cómo viajan tus datos?, ¿quién accede a ellos y desde dónde?, ¿qué aplicaciones están utilizando tus empleados y cómo las están utilizando? Estas son algunas de las preguntas que se han respondido en un webinar que bajo el título Seguridad y Cloud, ¿qué nos queda por aprender? ha celebrado IT Digital Security y en el que han participado Víctor Molina, Team Leader Security Engineers de Check Point España; Pedro García Villacañas, Director Preventa de Kaspersky Lab; Samuel Bonete, Director General de Netskope Iberia; José María Cayuela, Security Sales specialist de Akamai; Manuel

¿Te avisamos del próximo IT Digital Security?



Sánchez, especialista de ventas de Networking de Citrix; Ignacio Gilart, CEO de WhiteBearSolutions; Eutimio Fernández, director de ciberseguridad en Cisco España y José Manuel Canelada, Presales System Engineer de Infoblox.

Check Point

El 60% de las empresas españolas están adoptando soluciones cloud, dice Víctor Molina, Team Leader Security Engineers Check Point España, añadiendo que “la gran mayoría de las empresas consideran la seguridad como un barrea cuando hablan de este tipo de estrategias”.

La facilidad de migración de aplicaciones al cloud es una de las razones por las que las empresas adoptan este tipo de entorno; “lo que antes llevaba semanas de entregar ahora lleva muchos menos tiempo y la clave está en minutos de forma segura y minutos de cualquier manera”, asegura el ejecutivo de Check Point.

Lo que se plantean las empresas es quién tiene la responsabilidad de la seguridad de la nube. Y la respuesta es que depende del tipo de entorno. Se habla de responsabilidad compartida en la que el proveedor del cloud y el cliente tienen más o menos





peso en la seguridad; en todo caso y simplificando, mientras que el proveedor es responsable de la seguridad de la infraestructura, el cliente lo es de lo que lleve a esa infraestructura; “por ejemplo, el correo electrónico es un ejemplo de solución de SaaS donde la seguridad está a cargo del cliente”.

Habla Víctor Molina de “seguridad tradicional y seguridad evolucionada con el cloud”, explicando que, en el segundo caso, en un entorno cloud, es más fácil desplegar seguridad y conseguir una seguridad inherente por defecto.

¿Qué pasos mínimos tenemos que plantearnos cuando queramos hacer frente a la seguridad del cloud? El primer paso, dice el ejecutivo de Check Point, es controlar el perímetro mediante soluciones de amenazas avanzadas. Y puntualiza que, ya que las empresas suelen contar con soluciones avanzadas en entorno on premise, “no las quitamos por

¿Te avisamos del próximo IT Digital Security?

irnos a un entorno cloud”. Un segundo paso es proteger las comunicaciones dentro del propio entorno porque las comunicaciones este-oeste, no pueden quedar desatendidas. También hay que tener en cuenta que la adopción de la nube nos está llevando a un cloud híbrido, y hay que dedicar esfuerzos a saber manejarlo de manera consistente. “Como último punto, la seguridad debe ser adaptativa, ajustada al entorno, que se adapte a los cambios”, dice Víctor Molina.

Preguntamos al experto en seguridad si GDPR, ya de obligado cumplimiento, está impulsando la adopción de seguridad en la nube. Responde asegurando que la normativa de protección de datos está generando muchas conversaciones en torno a la seguridad y cómo hacerla frente; “una de las preocupaciones relacionadas con la seguridad en la nube es quién accede a la información, por qué canales se envía...”.

"Tenemos que entender qué tipo de entornos tenemos para saber quién tiene la responsabilidad de la seguridad en la nube, que siempre es compartida"

Kaspersky Lab

“Aquellos que tenían cierta concienciación y madurez de forma seria y aportando recursos”, dice Pedro García Villacañas, director preventa de Kaspersky Lab, cuando le preguntamos cómo están haciendo frente las empresas a la seguridad en la nube.

La tendencia, explica el ejecutivo, es que una parte de la infraestructura y los servicios van a seguir estando en la nube privada y otra se lleva a la nube pública, creando un concepto, nube híbrida, que es donde convergen ambas tendencias.

La situación supone un desafío a la hora de proteger las diferentes tecnologías que estemos utilizando, sin olvidarnos que al mismo tiempo “nos genera la necesidad de ser más eficientes para poder gestionar todo esto”.

Dice Pedro García Villacañas que una seguridad en la nube inadecuada significa mucho más que



Víctor Molina,

Team Leader Security Engineers Check Point España

"Una seguridad en la nube inadecuada significa mucho más que simplemente una protección débil"

Pedro García Villacañas, Director Preventa Kaspersky Lab Iberia

simplemente una protección débil. Como ejemplo, un aumento de la complejidad de la infraestructura puede suponer la reducción de la visibilidad. Hay que tener en cuenta que malware y el ransomware atacan tanto endpoints físicos como virtuales, que una ciberseguridad deficiente lleva a problemas de incumplimiento y que, en general, una seguridad diseñada ineficazmente deriva en procesos de sistemas ineficaces.

En enfoque de Kaspersky ha sido lanzar al mercado una nueva solución, Kaspersky Hybrid Cloud Security, compuesta por una serie de productos que están consolidados como los productos para proteger servidores Windows, tanto físicos como virtuales, así como la solución para proteger endpoint de Linux. "Nuestra prioridad ha sido la de siempre, que sea ágil y simple, y que nos permita proteger cualquier vector de ataque y cualquier amenaza. Y eso lo hacemos incorporando todas las tecnologías de detección, y de control y gestión que tienen nuestras soluciones", explica Pedro García Villacañas, añadiendo que también se ha tenido en cuenta que se pueda

gestionar de una manera centralizada desde una única consola que permita acceder a diferentes escenarios.

Kaspersky Hybrid Cloud Security está compuesto de varios productos: Kaspersky Security for Windows Server, Kaspersky Security for virtualización, tanto en la versión agenteless como en light agent, y Kaspersky Endpoint Security for Linux, todo ello gestionado desde una única consola y que además sólo te tienes que preocupar de adquirir una licencia. De esta manera, se busca "aportar



una protección lo más integral posible de la forma más fácil y simple".

Sobre si GDPR está fomentando la adopción del cloud, dice el director preventa de Kaspersky Lab que "una de las cosas buenas que la normativa ha aportado al mundo de la seguridad es que ha propiciado, si no la había ya un poco más concienciación sobre la protección del dato y la información".

Netskope

Asegura Samuel Bonete, director general de Netskope Iberia, que la situación actual es completamente diferente a la que teníamos años atrás: la seguridad perimetral ya no es suficiente porque hay comunicaciones que se producen en la nube sin pasar por ese perímetro.

Netskope es una compañía experta en CASB (Cloud Access Security Manager), que permite controlar el acceso a las aplicaciones en la nube. Netskope XD es una solución "que nos permite detectar la actividad, el trasiego de información, e incluso las amenazas dentro de los entornos cloud".

Asegura el directivo que las grandes empresas utilizan una media de mil aplicaciones en la nube, muchas de las cuales no están controladas por los departamentos de IT, y que en un 70%



"De media las empresas utilizan más de mil aplicaciones cloud en un entorno de gran cuenta, y en cerca del 70% se pierde la propiedad intelectual"



Samuel Bonete,
Director General de Netskope Iberia

de los casos, su uso implica la pérdida de la propiedad intelectual de la información que se utiliza en esa aplicación (convertidor de PDFs, transferencia de ficheros...).

Los departamentos de TI necesitan recuperar el control y para ello lo primero que tienen que hacer es descubrir las aplicaciones; "se darán cuenta que tienen tres tipos de aplicaciones: las reguladas por IT, sobre

loas que se tiene cierto control que van a necesitar potenciar. Sobre el resto de aplicaciones, se van a encontrar con las que por naturaleza son inseguras y tendrán que bloquear y el resto, que no son tan malas y son fundamentales para tu negocio, pero que se tienen que habilitar de forma".

Explica Samuel Bonete que hay que habilitar de forma segura los servicios cloud necesarios, y que el matiz importante es sobre cuántas aplicaciones se es capaz de hacerlo. En el caso de Netskope XD "somos capaces de aplicar grano fino de control en las más de 3.000 aplicaciones".

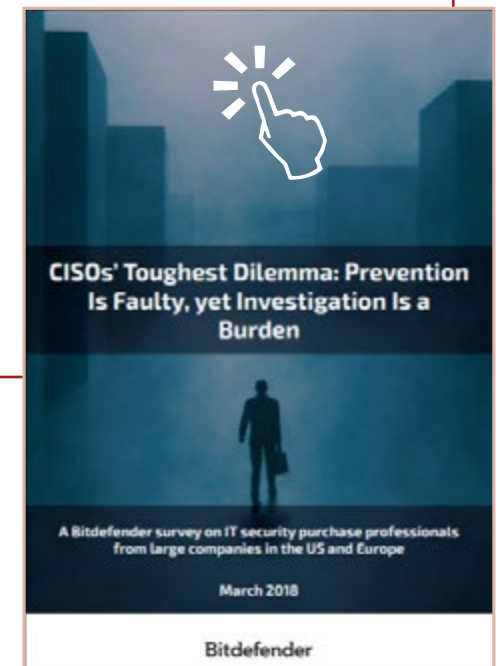
Hasta aquí el SaaS, el software as a Service, las aplicaciones, pero e cloud es también IaaS, o Infraestructura as a Service, y la navegación web. "Todo lo que es control de navegación o acceso a IaaS son también preocupaciones para nosotros", asegura el responsable de Netskope en España.

En la part de web se ha desarrollado un servicio de navegación segura, un proxy Gateway en nube de forma que se puede controlar la navegación de los usuarios cuando están fuera, pudiendo tener



EL DILEMA DE LOS CISO, PREVENCIÓN VS INVESTIGACIÓN

EDR está experimentando un crecimiento sólido. Los analistas dicen que el principal factor de crecimiento es que las empresas necesitan visibilidad y detección adicionales. Las soluciones de detección y respuesta de puntos finales no solo ayudarán a los CISO a proteger su infraestructura contra sofisticadas amenazas cibernéticas, facilitarán la detección temprana y recopilarán inteligencia, sino que también brindarán visibilidad a los ataques furtivos, lo que permite una contención rápida.





el control de a qué acceden, qué hacen, y desde dónde acceden.

¿Crees que este es el año de CASB? Sí lo creo porque en España estamos en la misma situación que había en Estados Unidos hace dos o tres años, cuando CASB empezó a explotar.

Akamai

Akamai es una compañía que nace en el mundo de la cloud, creada para entregar tráfico de internet donde. Hoy en día la compañía cuenta con una plataforma que consta de más de 200.000 servidores, 2.800 localizaciones, más de 1.600 redes y prácticamente en todos los países. “A nuestra plataforma se conectan cada día millones de seres humanos y millones de cosas”, asegura José María Cayuela, Security Sales specialist de Akamai, que es responsable de entregar alrededor del 30% del tráfico web

¿Te avisamos del próximo IT Digital Security?

mundial lo que da esta compañía una visibilidad muy grande de lo que está pasando en internet.

“Contamos con dos plataformas para defendernos de los ataques, uno que va a capa 7, que es la plataforma inteligente de Akamai, y Routed Platform que tienen siete Scrubbing center y que va a crecer hasta los 18”, dice el experto en seguridad de Akamai.

Según el informe de Akamai correspondiente al último trimestre del año, los ataques que van a la capa de aplicación, que buscan información, crecen un 10% anual. Los ataques que van contra la infraestructura, lo que suele ser una denegación de servicio tácita, también siguen creciendo año a año.

Explica el directivo que el tamaño de los ataques ha sufrido una evolución. En 2017, tras ponerse remedio a ataques detectados en 2016, el tamaño de los ataques, que no la cantidad, se redujo y, sin embargo, 2018 arrancó con un ataque de 1,5TB. ¿Qué papel tienen los botnets en todo esto? El hecho de que haya botnets buenos y malos hace que la si-



tuación no esté clara. Habla José María Cayuela de “una escala de grises”, y explica que en función de cada caso de uso las botnets tienen una sofisticación; “en cosas complejas, ligadas contra el fraude, como el robo de credenciales, intentan parecerse lo más posible a un ser humano”.

Explica el experto en seguridad de Akamai que según han ido evolucionando las tecnologías de

"No todas las redes de botnets son malas, las hay buenas y las hay malas, y en función del caso de uso tienen una sofisticación diferente"

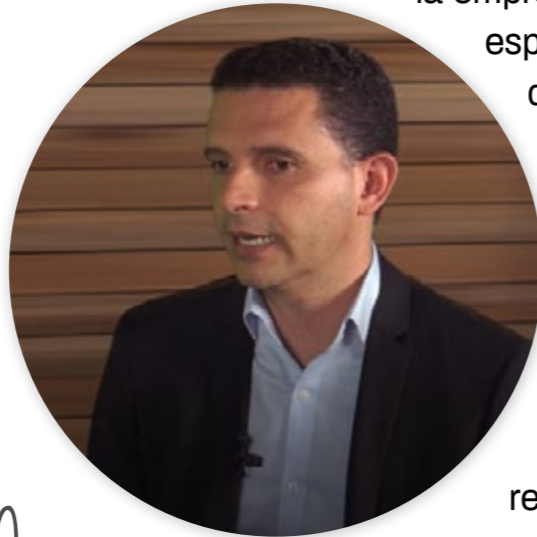
José María Cayuela, Security Sales specialist Akamai



detección de botnets, estas intentan parecerse cada vez más a un ser humano, haciendo parecer que sus peticiones son legítimas. Para su detección Akamai utiliza técnicas de telemetría. "La cadencia no es la misma si eres un bot o un ser humano, si la botnet está intentando simular que está utilizando un dispositivo móvil, este dispositivo no está quieto y el osciloscopio puede detectarlo, y debe haber presión sobre la pantalla Todo eso se utiliza para saber si es un ser humano o no", dice Cayuela.

"Los cuatro puntos a tener en cuenta para hacer frente a la seguridad del cloud son Consolidación, Protección del dato en SaaS, garantizar la identidad del usuarios y visibilidad y analítica"

Manuel Sánchez, especialista de ventas de Networking de Citrix



La propuesta de Akamai ha sido la de evolucionar la entrega de tráfico y las medidas de seguridad a la par. En función de cuál sea la tecnología o vector de ataque cuenta la compañía con una serie de elementos de protección, bien sea ataque HTTP/S, ataques DDoS, ataques contra el DNS, o contra el abuso de credenciales.

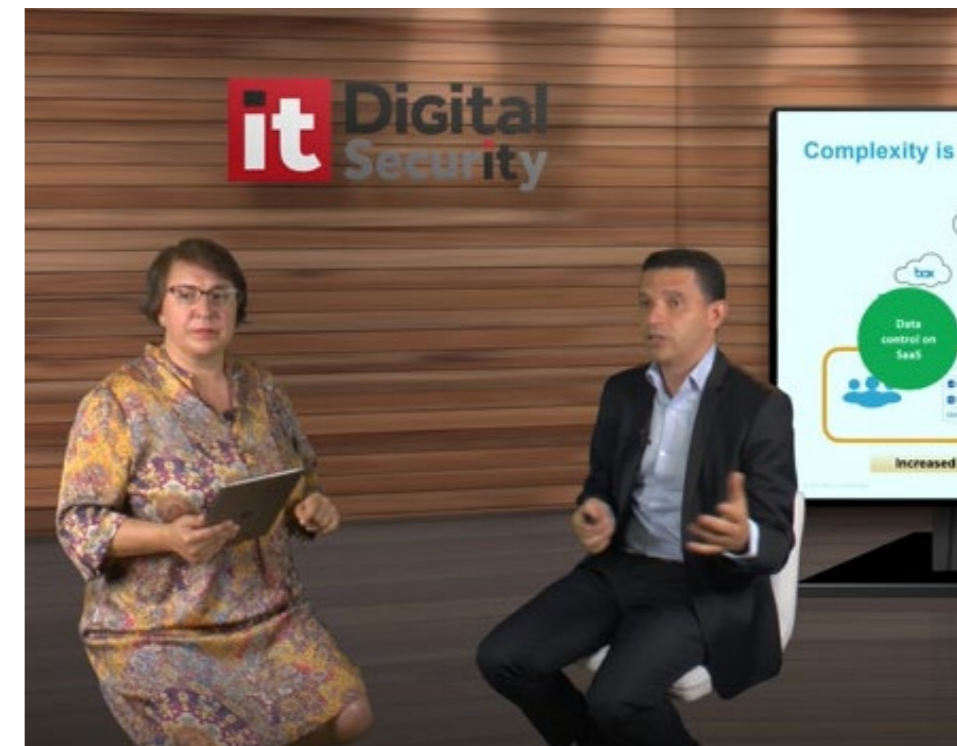
Citrix

Asegurando que la adopción del cloud crece entre la empresa española Manuel Sánchez, especialista de ventas de Networking de Citrix, asegura que la complejidad es el mayor enemigo de la seguridad. Explica el directivo que hasta ahora la seguridad se centraba en un perímetro detrás del cual estaba todo, pero ahora las aplicaciones se han ido a la nube. Y esto genera retos porque el control del dato se escapa del control del datacenter, a lo que se suma el problema de dar un acceso fácil a esas aplicaciones. "Esto conlleva la existencia de diferentes políticas de seguridad, múltiples endpoints y una visibilidad limitada", dice Manuel Sánchez.

Llegado a este punto, se requiere de una seguridad holística que contemple un único punto de acceso, políticas consistentes, control sobre las aplicaciones y, muy importante, visibilidad y conocimiento sobre lo que está ocurriendo en la nube, quién está accediendo a qué datos y desde dónde.

La solución de seguridad de accesos de Citrix proporciona consolidación, de todos los accesos a las aplicaciones aplicando además un Single Sign-on. También ofrece protección de dato, controlando las copias o impresiones no autorizadas y protegiendo la propiedad intelectual. "También es importante la parte de autenticación de los usuarios, así como la parte de visibilidad y analítica, donde Citrix está haciendo foco", explica especialista de ventas de Networking de Citrix.

La propuesta de la compañía para asegurar el cloud se concreta en Citrix NetScaler Unified Gateway, NetScaler Gateway Service y Citrix Access Control. El primero permite consolidar los accesos remotos, lo que no sólo mejora la eficiencia sino reduce la superficie de ataque, ofrece soporte a todos los dispositivos y mejora la visibilidad. El



Single Sign-On mejora la experiencia de usuarios al ofrecer un acceso consistente a todas las aplicaciones.

NetScaler Gateway Service, la parte de Netscaler Gateway como servicio, donde lo más importante son las funcionalidades añadidas para la entrega de aplicaciones. "Con Citrix Access Control lo que buscamos es mejorar la experiencia de usuarios", dice Manuel Sánchez, añadiendo que se hace entrega de un navegador para que aíse la navegación en entornos que no admite la ejecución y mejorando la protección.

WhiteBearSolutions

Qué tipo de dato están almacenando en el cloud, en qué tipo de cloud lo están haciendo, qué tipo de políticas están aplicando en ese cloud, qué tipo de tratamiento tienen que hacer de las identidades de esos accesos a ese cloud y sobre todo aquello que tenga que ver con el ámbito normativo son, en

"Las empresas deben plantearse seriamente cómo hacer un uso eficiente, normalizado y seguro del cloud"

Ignacio Gilart, CEO de WhiteBearSolutions



opinión de Ignacio Gilart, director general de WhiteBearSolutions, los elementos a y tener en cuenta por las empresas cuando quieran hacer frente a la seguridad en la nube.

La propuesta de la compañía, con 15 años de experiencia y que ofrece soluciones de seguridad basadas en OpenSource y estándares, gira en torno al pilar de la protección del dato, "el activo de la empresa que hay que proteger". Se trabaja en dos líneas de negocio principalmente: por un lado, una suite de almacenamiento y backup, y por otro en una suite de identidad y gestión de acceso. Y alrededor de todo hay diferentes soluciones para hacer frente a la seguridad del cloud.

Las suites se componen de tres productos. En el caso de almacenamiento y backup un producto llamado WBSAirback "y en el caso de gestión de identidad y gestión de accesos tenemos dos productos dentro del mismo appliances que son WBSVision y SmartLogin".

WBSVision es una nueva generación en los sistemas de gestión de identidades, que permite a través de sus múltiples módulos, provisionar y controlar el acceso de usuarios a aplicaciones on-premise y on-cloud, en base a perfiles, roles y reglas de negocio, así como establecer políticas globales de contraseñas comunes a dichas aplicaciones.

SmartLogin por su parte es una solución de Gestión de Accesos que da respuesta a uno de los problemas más habituales de los usuarios en una organización: la identificación y el acceso seguro con una sola contraseña a aplicaciones web on-premise y en la nube.

Y finalmente WBSAirback, una solución de nueva generación de Almacenamiento y Backup que da respuesta a uno de los problemas más habituales en una organización, la protección con una sola plataforma de servidores y puestos de trabajo, multiplataforma.

Sobre si este 2018 va a ser el año de la adopción definitiva de la seguridad cloud, dice Ignacio Gilart que "no nos va a quedar más remedio". Y ya



Algunos datos

64%	62%	81%	72%
Organizaciones que pueden identificar la actividad de sus usuarios con un único logueo.	Empresas que creen que su gestión de usuarios es completa y eficaz de gestión.	Incidentes de seguridad por robo o pérdida de contraseñas.	De las organizaciones que utilizan SSO para su planificación.
50%	61% - 83%	50%	55%
Organizaciones que utilizan un único logueo para sus usuarios.	De las empresas que creen que su gestión de usuarios es completa y eficaz de gestión.	Organizaciones que utilizan SSO para su planificación.	De las organizaciones que utilizan SSO para su planificación.



"En 2022 dejaremos de referirnos a Cloud computing como algo excepcional, y local computing pasará a ser el modelo menos extendido"

Eutimio Fernández, Director de ciberseguridad en Cisco España

no sólo por las sanciones, sino porque todas las ventajas que nos da el cloud para ser más competitivos, "nos lo puede dar de desventaja si no estamos seguros, con lo cual es una variable que tiene que estar ahí".

CISCO

"En España la adopción del cloud está siendo una explosión", asegura Eutimio Fernández, director de ciberseguridad en Cisco España. Dice el directivo que las arquitecturas on premise se van a descargar muchísimo y en 2022 dejaremos de referirnos a Cloud computing como algo excepcional



y local computing pasará a ser el modelo menos extendido.

Sobre quién es el responsable último de la seguridad del cloud, "depende del servicio que estés contratando. Al principio había mucha polémica, pero siempre es una responsabilidad compartida", explica Eutimio Fernández, asegurando también que porcentaje de responsabilidad estará medido por el servicio que contratemos. En todo caso es crítico, y por eso la evolución de los CASB, "siempre será responsabilidad nuestra los usuarios y los datos".

La propuesta de cisco para securizar el cloud es Stealwatch, CloudLock y Umbrella. Stealwatch es "la solución que tenemos para utilizar la red como un sensor". Se trata de una solución que tiene una parte que va directamente a la nube, que es



Stealthwatch for Cloud y hacemos uso de toda la información “que nos están dando los proveedores de infraestructura como servicio para hacer lo que ya hacemos en red: saber qué usuarios tenemos, cómo se están hablando, si hemos hecho bien la segmentación, modelizamos comportamiento de los usuarios, de los sistemas, de las comunicaciones, identificamos si hay malware corriendo por mi cloud, etc.”.

Y como está todo integrado, cuando se monitoriza la infraestructura, da lo mismo se tanga on premise o en cloud, se monitoriza la infraestructura esté donde esté, “y esa es la propuesta de cisco que tenemos para la infraestructura, que viene por Stealthwatch, y luego nos vamos a la parte que es nuestra responsabilidad que es la parte de CloudLock”.



Con CloudLock las empresas serán capaces de monitorizar todo, actividad de usuarios y datos en todos los sentidos: qué tipo de datos tenemos, qué usuarios acceden a ellos, qué otras aplicaciones se conectan a mis aplicaciones cloud.

Y desde aquí falta el control de acceso a la nube para garantizar que sea seguro, que vaya por donde debe y que los usuarios tengan la seguridad necesaria cuando acceden al cloud desde cualquier parte, “que es algo que solucionamos con Umbrella”, aplicado al DNS porque es una primera barrera de la que todo el mundo tiene que hacer uso. “Al DNS acceden aplicaciones, acceden servicios, acceden usuarios, dispositivos IoT... y el DNS nos cubre todo”, dice Eutimio Fernández.

¿Es este el año de Cloud Access Security Broker (CASB)? Dice Eutimio Fernández que llevamos varios años hablando de CASB y que aún no lo hemos visto arrancar del todo. El mercado, muy fragmentado hace pocos años se ha consolidado mucho, “podemos quedar cuatro o cinco de cara al mercado y esperamos que sí durante 2018 o 2019 podamos decir que el CASB arranque.”

"Existen una serie de retos desde el punto de vista de seguridad cuando vamos a la nube, como la pérdida de visibilidad, de contexto y de automatización"

José Manuel Canelada,
Presales System Engineer de Infoblox



Infoblox

Las empresas están adoptándolo desde diferentes puntos de vista. Las empresas adoptan una transformación digital primero y luego el cloud como una consecuencia de esa transformación digital, que nos lleva a la economía digital, asegura José Canelada, Ingeniero de sistemas de Infoblox.

El incremento del número de dispositivos conectados a internet ha aumentado mucho, también el número de usuarios con acceso a la

Compartir en RRSS




red, y sobre todo hemos incrementado el número de datos. ¿Qué nos ha hecho poder afrontar esta transformación? La velocidad del acceso se ha generalizado completamente, el descubrimiento del big data con el machine learning y la inteligencia artificial “que nos ha llegado a un nivel de interacción con el IT que nunca habíamos tenido hasta ahora”, dice José Canelada.

El datacenter ha cambiado, se ha transformado y también los recursos que se utilizando de ellos. Consecuencia directa es que existen muchos tipos de cloud. La seguridad se transforma de forma completamente dramática con la pérdida y control

del perímetro. Existen diferentes retos generados por este cambio: el primero son los silos de seguridad, “seguimos teniendo diferentes entornos con diferentes soluciones de seguridad para proteger contra diferentes amenazas, pero sin interrelación entre ellas”, dice el ingeniero de Infoblox; la pérdida de visibilidad, pérdida de contexto y pérdida de automatización son los otros retos.

La propuesta de Infoblox es buscar elementos que permitan unificar, como el DNS. “Cuando hablamos de aplicaciones cloud, el 99% van a utilizar el DNS”, lo que convierte al DNS en un elemento completamente horizontal en la seguridad cloud. El gran reto de la seguridad en el DNS es que ahora ahora el DNS ha estado completamente oculto para todos los administradores; era un elemento que se utilizaba para la conectividad, no para la seguridad.

Existen tres factores fundamentales en los que Infoblox puede ayudar. El primero es la protección de la infraestructura, el segundo la protección de datos y mitigación de malware y el tercero centrado en la eficiencia y optimización en las operaciones de seguridad basadas en contexto. “Apostamos por compartir la inteligencia que tenemos desde el DNS porque el primer acceso de esa aplicación maliciosa lo tenemos nosotros, compartámoslo con el resto de elementos”, reflexiona José Canelada.

Sobre si GDPR está impulsando la adopción de soluciones de seguridad en la nube, dice el ingeniero de Infoblox que la normativa “nos está obligando a trabajar a todos los elementos de seguridad juntos. Comparte esa información, utiliza el contexto”. 

Enlaces de interés...

W [20 casos de usos de CASB](#)

W [Diez consejos sobre a gestión de bots](#)

W [Qué es una solución EFFT](#)

W [Kaspersky Hybrid Cloud Security](#)

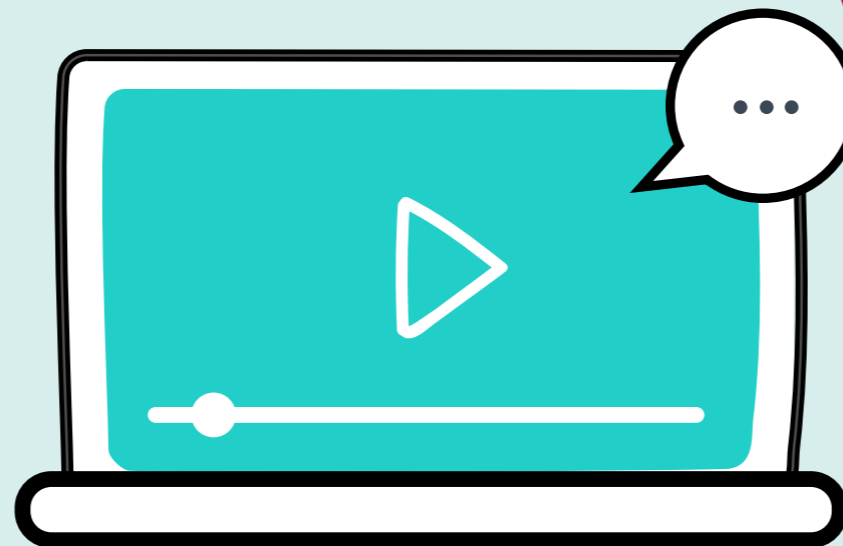
I [Las brechas de seguridad cloud hacen peligrar las estrategias de digitalización](#)

I [IoT, movilidad y cloud, entre las tecnologías que ponen a prueba la seguridad de las empresas](#)

I [La seguridad en la nube: ¿reto o ventaja para la empresa?](#)



Próximos #ITWebinars



www.ittelevision.es



**Resolviendo
los retos de IoT**

JULIO

Registro



**Inteligencia de amenazas.
¿a qué esperas?**

SEPTIEMBRE

Registro



**Dando forma al Big
Data para la toma
de decisiones**

Registro



OCTUBRE

Bots, ¿amigos o enemigos?

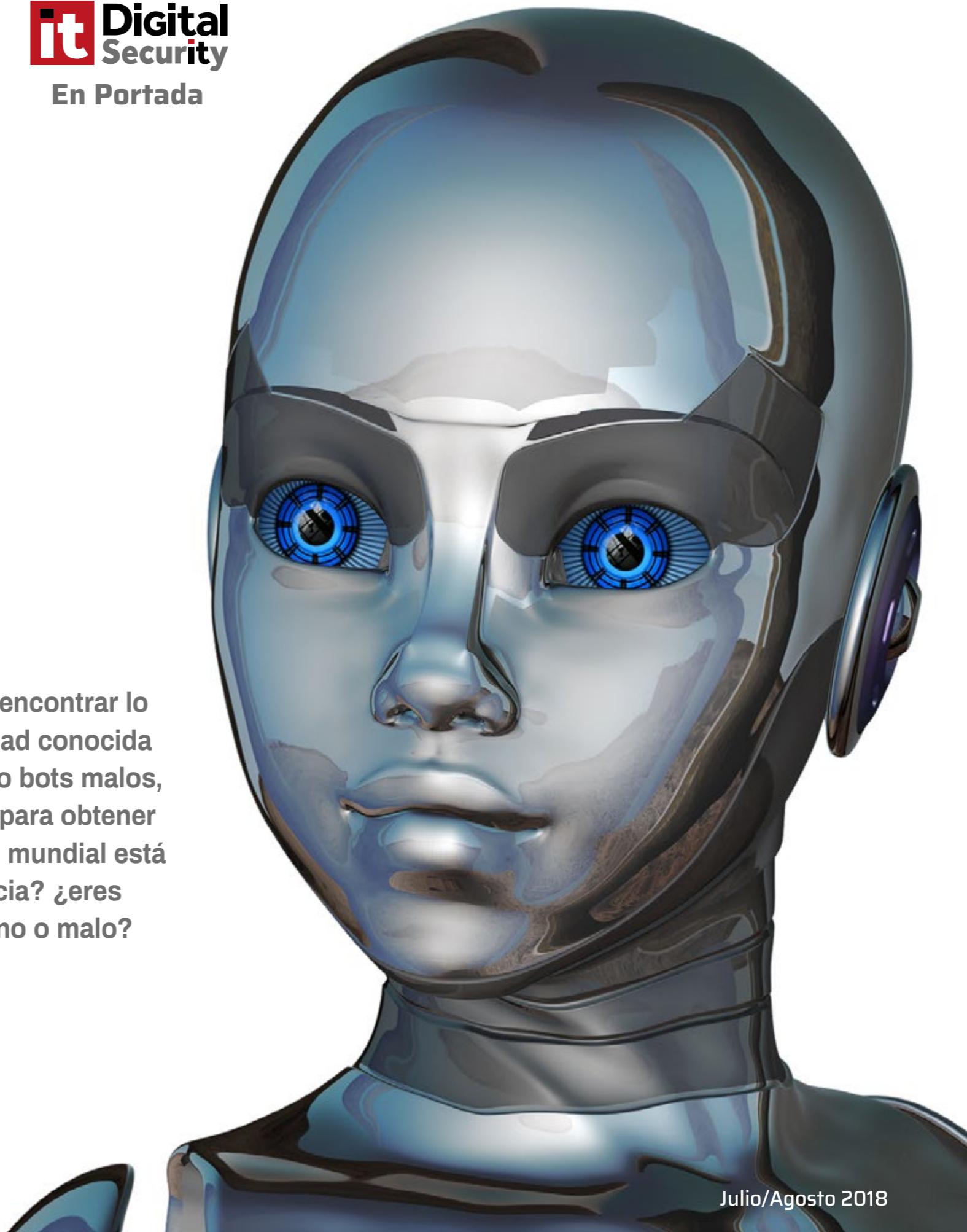
Si bien un bot bueno puede ayudar a los clientes a encontrar lo que buscan, sea un mejor precio o una vulnerabilidad conocida para su detección y parcheo, existen los bad bots, o bots malos, que se dedican a robar datos de sitios sin permiso para obtener una ventaja competitiva. Más de la mitad del tráfico mundial está generado por bots, ¿eres consciente de su existencia? ¿eres capaz de detectarlos? ¿y de saber si es un bot bueno o malo?

Compartir en RRSS



¿Te avisamos del próximo IT Digital Security?

Julio/Agosto 2018



Un bot, abreviatura de robot, es un tipo de aplicación de software o script que realiza tareas por comando, como indexar un motor de búsqueda, y son realmente buenos para realizar tareas repetitivas. Hay bots buenos, y bots malos que realizan tareas maliciosas y permiten a un atacante tomar el control del sistema afectado de forma remota.

Un uso típico de bot bueno es recopilar información. Los robots que se dedican a estas tareas se les conoce como rastreadores web, o web crawlers.



Otro uso positivo de los bots es en entornos mensajería instantánea, o chat de. La interacción dinámica con los sitios web es otra forma de utilizar los bots para fines positivos.

En cuanto a los bad bots, se utilizan para propagar malware que infecta el sistema que lo aloja, host, y se conecta a un servidor central desde el que recibe instrucciones. Se habla entonces de botnets, o redes de máquinas comprometidas, utilizados para lanzar ataques de denegación de servicio, reunir contraseñas, envíos masivos de spam, explotar puertas traseras abiertas por virus y gusanos, etc.

A finales del año pasado [Radware publicaba un estudio](#) en el que aseguraba que los bots son responsables de más de la mitad (52) del tráfico web mundial. Es más, para algunas organizaciones los bots representan más del 75% de su tráfico, un porcentaje significativo si se tiene en cuenta que una de cada tres organizaciones no es capaz de distinguir entre los bots buenos y los malos.

El problema de los bots afecta de manera diferente dependiendo del vertical. En el caso del Retail, los bots se han convertido en una herramienta imprescindible para los sites de agregación de precios, cupones, chats para atender a los clientes, etc. El 41% de los retailers aseguran que el 75% de su tráfico es generado por bots, pero no son capaces de diferenciar cuando el tráfico es de un bot dañino o cuándo un atacante está tomando ventaja de estos bots para lanzar ataques de web Scraping y robar propiedad intelectual, bajar los precios o comprar inventario

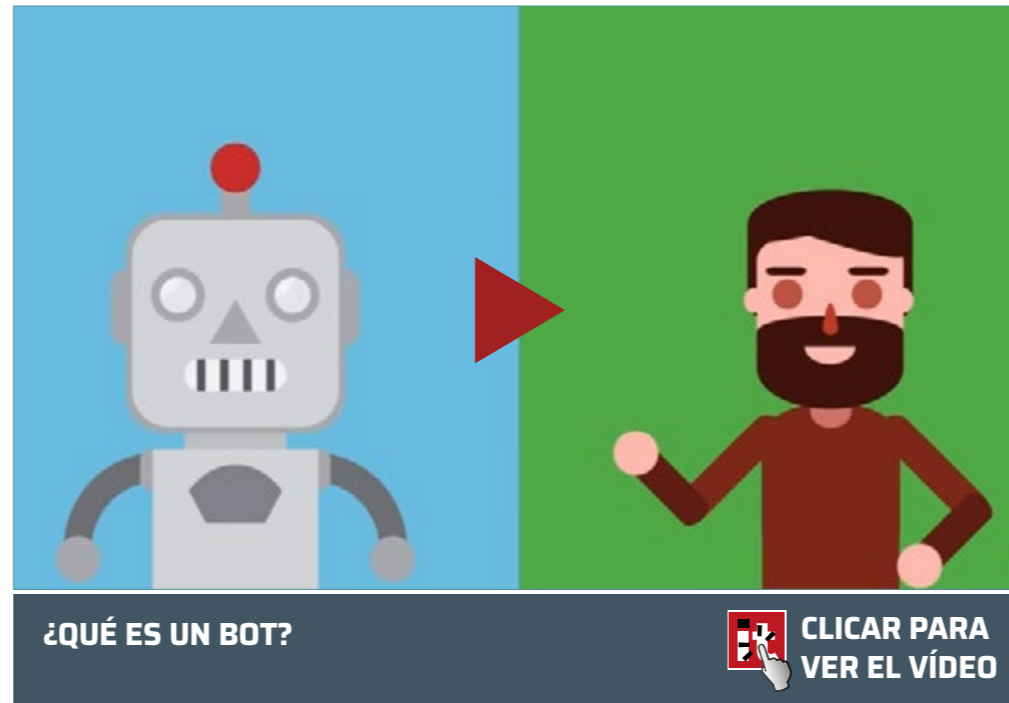


"Las botnets IoT están creciendo tanto en tamaño como en impacto, y son cada vez más capaces de desencadenar potentes ataques que podrían afectar gravemente a Internet"

Eutimio Fernández, Director de Ciberseguridad en Cisco España

para revenderlo por canales no autorizados. También se enfrenta el mundo del retail a picos en la demanda, coincidiendo con determinadas campañas. Lanzar un ataque que involucre miles, o decenas de miles de bots, puede ser un desastre financiero.

En el mundo de la salud el problema es similar: el 42% del tráfico está generado por bots, pero sólo el 20% de los responsables de seguridad TI serían capaces de identificar el que generan los bad bots. Más de la mitad (55%), dicen que no tienen forma de rastrear los datos compartidos con un tercero después de abandonar la red corporativa.



jan código malicioso y otros ataques cuyo objetivo es realizar fraude o robar contenido confidencial.

“Las botnets utilizadas con fines maliciosos se están convirtiendo en una commodity, siendo sumamente fácil y barato crearse una propia o alquilarlas”, dice Ángel Noguerras, Senior Technical Account Manager de Akamai, quien explica que dependiendo del uso que se le quiera dar, hay tipos de ataques que buscan pasar desapercibidos, mientras que otras son utilizadas para realizar ataques de DDoS. “Estas últimas son las que más preocupan si hablamos de tráfico de red, pues hay muchísimos dispositivos comprometidos en Internet formando

parte de estas redes de bots y pueden generar muchísimo tráfico”, asegura Noguerras.

Luis Miguel Cañete, director de Canal para España y Portugal de F5 Networks señala que los thinbots, construidos exclusivamente con dispositivos IoT, se están convirtiendo en el sistema preferido



Para Eutimio Fernández, director de Ciberseguridad en Cisco España, los bots tienen un gran impacto en la seguridad de las empresas, “especialmente si se utilizan en modo red (botnets) para ataques de Denegación de Servicio (DDoS)”. Asegura también el directivo que además de las denegaciones de servicio distribuidas, hay botnets que alo-

“En la identificación, análisis y eliminación del tráfico procedente de bots maliciosos es imprescindible contar con soluciones de seguridad de última generación, entre las que destacan los firewalls avanzados de aplicaciones web (AWAF)”

Luis Miguel Cañete, Director de Canal de F5 Networks Iberia

Algunas amenazas que un bad bot puede generar

Como hemos visto a lo largo de este reportaje, los bots buenos son, principalmente recolectores de información. Hacen su trabajo de manera efectiva, pero generalmente solo reúnen datos suficientes para completar sus tareas asignadas. Por su parte, los bad bots son una amenaza constante, y su principal directiva es atacar objetivos grandes y exitosos. Y a medida que un sitio web se vuelve más popular, también lo hace el incentivo para atacarlo.

Los propietarios de los sitios web deben ser plenamente conscientes de que los bad bots acechan en cada esquina: buscan robar su contenido, abusar de la funcionalidad, alterar las métricas del sitio y cometer fraude. Algunas de las actividades que pueden realizar los bots malos y que pueden impactar en sus webs:

- **WEB SCRAPING:** robo de contenido, extracción de datos y modificación de precios. Hay bots que recorren Internet pueden dedicarse a recopilar contenido que colocan en otros sites, lo que reduce el posicionamiento de su web en Google. Las empresas de comercio electrónico son un objetivo obvio. Cuando los bots extraen el precio y la información del producto, los datos agregados se alimentan a un motor de análisis, lo que permite a los competidores hacer coincidir precios y productos en tiempo casi real, de forma que pueden anular ofertas y promociones.
- **SKEWING, O MEDICIONES ERRÓNEAS.** Cada interacción de bot, sin importar lo que haga, sesga las métricas asociadas con ese negocio. Debido a que el número de bots que operan en Internet es tan

significativo, las decisiones comerciales basadas en tales métricas son obviamente defectuosas. Desde otra perspectiva, los operadores de bot pueden alterar fácilmente la reputación de alguien, influir en los demás o ganar notoriedad en línea, especialmente a través de las redes sociales.

- **DESCIFRADO DE CREDENCIALES.** Se trata de una técnica practicada por los operadores de bot cuando tienen un nombre de usuario conocido, pero necesitan adivinar la contraseña que lo acompaña. Usan técnicas de fuerza bruta contra procesos de autenticación de aplicaciones para llegar a la pieza de credencial faltante.
- **DDOS, O DENEGACIÓN DE SERVICIO DISTRIBUIDO.** Si el tráfico de su página de inicio se triplica, es probable que pueda gestionarse, pero si va contra el carrito de la compra causa problemas ya que su aplicación web envía múltiples solicitudes a todos los componentes involucrados en cada transacción. Esto incluye ponerse en contacto con la base de datos de inventario, conectarse con el procesamiento de pagos y las herramientas de fraude, y usar herramientas de análisis para oportunidades de venta cruzada.

- **FRAUDE DE CLIC, O DE PAGO POR CLIC.** Este utiliza bots para hacer clic en una publicidad interactiva con la intención de inflar falsamente los beneficios del portal o la página web, pues la compañía anunciante paga en función de las veces que un usuario presione el ratón.
- **ESCANEO DE VULNERABILIDADES.** Los escáneres de vulnerabilidad son herramientas automáticas, o bots, que ejecutan pruebas contra un sitio web o una aplicación web, buscando identificar debilidades y posibles vulnerabilidades. Hay muchas herramientas disponibles como Metasploit, Burp Suite, Grendel Scan y Nmap.
- **FOOTPRINTING.** Se trata de un proceso mediante el cual los bots sondean las aplicaciones para identificar sus propiedades. Incluye pruebas para aprender tanto como sea posible acerca de la lógica, estructuras, algoritmos, funciones, métodos, configuración y otros secretos subyacentes de una aplicación. También puede determinar los puntos de entrada, denominados colectivamente como la superficie de ataque.
- **SPAMMING.** Los bots pueden rellenar tus formularios con datos basura. El spam puede agregar datos cuestionables o incluso maliciosos a contenido público y privado, bases de datos y mensajes de usuario. El spam en formularios, comentarios no deseados, registros falsos y las revisiones deshonestas de productos contaminan los sites. Para resolver este problema se crearon los CAPTCHA.



BAD BOT REPORT

Este informe investiga los ataques diarios que pasan furtivamente por los sensores y causan estragos en los sitios web. Se basa en datos de 2017 recopilados de la red global de Distil Networks, e incluye cientos de miles de millones de solicitudes de bots, anonimizadas en miles de dominios.

Los bad bots interactúan con las aplicaciones de la misma manera que lo haría un usuario legítimo, lo que hace que sea más difícil de detectar. Los Bots permiten el abuso, mal uso y ataques de alta velocidad contra páginas web y API. Permiten que atacantes, competidores y estafadores llevar a cabo una amplia gama de actividades maliciosas como la minería de datos competitiva, recolección de datos personales y financieros, adquisición de cuentas, fraude publicitario digital, correo no deseado, fraude de transacciones y más.



por los ciberdelincuentes debido a la escasa seguridad y facilidad de compromiso de estos dispositivos, que los convierte en un recurso sencillo y económico. “Hay que tener también en cuenta que los riesgos de botnets aumentan significativamente en entornos multcloud, escenario al que miran ahora muchas organizaciones por un motivo de necesidad operativa”, explica el directivo.

Coincide también Eusebio Nieva, director técnico de Check Point en los bad bots impactan en la seguridad de las empresas a diario; “algunos simplemente recopilan datos de las compañías, por ejemplo, para espiar las facturas que emite, y cambiar el número de cuenta en ellas para que se ingrese el dinero a los ciberdelincuentes. Otros los usan para enviar spam y ataques de phishing”. Recuerda Nieva que más de la mitad de los bot son maliciosos y que navegan por Internet robando da-

tos, suplantando la identidad de un usuario o infectando los dispositivos de sus víctimas para lanzar ataques de ransomware o DDoS, entre otros.

Cuando se le pregunta por el impacto que tienen los bad bots en el tráfico de red, Alberto Ruiz Rodas, Sales Engineer de Sophos, recuerda el impacto de la botnet Mirai, compuesta por miles de elementos IoT, y que generó importantes ataques de DDoS. “Ya ha ocurrido y, muy probablemente, volverá a suceder”, asegura el experto añadiendo que no sólo hay que pensar en cámaras IP, “pensemos en pulseras de actividad que también se conectan a WiFi, los miles de diferentes dispositivos para ‘cloudificar’ los diferentes elementos de una casa (bombillas, aires acondicionados, calefacciones, etc...). Una botnet que, además de realizar ataques DDoS pueda permitir al atacante ‘echar un vistazo’ a lo que hay en esa





"Desde hace ya unos años, los bots generan más tráfico de red que los humanos. Y de estos bots, más de la mitad son maliciosos, que navegan por Internet robando datos, suplantando la identidad de un usuario o infectando los dispositivos"

Eusebio Nieva, Director Técnico de Check Point para España y Portugal

red, podría acabar dando muchísimo rédito a su dueño".

Los dispositivos controlados por una botnet "pueden ser utilizados para almacenar contenido ilegal sin que el usuario lo sepa", dice Josep Albors, responsable de concienciación de ESET España. Y añade que además de los usos más conocidos, como enviar cientos de miles de correos electrónicos o lanzar ataques de denegación de servicio hacia objetivos concreto "también están siendo usados desde hace meses como 'mineros' involuntarios, haciendo que los delincuentes obtengan criptomonedas a costa de los recursos de los usuarios".

Conciencia empresarial

De forma que en un entorno digital como el actual, la amenaza de los bots afecta a los negocios de

múltiples formas: la calidad del servicio se resiente, la integridad de los datos pelagra y la reputación de las compañías queda en entredicho. En esta situación, evitar que un frigorífico o una cámara de seguridad se conviertan en armas al servicio de los ciberdelincuentes es responsabilidad de todos. De los usuarios, que deben preocuparse por la seguridad de sus dispositivos, de los fabricantes, que deben incorporar estándares que dificulten su hackeo y también de los proveedores de servicios que proporcionan conexión a estos dispositivos. Por supuesto, también de la Administración Pública, con la aprobación de normas que obliguen a todas las partes a asumir la responsabilidad que les corresponda.

En todo caso, preguntamos a nuestros expertos si las empresas son en realidad conscientes de la

existencia de los bots, si serían capaces de detectarlos.

Eutimio Fernández tiene claro que las empresas "son conscientes, aunque quizá no le prestan la atención adecuada, especialmente en el caso de las botnets IoT". Sin embargo, las botnets IoT están creciendo tanto en tamaño como en impacto, y son cada vez más capaces de desencadenar potentes ataques que podrían afectar gravemente a Internet. "El cambio de los atacantes hacia una mayor explotación de la capa de aplicación indica que este es su objetivo", dice el responsable de ciberseguridad en Cisco España.

Con respecto a la capacidad de detección, "todo depende de la actividad de la botnet. En muchos casos los bots no desvelan su presencia con altas tasas de escaneo que dañan la infraestructura de la

Bad Bots, un problema desde los '90

Para la elaboración de este reportaje hemos contado con la ayuda de un grupo de expertos, a lo que preguntamos desde cuándo se ha detectado la grave amenaza que representan los bad bots. Sus respuestas son las que siguen.

Josep Albors, ESET. Si obviamos el gusano de Morris en 1988, las primeras botnets maliciosas comenzaron a labrarse su reputación a finales de los 90 (con sub7 como ejemplo representativo) y principios de los años 2000. A finales de esa década ya había numerosas botnets con millones de dispositivos bajo su control y, aunque actualmente ya no suelen observarse botnets tan grandes como las de hace una década, la facilidad para obtener nuevas víctimas ha hecho que sean una amenaza muy presente y con un objetivo concreto: el Internet de las cosas.

Ángel Nogueras, Akamai. Los robots maliciosos llevan funcionando mucho tiempo, pero no siempre como los conocemos ahora. Al principio no eran más que una o muy pocas IPs haciendo muchas peticiones, cosa que era muy sencilla de parar con una regla de bloqueo en el firewall. Desde ahí, han

red; en su lugar, infectan las redes de una manera que escapa a la notificación inmediata. Y, en muchas ocasiones, utilizan también el cifrado”, explica Eutimio Fernández.

En opinión de Ángel Nogueras, de Akamai, hace tiempo que las empresas son conscientes de la

¿Te avisamos del próximo IT Digital Security?

ido evolucionando hasta las grandes plataformas que hemos visto formadas por nodos comprometidos en Internet.

Eusebio Nieva, Check Point. El primer ataque de bots data de los años 90, cuando eran populares los canales de chat IRC. Sin embargo, su auge fue en 2016, cuando Mirai cayó, entre otros, a Twitter. Desde entonces, nuestro equipo de investigadores encuentra cada vez más casos de redes de bots que se aprovechan del IoT para lanzar ofensivas contra empresas y países.

Alberto Ruiz Rodas, Sophos. Creo que Mirai fue un punto de inflexión. Ya se conocían las botnet desde hace años, pero Mirai demostró cómo un ejército de zombies “decréptos” (los IoT no se caracterizan por tener grandes capacidades de cómputo) podían causar problemas tan serios.

existencia de los bots, “sobre todo gracias a los ataques contra DynDNS y el más reciente contra GitHub, y gracias también a la publicación de software como Mirai (el responsable del ataque contra Dyn). Aun así, muchas empresas consideran que no sufren ataques de botnets y aún no se plantean



Eutimio Fernández, Cisco. Ya hace 10 años, Cisco calificó a las botnets como una de las principales ciber-amenazas. En ese momento, era el acceso de los consumidores a las conexiones de banda ancha las que otorgaban a las botnets la capacidad de lanzar los ataques de denegación de servicio. Hoy, los dispositivos no seguros del IoT son los culpables.

Luis Miguel Cañarte, F5 Networks. No existe un momento puntual sino una gradual conciencia del peligro de los bots a lo largo de los últimos años. Si bien, la evolución de IoT, con cada vez más dispositivos conectados, y la aprobación de legislaciones que obligan a las organizaciones a hacer públicos los ataques sufridos y sus consecuencias, con su correspondiente repercusión mediática, han sido factores decisivos en este sentido.





MIRAI, DENTRO DE UNA BOTNET IOT



CLICAR PARA
VER EL VÍDEO

de proporcionar respuestas a nuevas inquietudes, por lo que cualquier propuesta que se lance al mercado deberá abordar el aspecto de la seguridad, pero no de forma parcial, dando solución a problemas específicos, sino en su globalidad, teniendo en cuenta los múltiples factores que pueden estar relacionados con el concepto de seguridad. Esto supone claramente un cambio de paradigma, con relación a la forma en la que se venía procediendo hasta hace relativamente muy poco tiempo”, reflexiona Cañete.

Para Eusebio Nieva, a pesar de que cada vez existe una mayor concienciación sobre el malware y las amenazas avanzadas, “todavía muchas empresas no saben qué es una botnet, o cómo puede afectar a su negocio. Entonces, si no saben lo que es un bad bot, no pueden detectarlo”. Pero además añade el directivo de Check Point que, a día de hoy detectar un bad bot no es suficiente, sino que es necesaria la prevención de amenazas avanzadas, que impida que tanto este tipo de malware como otros entren en el perímetro de la empresa.

“Se es consciente del mismo modo que son conscientes del ransomware: saben que existe y piensan que muy raramente les puede afectar, hasta que les afecta y lamentan el no haber tenido

cómo defenderse contra ellas”, dice el ejecutivo, añadiendo que las empresas más conscientes o las que ya están sufriendo este tipo de ataques, fundamentalmente el sector financiero, hotel & travel y retail, se están dando cuenta de que no son capaces de detectarlos, sobre todo con los dispositivos on-premise.

Coincide Luis Miguel Cañete, de F5 Networks, con Ángel Nogueras al decir que las empresas son cada vez más conscientes de esta realidad. En cuanto a si son capaces de detectar esos ataques, “es algo que ni siquiera resulta sencillo para los expertos”, asegura el directivo, añadiendo que de lo que tienen que ser conscientes es que deben incorporar estrategias de seguridad con las que puedan proteger las aplicaciones, los datos y las redes. “La industria de TI va a tener que ser capaz



“Ya se conocían las botnet desde hace años, pero Mirai demostró cómo un ejército de zombies “decrépitos” (los IoT no se caracterizan por tener grandes capacidades de cómputo) podían causar problemas tan serios”

Alberto Ruiz Rodas, Sales Engineer
de Sophos Iberia



"Bueno o malo es un concepto muy complicado cuando hablamos de bots. Lo que para un cliente puede ser bueno, para otro puede no serlo"

Ángel Noguerras, Senior Technical Account Manager de Akamai

¿Te avisamos del próximo IT Digital Security?

medidas proactivas para detectarlo", dice Alberto Rodas, de Sophos, en relación a si las empresas son conscientes de la existencia de bots. En cuanto a la detección de los mismos, propone el experto en seguridad que hay que garantizar que los bots no se conecta a recursos sensibles, no envíen tráfico de comando y control y no se puedan propagar, o atacar, a terceros dentro de la red.

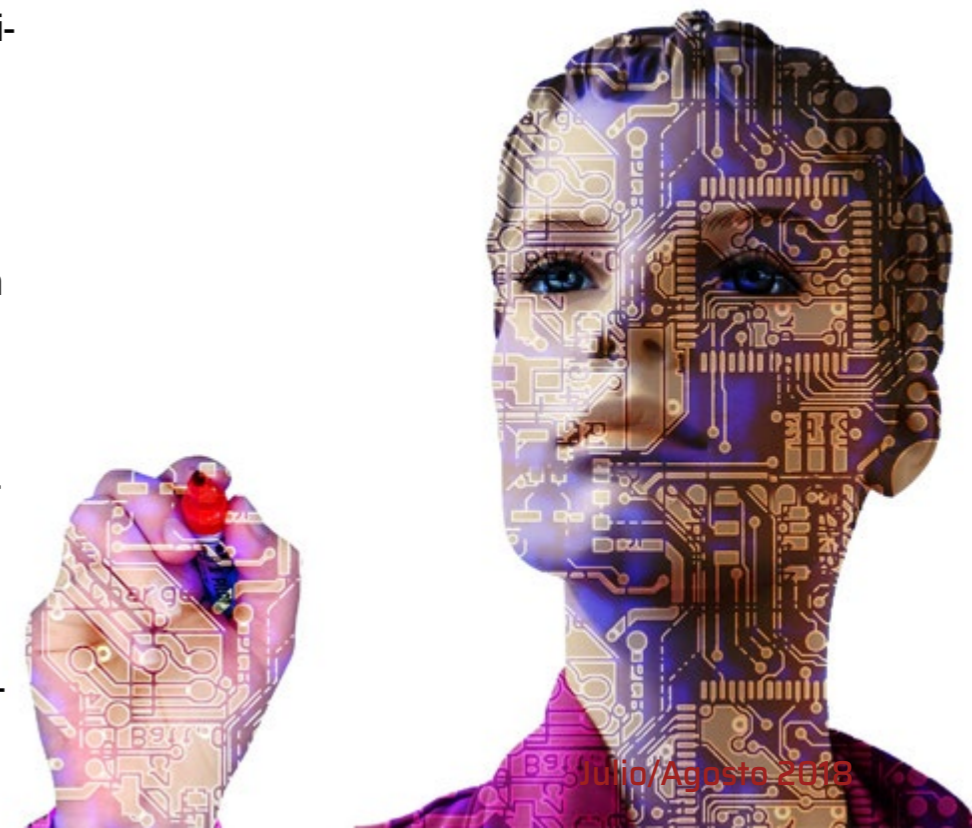
Josep Albors, de ESET, dice que, dependiendo de la actividad delictiva, los bots pueden ser detectados con mayor o menor facilidad. "Un bot que esté siendo usado como minero de criptodivisas es relativamente fácil de detectar puesto que el elevado consumo de recursos que requiere esta actividad impacta directamente en el rendimiento del sistema. Sin embargo, otras acciones como el uso de estos bots para almacenar contenidos ilícitos pueden ser más difícil de detectar o solo ser posible durante un periodo de tiempo, por ejemplo, cuando se lanza un ataque DDoS, siempre y cuando tengamos la actividad de la red monitorizada", explica Albors.

Bots buenos vs bot malos

Según el 2018 Bad Bot Report de Distin Networks, el tráfico de los bad bots se incrementó un 9,5% en 2017; también se incrementó el tráfico de los bots buenos, un 8,8%. La principal conclusión es que sólo puede esperarse que, de media, el 87,8% del tráfico de tu web proceda de un ser humano interesado en el contenido que estás mostrando.

Ya nos han contando el grupo de expertos contactados que detectar el tráfico de los bots es complicado. Y el siguiente paso sería cómo detec-

tar la actividad de un bot bueno de uno malo. Las opciones son varias. Según Eutimio Fernández, hay algunas medidas que los desarrolladores y administradores de sitios web pueden utilizar para contrarrestar la amenaza de los bots malos, como mantener las versiones actuales de los gestores de contenido (CMS), complementos y otros componentes del sitio web, intentando evitar respuestas a solicitudes anómalas. Y, además, "para aquellas organizaciones que utilizan servicios gestionados, deberían conocer los mecanismos de su proveedor para seleccionar y bloquear los bots, especialmente los responsables de los ataques DDoS de capa 7". Por último, añade el directivo que "también hay tecnologías específicas de gestión de bots, que precisamente tratan de discriminar para bloquear los malos y permitir las peticiones de los buenos".



Para Ángel Noguera, de Akamai, hablar de bueno o malo es un concepto complicado ya que lo que para un cliente puede ser bueno, para otro puede no serlo; “pongamos el caso de los indexadores de contenido de los buscadores: todo el mundo diría que son buenos, pero no diríamos lo mismo si el robot en cuestión indexa contenido únicamente para un buscador de un país donde no tenemos negocio, sobre todo, si la forma de indexar es muy agresiva. Lo que se puede hacer es detectar toda actividad de bot, dividirla en distintas categorías y dejar que quien gestione los robots se encargue de indicar cuales, para su negocio, son los buenos y los malos”.

Para el director de canal de F5 Networks una visibilidad completa y un análisis inteligente del tráfico que pasa entre el usuario y las aplicaciones resulta esencial. “La comprensión del contexto es igualmente importante”, asegura Cañete, igual que los firewalls avanzados de aplicaciones web (AWAF), que proporcionan potentes capacidades de defensa contra bots maliciosos y que brindan también una protección integral contra ataques dirigidos no solo a aplicaciones web, sino también a aplicaciones móviles; “esto último resulta especialmente relevante, porque la mayoría de las tecnologías actuales de protección de bots se basan en JavaScript, pero las aplicaciones móviles no son compatibles con ese lenguaje, con

¿Te avisamos del próximo IT Digital Security?

“Los bots están siendo usados desde hace meses como 'mineros' involuntarios, haciendo que los delincuentes obtengan criptomonedas a costa de los recursos de los usuarios”

Josep Albors, Responsable de concienciación de ESET España



lo que quedan en un estado de completa vulnerabilidad”, explica Luis Miguel Cañete.

Por eso de no empezar la casa por el tejado dice Eusebio nieva para que poder distinguir los bots

buenos de los malos, “es necesario saber qué hace cada uno”, explicando que los buenos son los de derechos de autor, que buscan contenidos plagiados en la red, los de datos (como Amazon Echo, Google Home o Siri), los araña (que permiten a los buscadores encontrar nuevos contenidos relevantes) y

los de comercio, que ayudan a los compradores a encontrar productos a buen precio. Con respecto a los malos, se encuentran los de clicks, que generan datos manipulados a los anunciantes que invierten en publicidad online, de descargas – similares a los de clicks, pero que falsean el número de descargas de, por ejemplo, una app en Google Play o en Apple Store, impostores (que se hacen pasar por usuarios reales), de copia de contenidos, de spam, espías y zombies – que usan los equipos de las víctimas para distribuir más malware.

Lo que se pregunta Alberto Rodas, de Sophos, es si hay botnets buenas. “Supongamos una red de medidores de algo, calidad del aire, está muy de moda. Podrán enviar sus mediciones a un servicio cloud, pero si dicha botnet es “buena”, como administrador de la red debería saber que tengo este tipo de servicio y saber por qué protocolo conecta, qué información envía y a quién se la envía. Cualquier otro tipo de tráfico que no pueda dar respuesta a esas tres preguntas debería ser denegado”, dice Rodas.

Cómo detectar un bot

Hay múltiples herramientas en el mercado para bloquear el despliegue de Bots dentro de una organización, pero lo que le preguntamos a César Moro, Sales Consultant en Quest Software, es cómo es posible detectar la actividad de un bot.

Cobran especial, o crítica, importancia las herramientas de tipo “User and Entity Behaviour Analytics” (UEBA). Dice César Moro que este tipo de soluciones, “se encargan de analizar patrones de comportamiento de usuarios o entidades en nuestra organización, y de esta forma poder detectar cualquier anomalía que se produjera en su comportamiento”.



Ataque de Fuerza bruta por el que se comprometen las credenciales de determinadas cuentas

- Múltiples intentos de logon sobre diversas cuentas, pero desde una misma IP

Movimiento Lateral para conseguir un radio de acción mayor

- Una vez comprometida una cuenta, se intenta hacer logon en diversos equipos. Además, serán equipos sobre los que no se actúa normalmente

Elevación de privilegios

- Introducción de la cuenta comprometida en grupos administrativos

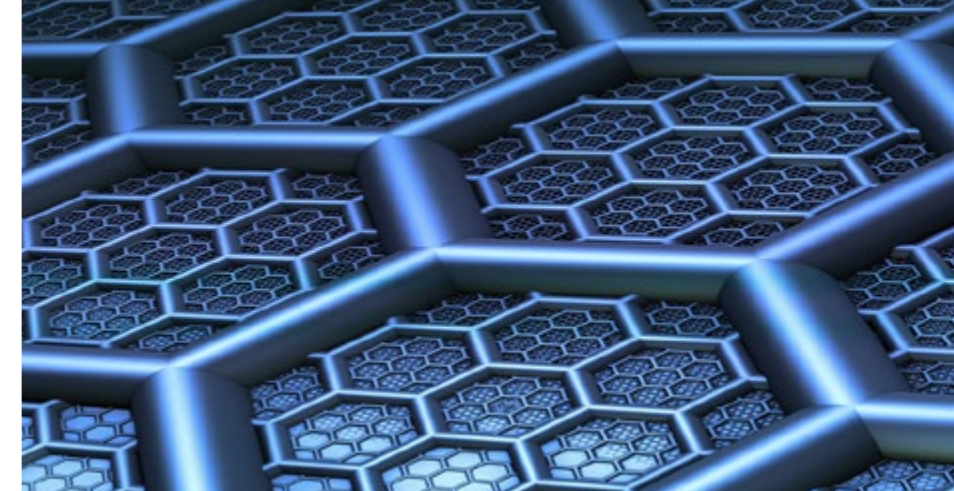
Filtración de Datos o ataque Malware

- El Bot podría acceder a datos de los servidores y volcarlos, generando un elevado número de eventos de ficheros accedidos, o simplemente encriptarlos o modificarlos para que no sean accedidos (ransomware o similar).

Para César Moro, una vez que el Bot está dentro de la organización, en muy poco tiempo puede causar agujeros de seguridad que comprometan los datos de la compañía, “y por lo tanto es necesario tener capacidad de reacción y detección en tiempo real. Esto se consigue con soluciones de análisis de comportamiento de usuarios y entidades”.

¿Qué podría interpretarse como una anomalía? Pues la actuación de Bot tratando de crear una brecha de seguridad. ¿Cómo podría detectarse? Pues porque sus actuaciones no deberían corresponder con las actuaciones normales o diarias del usuario que maneja ese equipo infectado, ya que el Bot intentará realizar una serie de ataques predefinidos a los sistemas, como podría ser un ataque de fuerza bruta, movimientos laterales, elevación de privilegios...

Hay soluciones, como Change Auditor Threat Detection, que mediante tecnologías de “machine learning” analiza en el tiempo los comportamientos de los usuarios y entidades, pudiendo detectar cualquier anomalía que indicara el posible ataque de un Bot. En el caso de los Bots, los ataques más comunes seguirían los siguientes patrones:



Detectar la actividad de un bot bueno de uno malo pasa por “monitorizar la actividad de estos bots para poder reconocer si se están conectando a direcciones legítimas para recibir órdenes”, dice Josep Albors, responsable de concienciación de ESET España. Esto se consigue con sistemas de seguridad capaces de reconocer las direcciones remotas maliciosas o sospechosas de serlo, sistemas que suelen estar alimentados por un servicio de inteligencia sobre amenazas que se actualiza constantemente.

Impacto de los bots en el Machine Learning

A estas alturas habrá quedado más que claro que los bots pueden ser útiles, o no; pueden hacer cosas buenas, o no; pueden ser buenos, o no. Un bad bot puede estar utilizando una falsa identidad para intentar superar las barreras de los firewalls y sistemas de seguridad, robar datos, identidades, números de tarjetas, realizar espionaje comercial, insertar spam o montar una campaña de denegación de servicio distribuido.

Por otro lado, los bots buenos están listos para desempeñar un papel cada vez más importante en nuestras vidas, permitiéndonos interactuar con software a través de voz, texto, emojis, imágenes, video u otros medios, usando inteligencia artificial

(AI), aprendizaje automático y procesamiento del lenguaje natural. En el lugar de trabajo, en las compras online, en el hogar y en el cuidado de la salud, bots con voz más inteligentes y rápidos ayudarán a los seres humanos a gestionar sus vidas.

Hay un punto, sin embargo, que ha comenzado a preocupar a algunos sectores del mercado, la utilización de bots para modificar los resultados del machine learning, o tener en cuenta las técnicas de machine learning para evitar su detección en lo que puede ser un símil del cazador cazado.

Dice Ángel Nogueras, Senior Technical Account Manager de Akamai, que como para cualquier proceso que se encarga de tratar datos, un agente externo que sea capaz de generar muchos datos dentro de un muestreo generará inconsistencias y afectará al resultado final. Si hablamos de analizar el tráfico web de una empresa para, aplicando algoritmos de machine learning, sacar unos resultados y aplicarlos de alguna manera, mucho tráfico de robots puede alterar los datos. Si hablamos por ejemplo de algoritmos

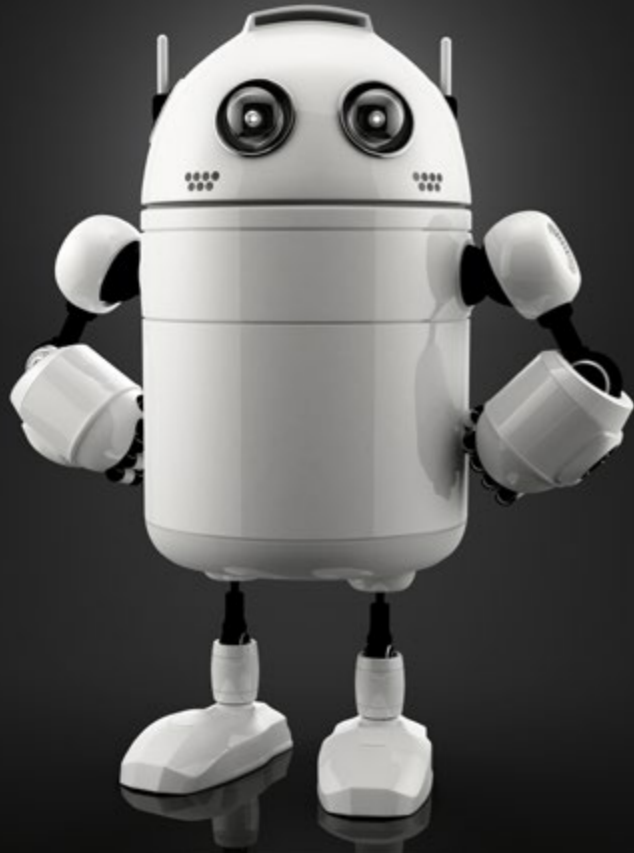
Las soluciones de tipo UEBA (User and Entity Behaviour Analytics) cobran cada vez más importancia en la detección de bots por su capacidad para analizar patrones de comportamiento

que intenten predecir los gustos de los clientes para mostrarles unos u otros productos en una web en un retailer, el hecho de tener un 20% o 30% de tráfico de robots sobre el tráfico de los clientes hace que los datos sobre los que se aplicarán los algoritmos no sean realmente todos de usuarios finales, con lo que, en este tipo de circunstancias, los robots están afectando en mayor o menor medida a los resultados de machine learning.

De la misma opinión es Luis Miguel Cañete, quien asegura que “en tanto que el machine learning analiza el comportamiento del tráfico, y si dentro de este tráfico, además del legítimo se encuentra mali-

cioso, dicho tráfico puede alterar los resultados del análisis. De hecho, incluso los Good Bots han de ser tenidos en cuenta de cara al análisis del tráfico”.

Eusebio Nieva, director técnico de Check Point, explica que más que generar errores graves en los resultados el problema es que en algunos casos los bots pueden eludir la detección basada en machine learning evitando utilizar características o métodos comunes, como por ejemplo minimizando el uso de la comunicación con comando y control centralizados, de esta forma se minimiza el impacto de uso de tecnologías de aprendizaje automático que habitualmente se centran en la detección de este tipo de



De media, sólo el 57,8% del tráfico que visita una web procede de un ser humano que está interesado en el contenido de la misma

comportamiento, es decir si cambiamos el comportamiento cualquier técnica de machine learning que se centre (o sea más potente) en la detección de un comportamiento determinado, minimizamos la posibilidad de detección. Ya hay muestras que utilizan este cambio de comportamiento para eludir su detección. En todo caso, asegura Nieva, “esto significa que hay que añadir parámetros y análisis de estadísticas que nos permitan diferenciar el tráfico humano del tráfico de máquina por parte de los algoritmos de análisis de machine learning aplicados a perfiles de tráfico o acceso a páginas web...etc.”.

Para Alberto Rodas el posible impacto de las bot en los algoritmos de Machine learning está relacio-

nado en la manera en que se obtengan los “training sets”. Explica el ejecutivo de Sophos que “muchos clientes nos preguntan si el sistema de Sophos de Deep Learning aprende de ellos y la respuesta es tajante: no”, y añade que es relación con este tipo de sistemas, “hemos de tener muy claro con qué los alimentamos, si con cosas maliciosas o benignas”, lo que lleva a la compañía británica a entrenar su Deep Learning con malware “certificado” por SophosLabs.

En la línea de Rodas se muestra Josep Albors, para quien “todo depende de cómo estén configurados los algoritmos de aprendizaje de ese sistema de Machine Learning en concreto y si éste está

preparado para lidiar con la incertidumbre”. Explica también el responsable de concienciación de ESET que hay que tener en cuenta que, en materia de seguridad, tanto la inteligencia artificial como el machine learning aún no pueden disponer de la misma autonomía que en otros ámbitos como, por ejemplo, el reconocimiento facial ya que un falso positivo puede desencadenar un efecto de bola de nieve y provocar numerosos fallos en la detección.

Un futuro con esperanza

Las botnets, como la mayoría de las amenazas de seguridad, no son nuevas, y sin embargo no somos capaces de frenarlas. ¿Hay esperanza? Eutimio Fernández tiene claro que, a pesar de los avances en los controles preventivos y la analítica, los robots siguen siendo una importante amenaza para la integridad de las aplicaciones y del contenido, así como para los sitios web en sí por la amenaza DDoS. “La solución está en las modernas técnicas de aprendizaje automático (para conocer su actividad) y la Inteligencia Artificial, con modelos capaces de detectar patrones y anomalías en el tráfico de red, pudiendo inspeccionar muchos más datos que cualquier persona y desarrollando un modelo mucho más sofisticado. Es decir, combatir a los bots con otros robots o mecanismos automatizados”, asegura el directivo de Cisco.

Los que Luis Miguel Cañete tiene claro es que las organizaciones deben actuar en tres frentes: incrementar su capacidad de vigilancia, implementar las soluciones de seguridad adecuadas y añadir inteligencia a sus sistemas. Dice el res-

ponsable de canal de F5 que las organizaciones cuentan con opciones para poder protegerse de una forma apropiada, alcanzando una buena visibilidad y aplicando inteligencia sobre el tráfico de la red corporativa y de la nube a través de herramientas analíticas que ya han demostrado su eficacia. También mediante la implementación de soluciones avanzadas de seguridad que se encargan de proteger las aplicaciones y de proporcionar información valiosa sobre los ataques. “Al mismo tiempo, resulta vital llevar a cabo audi-


torías periódicas de seguridad de los dispositivos IoT, probarlos antes de su uso y, como siempre, poner en marcha programas de formación para los empleados”, dice Cañete.

“La ciberseguridad no es una cuestión de esperanza”, dice Eusebio Nieva, sino de concienciación y de tomar medidas adecuadas. “Sin embargo, la gran mayoría de las empresas a día de hoy solo está preparada para luchar contra las infecciones Gen III. Hace falta un cambio de mentalidad para poder luchar contra las botnets y las demás amena-

Enlaces de interés...

- | [Los bad bots contabilizaron el 22% el tráfico web en 2017](#)
- | [Akamai mejora la defensa contra el Credential Stuffing](#)
- W [Bad Bot Report 2017](#)

zas avanzadas conocidas, desconocidas y de día cero”, dice el directivo de Check Point.

Para Alberto Ruiz Rodas, de Sophos, “si bien es cierto que durante años hemos vivido en entornos de seguridad con una componente reactiva que prácticamente desempeñaba el 100% de las capacidades de protección, a día de hoy con tecnologías avanzadas (el famoso “next-gen” del que se habla) donde con distintas aproximaciones a la tradicional de las firmas como Deep Learning, detección de Exploits, análisis de comportamiento o detección de técnicas post-explotación, podrán permitir la detección de lo que antes muchas veces pasaba inadvertido y permitía el rápido despliegue de estas botnets. Gracias a estas nuevas tecnologías, se entra en un nuevo campo de juego de la seguridad, la Seguridad Predictiva, donde un componente botnet nunca visto podrá ser detectado en sí mismo, por su tráfico, por sus acciones, por sus métodos de propagación, etc.”. 



¿CUÁLES SON LAS **VENTAJAS** DEL SOFTWARE DE GESTIÓN EMPRESARIAL EN CLOUD?



Descarga este **documento ejecutivo** de



**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

¿Te avisamos del próximo IT Digital Security?



Truco o Trato. La historia de la Ciberseguridad se repite una vez más

¿Qué hemos aprendido de los últimos incidentes de ciberseguridad? Cuando hablamos de ciberseguridad, es inevitable hablar de datos. La relación Ciberseguridad ---- Datos es un binomio que debe adherirse al ADN de cualquier organización que pretenda tener presencia en la actual era digital.

Es cierto que las tendencias en ciberseguridad han cambiado mucho durante los últimos años, al igual que las propias amenazas que ponen en jaque a las medidas de protección adoptadas. Quizás, la más significativa es el Ransomware, una variante de malware conocida desde sus orígenes allá por 2005, pero que en los últimos tres años ha mostrado

Es imperativo continuar mejorando los planes de prevención y gestión de vulnerabilidades, pero también interiorizar el desarrollo de aplicaciones/servicios digitales de forma segura desde la fase de diseño



de la mano de representaciones tan significativas como WannaCry y Petya, que cualquier organización puede estar expuesta a amenazas muy difíciles de contener y que atacan directamente a su mayor activo, el dato, realizando el secuestro del mismo mediante técnicas de cifrado y que dificultan su recuperación de no sucumbir al chantaje económico que se plantea a cambio de recuperar dicha información.

Ante este contexto el mundo corporativo se replantea dos situaciones:

- **Cómo mejorar la estrategia de ciberseguridad para salvaguardar el dato**
- **Cómo asegurar la disponibilidad del dato y minimizar el menor tiempo de respuesta ante nuevos incidentes**

La gran mayoría de los impactos de este tipo de amenazas consiguen penetrar en las líneas de defensa de las organizaciones gracias a las continuas vulnerabilidades que los diferentes sistemas presentan en la actualidad. Por ello, es imperativo continuar mejorando los planes de prevención y gestión de vulnerabilidades, pero también interiorizar el desarrollo de aplicaciones/servicios digita-



EL DILEMA DE LOS CISO, PREVENCIÓN VS INVESTIGACIÓN

Este documento explora las necesidades de los CISO en la era de prevención-detección-respuesta-investigación y pondera cómo la falta de visibilidad, velocidad y el personal afecta

la construcción de prácticas de seguridad más sólidas en las empresas con equipos de TI sobrecargados y con recursos insuficientes.



Enlaces de interés...


- I [SamSam y Mylobot encabezan las principales amenazas de seguridad](#)
- I [La extorsión y el ransomware son las mayores amenazas para los CIO](#)
- I [Atlanta, la ciudad devastada por un ransomware](#)
- W [Evite que el ransomware llegue a su Puerta](#)
- I [Un año después EternalBlue sigue amenazando a sistemas desprotegidos y sin parche](#)

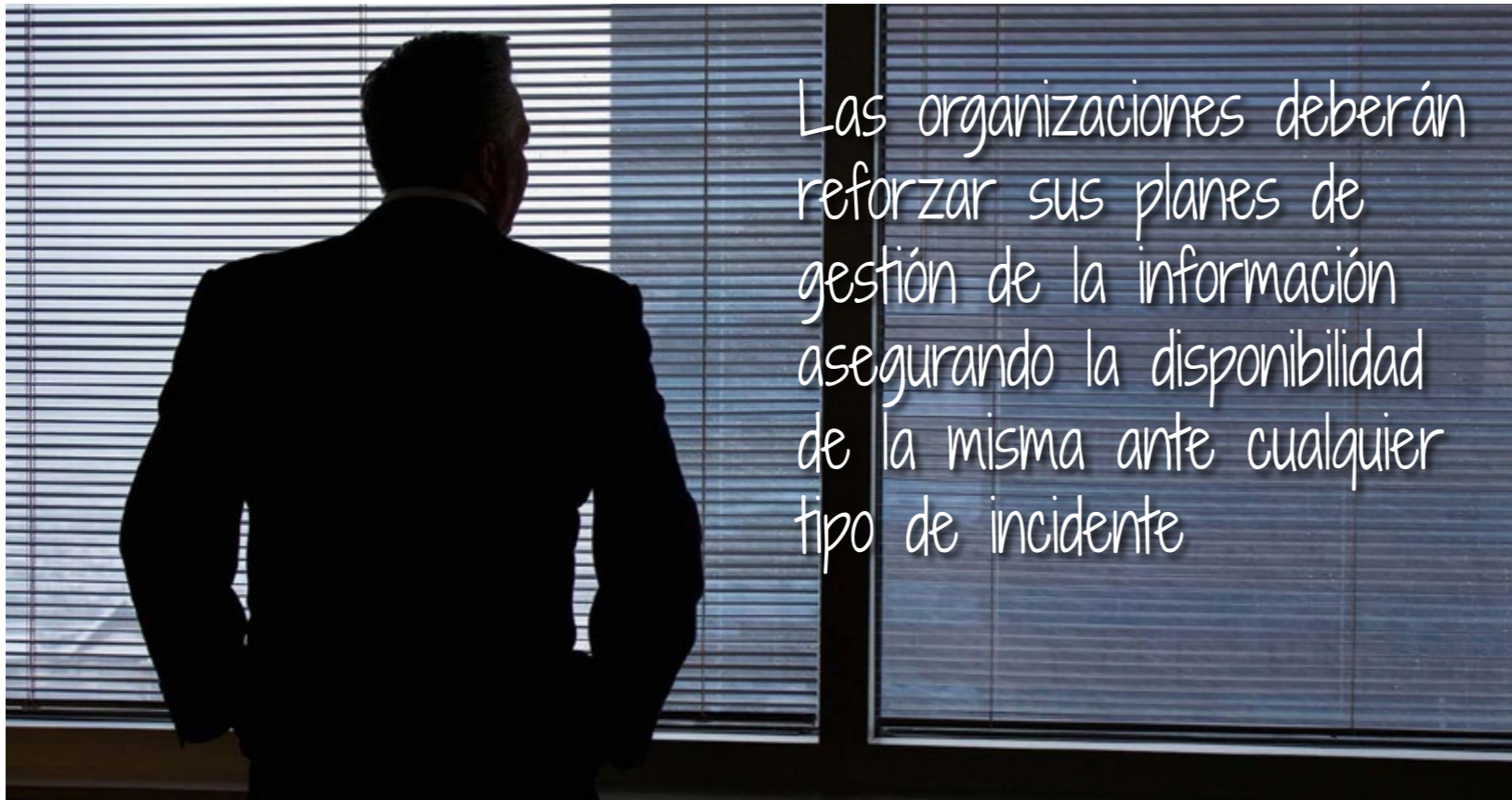
les de forma segura desde la fase de diseño que permita minimizar al máximo la exposición que las organizaciones tienen hoy en día por la acumulación de vulnerabilidades no solventadas. Desde IDC se observa como el mercado de ciberseguridad asociado a la gestión de vulnerabilidades en España crecerá en los próximos 3 años alcanzando una tasa de crecimiento sostenido del 6% (CAGR) y llegando a acumular en dicho periodo una previsión de gasto de este tipo de soluciones de 176,45 M€.

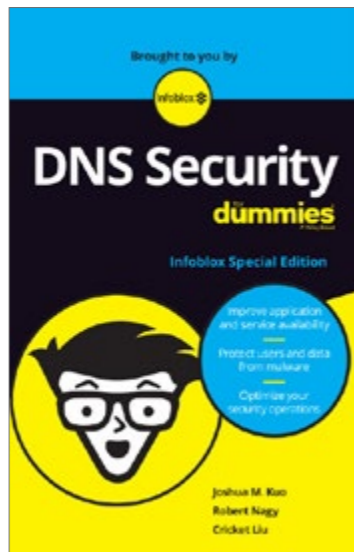
La mejora de los procesos de desarrollo de software y servicios digitales será clave para cualquier organización digital, ya que permitirá

introducir la seguridad desde la fase de diseño, también conocido por sus siglas en inglés SSDLC (Secure Software Development Life Cycle) Según IDC, en 2020, en cualquier nuevo servicio/activo digital SSDLC será una prioridad para el 90% de las organizaciones, lo cual ayudará a minimizar el impacto que las vulnerabilidades tengan en los nuevos servicios digitales, mostrando una nueva forma de implementar la seguridad desde el diseño que afectará a todas las estrategias de ciberseguridad que se desplieguen a lo largo de la nueva era digital.

Mientras tanto, las organizaciones deberán reforzar sus planes de gestión de la información asegurando la disponibilidad de la misma ante cualquier tipo de incidente, incluyendo ciberamenazas amenazas como los últimos casos de ransomware. Para ello, los planes de almacenamiento y salvaguarda del dato en el Cloud deberán contribuir a reforzar las estrategias de seguridad de las organizaciones, al mismo tiempo que se confirma una tendencia alcista de un mercado cada vez más importante. Según IDC, el mercado de servicios de almacenamiento basados en Cloud Pública en España crecerá entre 2018-2021 un 25,7% (CAGR) alcanzando una previsión de gasto que rondará los 246 M€ hasta 2021.

El actual contexto digital marca líneas inevitables de trabajo para las organizaciones que quieran estar presentes en los nuevos entornos digitales, para los que habrá que minimizar al máximo la existencia de vulnerabilidades y asegurar planes de continuidad y disponibilidad del dato. 





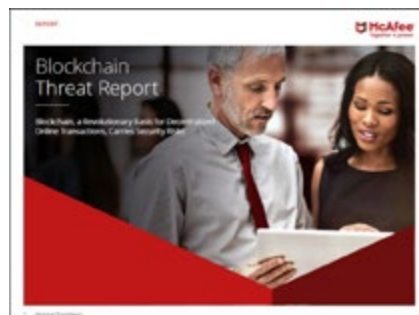
DNS Security for Dummies

Como uno de los protocolos más antiguos y más fiables del Internet moderno el Sistema de Nombres de Dominio (DNS) es la piedra angular de casi todos los servicios de navegación y clave para otros protocolos. Desafortunadamente, su rol como el primer paso en la conectividad de Internet, hace que el DNS sea el primer objetivo para las nuevas variantes de ciberataques maliciosos y con unos costes muy elevados. Con este libro de lectura fácil aprenderá no solo qué es el DNS y cómo funciona, sino a qué amenazas se enfrenta el Sistema de Nombre de Dominio y diez claves para mejorar su seguridad.



Iluminando el shadow IT

Más del 70% de las organizaciones saben o sospechan que los empleados están usando cuentas personales para compartir archivos. Este documento explora cómo hacer frente al Shadow IT y el uso de aplicaciones personales de intercambio de archivos que ponen en riesgo los datos confidenciales al colocarlos fuera del control y la visibilidad de TI. Conozca las cinco razones por las cuales una plataforma para compartir archivos de nivel empresarial puede ayudar a los empleados a colaborar y acceder a la información mientras se mantiene la seguridad de los datos.



Los riesgos de Blockchain

Casi todas las industrias han invertido, adquirido o implementado blockchain en alguna capacidad. Sin embargo, McAfee prevé un enorme potencial de riesgos de ciberseguridad que podría amenazar el rápido crecimiento de esta tecnología revolucionaria. Según el informe de McAfee, los malos actores buscan aprovechar la rápida adopción de las criptomonedas y los primeros usuarios que las usan a través de cuatro vectores clave de ataque: esquemas de fraude o phishing, malware, exploits de implementación y vulnerabilidades tecnológicas.



Informe global de seguridad de aplicaciones y redes

Los constantes problemas de seguridad han estimulado una mayor inversión en ciberdefensa por parte de todos, desde estados nación y corporaciones globales hasta individuos que compran soluciones antimalware para dispositivos personales. Sin embargo, incluso cuando las inversiones aumentan, también lo hacen las amenazas, los piratas informáticos y las vulnerabilidades. Comprender estas dinámicas complejas y desafiantes es lo que impulsa este informe, que ofrece información sobre dónde estamos y qué pueden hacer los profesionales de la seguridad.



La Seguridad TIC a un solo clic



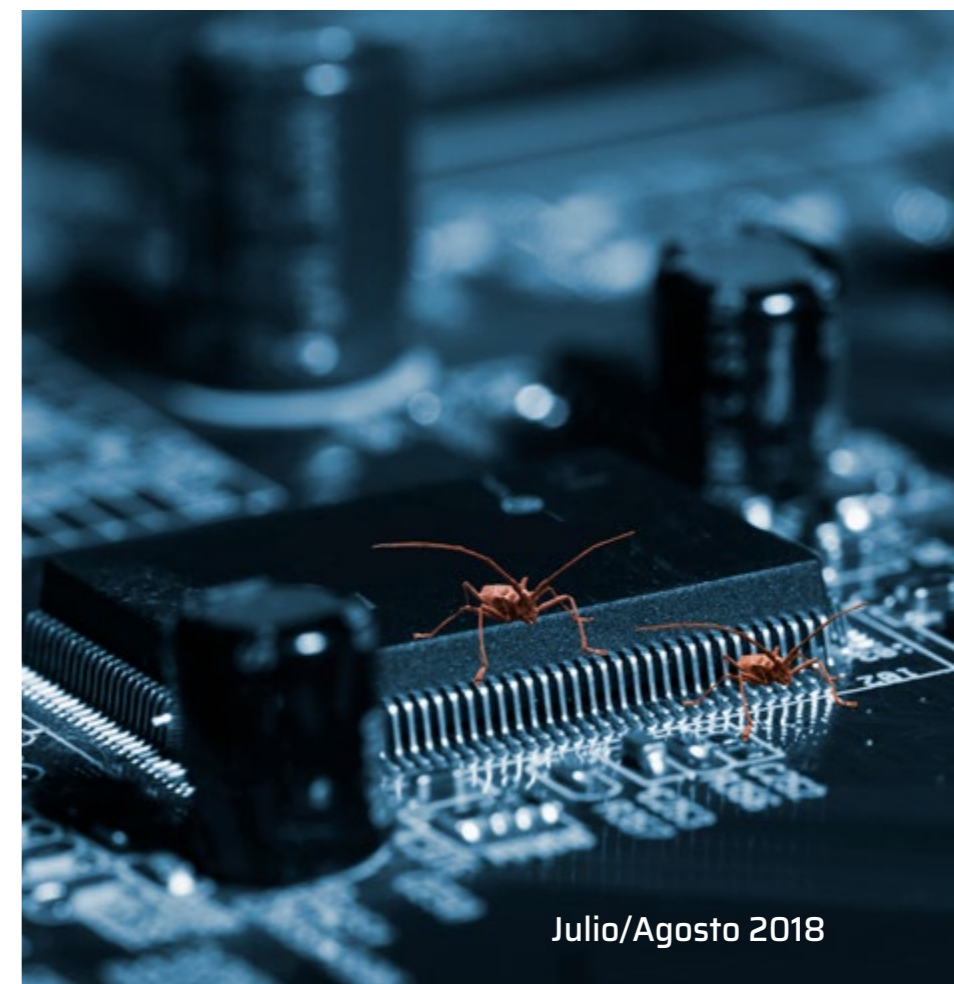
FERNANDO PICATOSTE

SOCIO DE RISK ADVISORY DE DELOITTE

Fernando Picatoste es socio en el área de Riesgos de Deloitte (Risk Advisory), donde se ha desarrollado toda su carrera profesional desde 1996. En la actualidad es el Responsable en España de Gestión de Crisis y ha sido el responsable para EMEA de Ciberseguridad entre 2014 y 2016. Durante su trayectoria ha dirigido un elevado número de proyectos de auditoría, consultoría de riesgos tecnológicos en sistemas de información, gestión de crisis y ciberseguridad, así como liderado campañas con equipos en distintos países para clientes multinacionales, y participado como ponente en múltiples eventos relacionados con la gestión de crisis, la seguridad y la gestión de riesgos tecnológicos tanto en España como en otros países de EMEA.

Preparación para la gestión de crisis, un imperativo para cualquier compañía

En los últimos años algo ha cambiado en la forma en la que las empresas se preparan para la posibilidad de sufrir una crisis. El desarrollo digital o la internacionalización de la actividad que ha permitido la globalización, entre otros avances, han contribuido a crear un campo de juego lleno de oportunidades para los más sagaces. Pero también nos expone a un número creciente de riesgos, no sólo en cantidad, sino también en tipología. Empresas que desarrollan su negocio a través de Internet, y que hace unas décadas no habría tenido la misma proyección global, se ven directamente afectadas por crisis geopolíticas en países lejanos, o incluso por desastres medioambientales que ocurren lejos de sus sedes. Hoy, más que nunca, es necesario que las compa-





RESOLUCIÓN DEL PUZZLE DE GDPR

Para ayudar a las organizaciones a entender mejor el papel de la ciberseguridad en el contexto del GDPR, este documento técnico

proporciona una descripción precisa de la normativa, junto con un marco que le ayudará a iniciar el camino al cumplimiento.



ñías estén preparadas para cualquier tipo de crisis, porque todas están expuestas a ellas. Como hemos dicho en más de una ocasión, hay dos tipos de compañías: las que ya han tenido alguna crisis y las que la van a tener.

Además, es necesario tener en cuenta que, a medida que la complejidad de las organizaciones crece, la posibilidad de enfrentarse a situaciones "especiales", difícilmente predecibles e inestables, aumenta. Y, con ello, la necesidad de que los ejecutivos estén preparados para hacerlas frente de manera decidida y eficaz. Es imprescindible, para garantizar un adecuado nivel de preparación, que los miembros de los Consejos de Administración y



Hoy, más que nunca, es necesario que las compañías estén preparadas para cualquier tipo de crisis, porque todas están expuestas a ellas

Comités de Dirección se aseguren de que las gerencias de sus compañías conocen y comprenden los riesgos que podrían comprometer los objetivos estratégicos. Es igualmente importante fortalecer los mecanismos establecidos para prevenir, detectar y reaccionar ante las amenazas de manera ágil. La monitorización, preparación y capacidad de respuesta temprana son los conceptos que toman protagonismo para aumentar la resiliencia de la organización.

La vigilancia continua, la planificación de la respuesta y ensayo de diversos escenarios son la úni-

ca receta eficaz para reaccionar de manera rápida y efectiva ante una situación de crisis. Los simulacros periódicos permiten comprobar si los procesos, capacidades y recursos definidos dentro de la organización se ejecutan de manera adecuada en cualquier situación excepcional. Son también una forma práctica de determinar qué áreas deben reforzar sus procesos, tanto humanos como técnicos, para conseguir respuestas más ágiles y competentes. Pero, ante todo, los simulacros son una experiencia para los equipos que deben liderar y solventar las crisis, cuando todavía no ha pasado nada, que nos

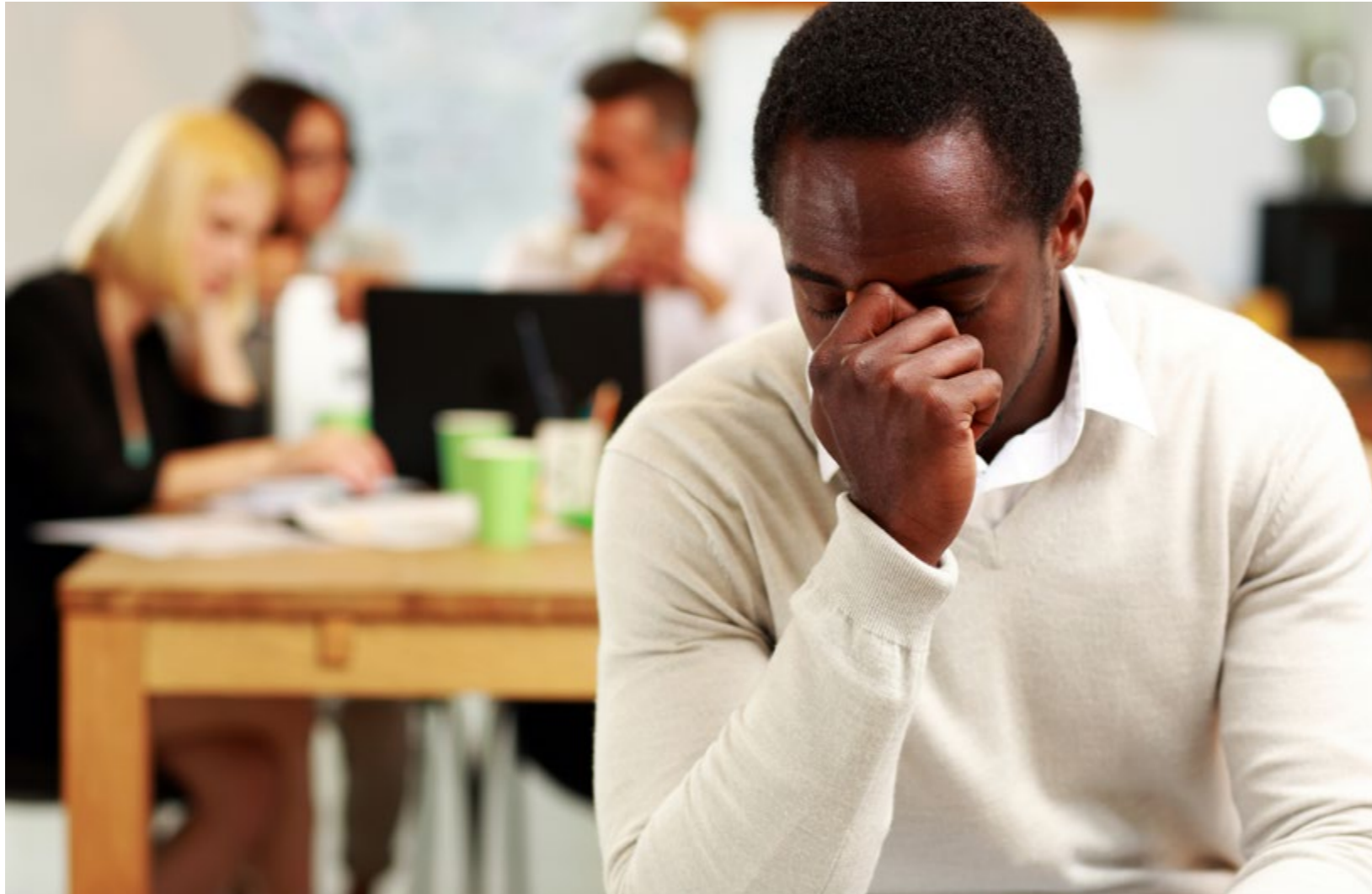
La vigilancia continua, la planificación de la respuesta y ensayo de diversos escenarios son la única receta eficaz para reaccionar de manera rápida y efectiva ante una situación de crisis



hace interiorizar los aspectos más relevantes mediante una vivencia difícil de olvidar.

En Deloitte creemos que los simulacros y, en su nivel más avanzado, los juegos de guerra, usados desde hace años en el entorno militar, ofrecen la posibilidad de identificar y asignar responsabilidades en la gestión de crisis. Mediante la inmersión en un escenario de crisis realista los representantes de los diferentes grupos de interés de una empresa, no sólo pueden poner a prueba los planes ya existentes, sino que además se les ofrece un campo de pruebas de ideas de gestión innovadoras sin la carga económica que supondría ponerlas en marcha de forma real.

Un error en el que las compañías caen de manera, más o menos generalizada, es el de asumir que todas las crisis son similares, y que por lo tanto un plan de actuación genérico es suficiente como para afrontarlas. Pero la realidad nos enseña que no es así. No se trata solo de clasificarlas según el tipo de riesgo (reputacional, financiero, regulatorio, geopolíticos, ciberseguridad, etcétera), sino también de diferenciar por evolución y velocidad de propagación. Tendemos a llamar crisis a un suceso inesperado que, provoca un cambio profundo y repentino en la marcha habitual de las empresas, pero lo cierto es que no son pocos los casos en los que los incidentes se desarrollan lentamente y, poco a poco, se convierten en un



y la reputación de una empresa. Para mantener la confianza de todos los stakeholders implicados, los directivos de las compañías deben ser capaces de mitigar los riesgos a los que estas se enfrentan, así como de liderar la toma de decisiones necesarias. Y estos son, sin duda, dos de los mayores desafíos en la gestión de una crisis.

Desafíos que es imperativo enfrentar cuanto antes. Y es que el número de crisis que una organización puede enfrentar se ha incrementado en los últimos años. De hecho, según el estudio Stronger, fitter, better: Crisis management for the resilient enterprise, hecho público recientemente por Deloitte, cerca del 60% de participantes en él cree que las empresas están mucho más expuestas a sufrir una crisis hoy que hace diez años. Es más, el 80% de las compañías, a nivel mundial, ha tenido que movilizar a sus equipos de gestión de crisis al menos una vez en los últimos dos años. Y aunque son los ciberincidentes y los relacionados con la seguridad los más repetidos, los riesgos operativos son

problema de gran alcance. Por usar dos metáforas fácilmente visibles, el primer tipo de crisis se podría comparar con un incendio, mientras que el segundo, con una bola de nieve que, poco a poco, va creciendo hasta convertirse en alud. La popularización de las redes sociales en nuestro día a día ha contribuido de forma significativa a que cualquier incidente, por pequeño que sea, pueda llegar a desencadenar una crisis en toda su magnitud.

Estos incidentes pueden tener un efecto devastador en el rendimiento financiero, la moral, las ventas

Un error en el que las compañías caen de manera, más o menos generalizada, es el de asumir que todas las crisis son similares, y que por lo tanto un plan de actuación genérico es suficiente como para afrontarlas

El 80% de las compañías, a nivel mundial, ha tenido que movilizar a sus equipos de gestión de crisis al menos una vez en los últimos dos años



responsables también de un gran número de situaciones excepcionales. Concretamente del 34% de las crisis registradas en los últimos dos años a nivel mundial, y del 38% en España.

Y aunque la concienciación va calando entre los empresarios, y cerca del 90% de los encuestados confía en la capacidad de su organización para hacer frente a un escándalo corporativo, lo cierto es que aún queda mucho camino por recorrer. Por ejemplo, solo el 17% de las compañías han utilizado la simulación como ejercicio de preparación

ante una crisis y solo un 55% afirma participar en ejercicios de crisis con terceros, como proveedores y socios estratégicos. Es más, a pesar de la buena noticia que supone que casi el 90% de las compañías hayan realizado revisiones de sus protocolos de actuación después de una crisis (80% en España), los análisis realizados ponen en evidencia que muchas de estas podrían haberse evitado.

Concentrados en conseguir las últimas tecnologías de monitorización, protección y respuesta, no es inusual que las compañías descuiden la formación de los profesionales, que se convierten así en el eslabón más débil de la cadena. Planes de formación continuos, el establecimiento de políticas de comunicación claras y efectivas, así como el desarrollo e implementación de políticas de prevención y protección permitirán asegurar que la implicación

Enlaces de interés...

- | [Stronger, fitter, better: Crisis management for the resilient enterprise](#)
- | [Las utilities están mal equipadas para hacer frente a las ciberamenazas](#)
- | [El Gobierno facilita el intercambio de información ante crisis cibernéticas](#)

de la plantilla es total en este ámbito. Si además reforzamos estas pautas con la calendarización de entrenamientos y simulacros, igual que hacemos con los planes de evacuación de edificios, las habilidades de los profesionales ante una situación crítica permitirán no sólo reaccionar más rápidamente, sino también hacerlo de forma ordenada, racional y consistente, reflejando una perfecta alineación entre el plan estratégico, el táctico y la operativa de respuesta.

En definitiva, planificación, monitorización, entrenamiento y gestión de la comunicación, a todos los grupos de interés de la organización, son los cuatro elementos clave que cualquier empresa debe dominar si quiere enfrentarse a una realidad en la que las amenazas son cada vez más frecuentes y globales. **it**

Compartir en RRSS

