it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Marzo 2019 - nº 17

NAC, el ojo seguro que todo lo ve

De las Cartas nigerianas a la ingeniería social

“Los clientes no van a utilizar tecnología en la que no confían”

Infinity 2.0, la era de los nanoagentes ha llegado

Backup y continuidad de negocio, ¿estás preparado?

La Seguridad Gestionada o el caos

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

it Digital Security

Directora **Rosalía Arroyo** rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez Bárbara Becares y Jaime Velázquez

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

it Digital MEDIA GROUP

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

Director de IT User Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es

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

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

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

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

La seguridad también tiene cabida en MWC 2019

Una vez más febrero se ha convertido en el mes de la movilidad. Ocurre cada año, cuando decenas de miles de personas invaden Barcelona para asistir al MWC. Hace tiempo que se habla de seguridad en el Mobile; los inicios fueron tímidos, circunscritos a antivirus para móviles, basados en Android, que iOS nunca se ha dejado. Más tarde, cuando Android invadió las empresas con terminales que se conectaban a las redes empresariales, desde los que se enviaban documentos y que accedían al correo, la cosa se complicó. Empezó a hablarse de gestión e dispositivos móviles, MDM, para terminar hablándose de EMM, o gestión de la movilidad empresarial. Ahora ya no es raro ver empresas de seguridad en el MWC. Ya os los hemos contado en una serie de artículos de opinión incluidos en un Especial Mobile World Congress que recoge todo lo acontecido en la feria. También podrán acceder a ellos en uno de los contenidos de este número de IT Digital Security, que recoge algunos de los anuncios más destacados del Mobile en materia de seguridad

La portada de este número está centrada en los NAC, los controladores de acceso a la red, soluciones cada vez más imprescindibles en un mundo plagado de cosas conectadas. La última generación de soluciones NAC permiten establecer políticas granulares basadas en el quién, el qué, el dónde y el cuándo.

En este número os contamos también a través de uno de nuestros IT Webinar, cuáles son las ventajas de los Servicios de Seguridad Gestionados, con la colaboración de Sarenet, Sophos, Trend Micro, Panda Security y S21sec.

Los #DesayunosITDS de este mes se han centrado en el backop y la disponibilidad, para lo que hemos contado con la opinión experta de WhiteBearSolutions, Veeam, Rubrik y StorageCraft, a través de su mayorista Ireo.

Además, entrevistamos a Héctor Sánchez Montenegro, National Technology Officer de Microsoft; destacamos las novedades del CPX360 de Viena; y hablamos sobre la evolución de los Yahoo Boys, los estafadores nigerianos que pasaron del Spam a la ingeniería social.

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

itds

Sumario

Actualidad

No solo IT

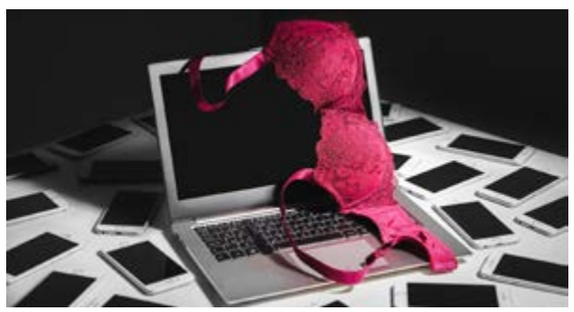
Zero Trust, la desconfianza que refuerza las estrategias de protección del dato

La Inteligencia Artificial: ¿debemos preocuparnos de ellos o preocuparnos por ella?

En diez años, la Inteligencia Artificial en empresas y sector público añadirá 14% al PIB Mundial

Índice de anunciantes

Reportaje



Los ‘yahoo boys’ crecen: del spam de las cartas nigerianas a la ingeniería social

Webinar ITDS

La Seguridad Gestionada o el Caos

Desayunos ITDS

Backup y continuidad de negocio, ¿estás preparado?

SOPHOS

INTERCEPT X

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

© Copyright 2018. Sophos Ltd. Todos los derechos reservados.

Sophos es una marca registrada de Sophos Ltd.

Compartir en RRSS

Infinity 2.0, la era de los nanoagentes ha llegado

Rosalía Arroyo

Check Point avanza su arquitectura de seguridad en su CPX360 Viena. Dotada de nanoagentes para un mundo IoT y en el que el nube se convierte en el cerebro donde se tomarán todas las decisiones, Infinity 2.0 incorpora un enfoque que ayudará a que las protecciones de seguridad sigan a los activos más de cerca y con controles más precisos de lo que ocurre con cada elemento de la red.

Con 25 años de historia a sus espaldas, Check Point tiene mucho que decir, y que recordar. Su fundador y CEO, Gil Shwed, lo hacía durante el CPX360 de Viena, un evento que reunió a más de cuatro mil asistentes, el mayor en la historia de la empresa. Decía Shwed que en todos estos años se ha avanzado mucho en la protección de Internet mientras recordaba aquellos primeros años dedicados a "convencer a la gente del potencial del Internet".

25 años hasta llegar a 2018, un año en el que Check Point bloqueó más de cien millones de ata-

"Hay demasiadas categorías de productos, demasiados fabricantes, demasiados tipos de ataques"

Gil Shwed, Fundador y CEO, Check Point

ques desconocidos, mayor cantidad de cibercriminales fueron procesados, el servicio de seguridad administrado por Threatcloud monitorizó 86.000 millones de indicadores de compromiso por día, y en el que ha quedado claro que "todos nosotros tenemos trabajo para toda la vida", debido a la escasez de expertos en seguridad.

Al mismo tiempo, y a pesar de que las empresas gastaron un 11% más en seguridad, los resultados fueron peores si se tiene en cuenta que 46% de las empresas se vieron afectadas por un problema de seguridad o el 36% de los consumidores perdieron datos. Por eso establece Gil Shwed tres grandes retos. Por un lado cambiar la mentalidad, pasar de la detección a la prevención; "estamos luchando con millones de bots y no podemos correr tan rápido", aseguraba el directivo.

En segundo lugar habló de la Quinta Generación de Ataques, que son a gran escala, que afectan a múltiples vectores y que a menudo implican a gobiernos. Actualmente, aseguraba el fundador de Check Point, las empresas están preparadas para afrontar ataques de segunda y tercera generación -contra redes y aplicaciones, por lo que hay un gap que debe superarse. La infraestructura cloud es, en este punto, el "eslabón más débil", aseguraba Shwed.

El tercer gran reto es la complejidad. Hay "demasiadas categorías de productos, demasiados fabricantes, demasiados tipos de ataques", decía Gil Shwed, añadiendo que la complejidad se va a multiplicar por dos en los próximos tres años; "para resolver este problema necesitas ser súper sofisticado, probablemente más inteligente que Einstein".

El futuro pasa por la simplificación y la consolidación de la ciberseguridad, pasa por centrarnos en la prevención, pasa, en definitiva por "tener una arquitectura que pueda mantenerse al frente y que pue-

"En Infinity 2.0 en lugar de asegurar una red que contiene multitud de elementos, aseguramos cada elemento de manera individualizada"

Itai Greenberg, VP of Product Marketing & Product Management, Check Point

da actualizarse automáticamente". Pasa por Infinity, la arquitectura de seguridad que Check Point presentó en 2017 y que permite compartir la inteligencia de amenazas con el endpoint, los dispositivos móviles, la red y los sistemas de gestión unificada.

Trabaja ya Check Point en "unificar la seguridad e implementar el control de seguridad adaptativo de la IA", dijo Shwed, añadiendo que la compañía tendrá toda la oferta de servicios y soluciones disponibles en la nube para 2020.

Check Point Infinity 2.0

Se sigue avanzando en la primera versión de Infinity, arropada ya con un modelo de consumo a medida bautizado como Infinity Total Protection, que permite a los clientes poder consumir y acceder a todas las soluciones de seguridad de Check Point por un coste fijo por usuario y mes. Infinity Total Protection es la única solución de suscripción disponible actualmente que incluye hardware y software de seguridad de red, con protección integrada para endpoints, nubes y dispositivos móviles, y prevención de amenazas de día cero, junto con una administración unificada y soporte premium 24×7.

Pero detrás hay más y Check Point lo contó en Viena, en su CPX360. Lo hacía Itai Greenberg, VP of Product Marketing & Product Management de la compañía, con quien tuvimos la oportunidad de hablar. Nos contaba Greenberg que ha habido un cambio en la manera en que se consume el software y las tecnologías. Las empresas, aseguraba, "son compañías de software" en tanto en cuanto están en constante proceso de desarrollo de aplicaciones que permitan interactuar a los usuarios con sus servicios. "Todo el mundo está desarrollando software y quieren hacerlo rápido, ser los más innovadores", pero eso despierta las alertas de los responsables de seguridad, que deben permitir la innovación, ser los facilitadores del negocio, pero de una manera responsable.

"Necesitamos llegar a un nuevo concepto de seguridad que permita a los desarrolladores moverse rápidamente, pero de forma muy segura. Y eso es lo que viene a hacer Infinity 2.0", aseguraba el directivo.

Se trata por tanto de cerrar el gap entre los desarrolladores que quieren correr rápido para llevar a la empresa adelante con innovación, y asegurar a

CYBERSECURITY FOR 2020. PONENCIA DE GIL SHWED, CEO DE CHECK POINT

CLICAR PARA VER EL VÍDEO

Se sigue avanzando en la primera versión de Infinity, arropada ya con un modelo de consumo a medida bautizado como Infinity Total Protection

los responsables de seguridad que en ese proceso no se está poniendo a la empresa en riesgo.

Y eso quiere hacerlo Check Point con nanoagentes, en el cloud y monitorizando cada activo digital. "En lugar de asegurar una red que contiene multitud de elementos, aseguramos cada elemento de manera individualizada", nos contaba Itai Greenberg. Es decir que se asegura el PC, el smartphone, el reloj, la luz, el televisor… cada elemento conectado a la red se asegura de manera independiente y a través de nanoagentes muy ligeros "porque en lugar de dejar que las decisiones se tomen en el elemento, se tomarán en la nube".

La nube será en lugar donde cada activo realizará la consulta y desde donde recibirá una orden sobre lo que tiene que hacer. "El cloud se convierte en el cerebro", decía Greenberg, introduciendo el concepto Fog; no se trata de algo nuevo, pero se incorpora al mensaje de Infinity 2.0 porque hace referencia a un modelo de computación más ágil y eficiente, basado en infraestructuras híbridas, que reduce la cantidad de datos que se necesitan llegar a la nube para su procesamiento.

El tercer elemento clave de Infinity 2.0 está relacionado con el Activo Digital. Se monitoriza cada activo digital, explicaba el VP of Product Marketing

LA SEGURIDAD ES INFINITY

Coincidiendo con el 25 aniversario de la compañía, Check Point Software Technologies celebró los días 17 y 18 de octubre en El Escorial una nueva edición de CPX España, en el que participaron más de 400 profesionales del sector de la seguridad informática. Los expertos más destacados de la compañía explicaron cuál es el panorama de la ciberseguridad en España, así como los principales desafíos y amenazas actuales como los ataques a móviles e infraestructuras cloud y las herramientas de las cuales se dispone para enfrentarse a estas amenazas, como la aplicación de la Inteligencia Artificial de forma práctica.

& Product Management de Check Point. Y eso implica que de cada elemento de esa red se recoge información sobre su localización, el sistema operativo y versión que está utilizando, cuándo se conecta y quién interactúa con él, quién lo gestiona…. Un montón de información que genera un contexto en base al cual "el riesgo se está recalculando de forma constante". Un montón de información que exige no sólo de gran capacidad de computación, sino de almacenamiento, reconoce el directivo de Check Point.

¿Qué tipo de empresa está preparada para adoptar Infinity 2.0? Check Point ya está trabajando con varias empresas grandes, del sector financiero, utilities, del sector seguros… "Hemos seleccionado ya algunas empresas. A finales de este año abriremos Infinity 2.0 para otros 20 clientes y en 2021 lo abriremos más aún", concluye el directivo.

Ya ven que Infinity 2.0 se prepara para la siguiente oleada tecnológica, para un mundo de IoT, de Redes 5G, de amenazas cada vez más avanzadas, de orquestación y automatización, un mundo en el que la seguridad será entregada como servicio y a través de nanoagentes.

Sí, suena como Matrix. Pero en un mundo en el que apenas se ha arañado la superficie, en el que las empresas focalizan sus recursos para proteger apenas los ordenadores, servidores y algún dispositivo móvil, olvidando routers, cámaras, impresoras, dispositivos del hogar inteligente o de la medicina avanzada, hay que prepararse. Y eso es lo que hará Infinity 2.0, una arquitectura abierta, que se adaptará a las necesidades de crecimiento que impondrá la explosión del IoT y que será capaz de proteger un contexto cada vez más rico y variado.

Enlaces de interés…

- Check Point avanza su Infinity 2.0 en Viena
- Check Point compra ForceNock para potenciar la seguridad de las API
- Nueva vulnerabilidad en WinRAR que pone en riesgo a sus más de 500 millones de usuarios
- El grupo cibercriminal Lazarus ataca empresas privadas en Rusia
- Check Point previene los ciberataques Gen V con Infinity Total Protection

TREND MICRO™

POWERED BY XGen™ SECURITY

Detectar y prevenir las brechas a la velocidad del rayo

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

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

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

Capacidad probada

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

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

NSS LABS RECOMMENDED

Inteligencia de amenazas líder del sector

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

www.trendmicro.es

La Seguridad se expande en el MWC

5G, Inteligencia Artificial, IoT y, por supuesto, móviles. Todos coinciden en que éstas han sido las grandes estrellas del Mobile World Congress 2019. Y alrededor de todo ello, la seguridad.

Compartir en RRSS

Parece que cuesta hablar de seguridad en el MWC, aunque cada vez sea más las empresas de este sector que acuden a la feria. Llegan para hablar de la seguridad de los dispositivos móviles, del IoT, de propuestas para que las telecos puedan hacer frente a las nuevas tecnologías de manera más rápida y más segura, o incluso de seguridad biónica.

Sophos, por ejemplo, anunciaba una gestión de dispositivos móviles más inteligente con la integración de Microsoft Intune, una integración que según la compañía permite "ofrecer información detallada sobre las amenazas relacionadas con endpoints móviles individuales", lo que lleva a que los administradores de TI puedan tomar decisiones más fundamentadas sobre si bloquear el acceso a la red de un dispositivo.

Al ejecutarse en Microsoft Azure, la integración de Sophos permitirá a los administradores de TI configurar políticas de uso individualizadas para dispositivos dentro de Microsoft Intune haciendo posible que los empleados sean productivos y trabajen desde los dispositivos y aplicaciones que ellos mismos prefieran, mientras se garantiza el cumplimiento con los datos corporativos.

La seguridad aplicada a la biónica llegaba de la mano de Kaspersky, que en colaboración con la compañía Motorica, ha realizado una evaluación de ciberseguridad de un software experimental para una mano protésica digital, desarrollada por la start-up rusa. La solución consiste en un sistema cloud remoto, una interfaz para la monitorización del estado de todos los dispositivos biomecánicos registrados. También proporciona a otros desarrolladores un conjunto de herramientas para el análisis de las condiciones técnicas de varios dispositivos, como sillas de ruedas inteligentes, manos y pies artificiales.

Dicha evaluación identificó varios problemas de seguridad, como conexión http insegura, operaciones de cuenta incorrectas y validación de acceso insuficiente. Cuando está en uso, la mano protésica transmite datos al sistema cloud. Debido a las brechas de seguridad, un ciberatacante podría llegar a obtener acceso a la información disponible en la nube de todas las cuentas conectadas (incluidas

Para el 55% de los proveedores de servicios el IoT es la tendencia más importante desde el punto de vista estratégico para los próximos dos a cinco años

Dos de cada cinco hogares conectados son vulnerables a los ciberataques

credenciales de acceso y contraseñas en texto sin formato de todos los dispositivos protésicos y sus administradores); manipular, agregar o eliminar dicha información y agregar o eliminar usuarios regulares o con privilegios de administrador.

Los avances en conectividad móvil ya han tenido un gran impacto en los estilos de vida de los consumidores, especialmente dada la adopción generalizada de dispositivos IoT y dispositivos inteligentes. Pero el aumento en la popularidad de estos dispositivos también ha atraído el interés de los actores maliciosos que buscan acceder a las redes de los usuarios. Avast anunciaba los resultados de un estudio, Avast Smart Home Report 2019, que concluye que dos de cada cinco hogares digitales son vulnerables a los ciberataques. Según el informe el 40,3 de los más de 16 millones de hogares analizados, tienen más de cinco dispositivos inteligentes, un 45,6% en el caso de España, y que un 40,8%, o 35,1% en España, tienen al menos un dispositivo vulnerable. “Esto ilustra la cantidad de hogares que corren riesgo con los dispositivos de Internet de las cosas, ya que solo se necesita un dispositivo vulnerable para comprometer la seguridad de toda la red doméstica”, dice Avast en su informe.

Se descubrió que la mayoría de los dispositivos vulnerables (69,2%) en hogares en todo el mundo, el 65% en España, son vulnerables debido a la debilidad de las credenciales. Además, un 31,8% de estos dispositivos en todo el mundo, o el 35,6% en España, son vulnerables debido a que no se les aplicó un parche.

MWC Security 2019, las tribunas

El despliegue para la cobertura del Mobile World Congress realizado por IT Digital Media Group estableció la publicación de tribunas de opinión que mostraran una visión personal de la feria, la otra cara del Mobile, cómo se reflejan las TI y el negocio y, como no podía ser de otra manera, la seguridad del MWC.

Puedes acceder a las tribunas sobre seguridad en los siguientes enlaces:

- La ciberseguridad también está de moda en el MWC
- No sin mi móvil
- IoT, el ejército durmiente
- La seguridad biónica también tiene cabida en MWC

5G abre nuevas oportunidades para el compromiso y la productividad de los empleados

En España los dispositivos del hogar más vulnerables son: dispositivos de red, como routers. (25,9%); Impresoras (25,1%); NAS, sistemas de almacenamiento (21%); Cámaras de seguridad (20,1%) y Media Streaming (4.6%).

Ya decíamos que el 5G ha sido estrella inequívoca del MWC. La quinta generación de redes móviles está en la mente de todos los proveedores de servicios de comunicaciones (CSPs por sus siglas en inglés). Entre otras cosas, 5G abre nuevas oportunidades para el compromiso y la productividad de los empleados, haciendo que los móviles e informática remota sean cada vez más disponibles a más dispositivos y más aplicaciones.

En su paso por la feria de Barcelona, VMware ha mostrado las ventajas de su Workspace ONE, que permite la gestión y seguridad de todos los dispositivos de los clientes, dispositivos basados en SIM vendidos por los operadores a las organizaciones de negocios (propiedad de la corporación), dispositivos que son propiedad del empleado (BYO) y endpoints (no-SIM) como MacBooks y PCs.

F5 Networks mostraba en MWC 2019 soluciones diseñadas específicamente para ayudar a los proveedores de servicios a funcionar de manera más rápida, inteligente y segura a medida que incorporan nuevas tecnologías. En particular, las ofertas de F5 abordan los desafíos relacionados con el aumento del tráfico de datos desde la aparición de 5G y la creciente presencia de IoT comercial y de consumidores.

Explicando que según uno de sus informes más de la mitad de los proveedores de servicios encuestados (55%) creen que IoT es la tendencia más importante desde el punto de vista estratégico en los próximos dos a cinco años. Un 83% dijo que tenía

AVAST SMART HOME REPORT 2019

Según este informe de Avast dos de cada cinco hogares digitales son vulnerables a ciberataques. El Avast Smart Home Report 2019 contiene información de más de 16 millones de redes de hogares inteligentes, revelando que el 40,3% de los hogares en todo el mundo tienen más de cinco dispositivos inteligentes conectados (EEUU: 62,0%, España: 45,6%) y el 40,8% de estos hogares digitales en todo el mundo; (EEUU: 35,2%, España: 35,1%) contiene al menos un dispositivo conectado vulnerable. Esto ilustra la cantidad de hogares que corren riesgo con los dispositivos de Internet de las cosas, ya que solo se necesita un dispositivo vulnerable para comprometer la seguridad de toda la red doméstica.

proyectos de transformación digital en marcha, y el 56% de estos proyectos ya han influido en una mayor automatización y orquestación de los sistemas y procesos de TI.

Las nuevas soluciones de F5 para los proveedores de servicios incluyen el BIG-IP i15000 Series, que ofrece un rendimiento de alta calidad para la seguridad y los servicios en un formato compacto (2 RU). El i15000 permite la consolidación de múltiples servicios en un solo dispositivo, incluido el equilibrio de carga, la optimización de TCP/IP, la dirección de tráfico, DDoS, CGNAT, DNS y las capacidades de firewall en el Gi LAN o centro de datos.

Por otra parte, Trend Micro ha aprovechado la celebración del Mobile World Congress para presentar Trend Micro Consumer Connect, una suite de seguridad completa diseñada para que las empresas de telecomunicaciones lo implementen a fin de proteger mejor a sus usuarios. La solución protege la vida digital completa de los clientes contra amenazas conocidas y desconocidas al colocar una capa de seguridad virtual alrededor de los dispositivos. Trend Micro Consumer Connect es altamente escalable, fácil de integrar y fácil de implementar, y añade una ventaja competitiva para los proveedores de telecomunicaciones.

Trend Micro Consumer Connect protege contra el ransomware, las amenazas de día cero, los troyanos de robo de información, la extracción de criptomonedas y otras amenazas online diseñadas para comprometer los endpoints de IoT, cubriendo todos los dispositivos domésticos inteligentes, además de PC y móviles.

Este año la presencia de Fortinet en MWC se ha centrado, a grandes rasgos, en tres temas: asegura el camino hacia 5G, IoT y SD-WAN.

En lo que respecta a 5G, dice la compañía que su adopción requiere pasar de una infraestructura predominantemente física a una virtualizada en gran medida. “Si bien la agilidad y flexibilidad resultantes permiten a los operadores responder mejor a las

Los avances en conectividad móvil ya han tenido un gran impacto en los estilos de vida de los consumidores, especialmente dada la adopción generalizada de dispositivos IoT y dispositivos inteligentes

nuevas demandas de los clientes, también requieren que la seguridad se implemente como funciones de red virtual (VNF)". Estas funciones de red virtualizadas necesitan interoperar sin problemas con sus soluciones de seguridad física existentes para crear y mantener un único marco de seguridad de alta confianza.

Menciona también Fortinet el Multiaccess Edge Computing (MEC) para señalar que también requiere de seguridad "para funcionar como un componente fundamental y totalmente integrado de ese entorno para garantizar el aislamiento y la protección de amenazas entre las aplicaciones, los servicios y la red móvil central". Sobe el IoT, dice la compañía que tanto las plataformas como los servicios del Internet de las cosas exigen de los operadores móviles una mayor visibilidad y seguridad.

Y por último, dice Fortinet que los proveedores de servicios de seguridad gestionados (MSSP) deben abordar continuamente los desafíos de seguridad de sus clientes comerciales, y que eso conlleva incluir una serie de elementos en sus infraestructuras de seguridad, como es SD-WAN, visibilidad y automatización, protección avanzada contra ameneza o UEBA o análisis de conductas de entidades y usuarios.

Caminemos hacia 5G, adoptemos la movilidad, integremos el IoT en nuestras empresas y hogares, y permanezcamos atentos y hagamos de la ciberseguridad una prioridad.

Enlaces de interés...

- Especial Mobile World Congress 2019
- Kaspersky Lab muestra en MWC los escenarios de la ciberseguridad del futuro
- Android, el Dorado de los ciberdelincuentes

IMPULSANDO LA INDUSTRIA 4.0

NUEVOS RETOS, NUEVAS SOLUCIONES

Fabricación Aditiva

Big Data

Cloud Computing

Sistemas Ciber-físicos

CIBERSEGURIDAD

AUTOMATIZACIÓN

DIGITALIZACIÓN

Ciberseguridad

Visión Artificial

Internet of Things

Robótica

Simulación

www.gmv.es

gmv®
INNOVATING SOLUTIONS

“Los clientes no van a utilizar tecnología en la que no confían”

(Microsoft)

Pocos consideran a Microsoft como una empresa de seguridad, y sin embargo lleva la seguridad en su ADN, desde que hace más de dieciséis años Bill Gates formulara su Trustworthy Computing Initiative. Hoy nos reunimos con Héctor Sánchez Montenegro, el National Technology Officer de Microsoft, la persona responsable del negocio de seguridad en España, con quien hablamos de la aproximación, holística, de la compañía al mundo de la seguridad.

Rosalía Arroyo

15 de enero de 2002, martes, cinco y veinte de la tarde, los miles de empleados de Microsoft reciben un email de Bill Gates, co-fundador y entonces CEO de la compañía, hablando sobre una nueva iniciativa, Trustworthy Computing. Ente los mensajes de Gates, que la informática se había convertido en una parte importante de la vida de muchas personas, y que en diez años iba a ser una parte integral e indispensable de prácticamente todo lo que hagamos; el memorándum, publicado íntegro por Wired.com, destacaba también la

importancia de la disponibilidad, la seguridad y la privacidad.

El mensaje de Trustworthy Computing lanzado por Bill Gates hace dieciséis años, que promovía la seguridad por diseño, por defecto y en el despliegue, sigue vigente. “Sabemos perfectamente que los clientes no van a utilizar tecnología en la que no confían”, asegura Héctor Sánchez Montenegro, National Technology Officer de Microsoft, durante una entrevista en la que empezamos planteando que se ve menos a Microsoft en temas de seguridad que lo que sería previsible para una empresa que Gartner lleva años colocando en su cuadrante de líderes del mercado CASB, o que tiene un peso importante en el mercado de seguridad endpoint.

Recuerda Montenegro la presencia de Microsoft como partner Platinum en las jornadas del CCN CERT del pasado mes de diciembre, “el evento de seguridad más importante de España”, con más de 2.500 asistentes. Dice también el directivo que Microsoft es una de las compañías tecnológicas que más invierte en seguridad: 1.000 millones de dólares anuales, “que se traducen en productos, tecnologías y servicios que refuerzan el resto de propuestas que tiene Microsoft en diferentes ámbitos”, añadiendo después que aunque Microsoft no sea una empresa de nicho en seguridad, como pueda ser un Symantec o un Panda, “nosotros tenemos una aproximación holística y planteamos la seguridad integrada y como servicio horizontal en el resto de productos de la compañía”.

Tiene claro el National Technology Officer de Microsoft Iberia que los clientes no utilizan tecnología

en la que no confían y por esto “tenemos claro que lo primero es construir soluciones que generen de forma real confianza en los usuarios antes de considerar otras capacidades y características por muy ‘cool’ que estas sean; nadie arriesga sus datos o servicios en algo en lo que no confía”.

Oferta de seguridad

Explica Héctor Sánchez Montenegro que hay cuatro escenarios en los que se despliegan las diferentes soluciones de seguridad de Microsoft, y el primero de ellos es la gestión de identidades y la autenticación. Asegura Sánchez Montenegro que el perímetro es la identidad de los usuarios, y por lo tanto el reto está en “ser capaz de generar una identidad ro-

"Los millones de sistemas Windows repartidos por todo el mundo son sólo una de las fuentes que alimentan nuestro Security Graph"

busta y lo suficientemente fuerte como para poder autorizar a esa persona a acceder a la información que le corresponda, y no autorizar a otra". Para que sea robusta, la autenticación debe ir más allá de las contraseñas, "ir a otro tipo de autenticaciones con otros parámetros, como el doble factor de autenticación, biométricos, accesos condicionales…". De forma que dotar a los sistemas de criterios de validación en el proceso de autenticación diferentes a los habituales es parte de la propuesta de seguridad que cubre ese primer gran bloque de tecnologías de la compañía.

Un segundo escenario tiene que ver con la detección de amenazas, o Advaced Threat Protection. Explica el directivo de Microsoft que hay que combatir la amenaza, y hacerlo tanto en la parte de detección como en la parte de prevención y en la parte de respuestas; "no puedo tardar tres días en saber lo que tengo que hacer, tengo que automatizar las respuestas, las decisiones".

El tercer gran bloque donde Microsoft posiciona sus soluciones de seguridad tiene que ver con la protección del dato, de la pieza de información. Se trata de proteger la información que hemos creado a partir de cualquier tipo de dispositivo y en todo su ciclo de vida. "Tenemos propuestas para facilitar esa capacidad de control de la información en cualquiera que sea su estado, en cualquier momento", dice Héctor Sánchez, añadiendo que esto es muy útil y tiene una relación directa con todo el tema de cumplimiento, porque el marco regulatorio pasa por saber quién genera la información, cuándo se ge-

LA SIGUIENTE ETAPA DE LA INFORMÁTICA DE LA CONFIANZA

El 15 de enero de 2002, Bill Gates envió un memorándum a todos los empleados de Microsoft en el que se anunciaba la iniciativa Informática de confianza (TwC, Trustworthy Computing). Este documento lo analiza.

En el memorándum, destacaba la importancia de ofrecer una informática "tan confiable y segura como los servicios de electricidad, agua y telefonía", y señalaba que los aspectos clave de una plataforma confiable son la disponibilidad, la seguridad y la privacidad. También dejaba claro que la iniciativa no se refería a la tecnología únicamente: "Hay muchos cambios que Microsoft debe realizar como empresa para garantizar y proteger la confianza de nuestros clientes en todos los niveles, desde la forma de desarrollar nuestro software a la asistencia técnica y las prácticas operativas y comerciales".

nera, si incluye información sensible o no para, en función de esa sensibilidad, darle unas mediadas u otras. Es lo que la compañía de Redmond llama Information Protection, bajo la cual se despliegan toda una serie de soluciones.

Y finalmente hay una cuarto área que busca poner orden en todo eso. “Se trata de contar con una consola única que nos permita ver cuál es mi estado de la seguridad con respecto a las diferentes preguntas que se pueden hacer: si tengo la información correctamente protegida, si tengo los SIEMs integrados perfectamente, y si con esa enorme cantidad de datos puede sacar inteligencia y aplicar nuevas capacidades”, explica el directivo. Aquí se trabaja con sistemas de inteligencia artificial que puedan ayudar a sacar conclusiones de la enorme cantidad de datos que se manejan en cada uno de estos cuatro escenarios.

Estos cuatro escenarios, o bloques, “es la forma de comprender la oferta de seguridad de Microsoft, que pensamos que cubren el total de posibles necesidades que un CISO pueda tener y además en cada uno de los tres aspectos, desde la detección, desde la protección, desde la respuesta”, asegura Héctor Sánchez Montenegro, añadiendo que es efectivo para todo tipo de clientes, “porque cualquier cliente necesita todo eso”.

El endpoint y la pérdida de perímetro

Reina en el mundo del endpoint a través de su sistema operativo, la compañía decidió añadir un plus de seguridad, algo que empezaban a demandar los usuarios ante el incremento y variedad de los virus.

> "En un tema tan fundamental y tan importantísimo como es el de la seguridad, que lo es todo, no podemos tener una dependencia al 100% de soluciones de terceros"

En diciembre de 2004 se compraba la compañía GIANT que contaba con un producto AntiSpyware, en el que se basó Windows Defender, anunciado por Bill Gates en la conferencia RSA de 2005, para todos los usuarios de Windows 2000, Windows XP y Windows Server 2003 con licencia válida y con el objetivo de ayudar esos usuarios a asegurar sus sistemas contra la creciente amenaza de malware.

Windows Defender fue sustituido en 2008 por Microsoft Security Essentials, nombre en clave Morro, que también sustituyó a Windows Live Care, la propuesta de pago de la compañía.

Recuerda Héctor Sánchez Montenegro que “hubo mucho debate al inicio sobre si Microsoft iba a competir con otro tipo de servicios antivirus”. El debate se extendió a la Bolsa, donde las acciones de Symantec cayeron un 9,44% y las de McAfee un 6,62% después de que Microsoft anunciara públicamente Morro en noviembre de 2008, y eso a pesar de que se dijo que Security Essentials no competiría directamente con otros programas antivirus de pago. Hoy el mensaje es que hay espacio para todos, y que “todos los fabricantes de antivirus son partners muy estrechos de Microsoft”. Dice también Montenegro que, “en un tema tan fundamental y tan importantísimo como es el de la seguridad, que

lo es todo, no podemos tener una dependencia al 100% de soluciones de terceros. Trabajamos muy bien con soluciones de terceros, pero necesitamos tener una propuesta propia e implícita al sistema que sea capaz de dar una respuesta directa y mostrar un valor directo a los clientes. Y eso es así. Ahora mismo no existe la opción de tener un sistema de puesto de trabajo sin este tipo de soluciones".

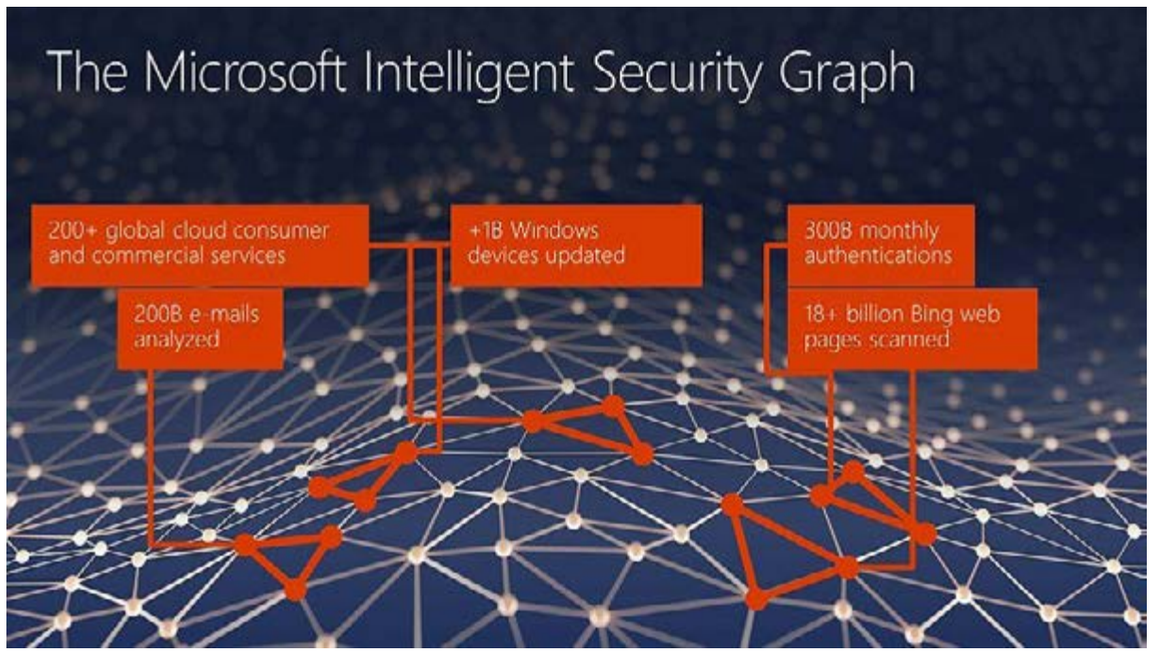
La pérdida de perímetro, que colocó a los endpoint detrás de la línea de los firewalls, ha vuelto a darle protagonismo a esos puntos finales. Según datos de NetMarketShare, la cuota de Windows en el mundo del PC era del 87,56 en enero de 2019, seguida de Mac OS (9,68%) y Linux (2,14%). Y teniendo en cuenta que la información es poder, planteamos a Héctor Sánchez Montenegro si la situación les coloca en una posición de ventaja frente a fabricantes de seguridad tradicional. "Yo creo que estamos en esa posición inigualable precisamente por ese tema, porque efectivamente cuando algunos hablan de sondas, nosotros hablamos en términos de puestos de trabajo; podemos tener un número mayor de señales que nos ayudan a capturar y esto lo posicionamos como un auténtico valor diferenciador de muchas propuestas", dice el directivo, añadiendo que debido a esa cantidad de señales "somos capaces de tener algo más que una estadística, tenemos una foto real", a lo que se suman la capacidad de analizar todas esa información, "que la tenemos".

Microsoft Intelligent Security Graph

Los millones de sistemas Windows repartidos por todo el mundo "son solo una de las fuentes que alimentan nuestro threat de inteligencia, nuestro Security Graph".

Lo que hace Microsoft Intelligent Security Graph es recopilar toda la telemetría de cada una de las aplicaciones de Microsoft. A partir de ahí y aplicando modelos de machine learning, la compañía genera alertas, así como opciones de remediación. Explica Héctor Sánchez Montenegro que además de alimentarse de toda la información que llega de los endpoint, lee otras fuentes de información, que lo mismo a priori se piensa que no tiene nada que ver con la seguridad, como es Bing. "Independientemente de que lo use más o menos gente, Bing hace su función semanal de indexar millones de páginas para luego dar el servicio de búsqueda adecuada, y en esa tarea también es capaz de detectar cantidad de sites maliciosos que están esperando la llegada de un incauto", dice el directivo de Microsoft. A este Security Graph también llega información de otros sistemas de la compañía, como Hotmail, desde donde se pueden detectar niveles de spam, o de phishing, así como las señales derivadas del uso profesional de entornos de Office 365.

> "Para que sea robusta, la autenticación debe ir más allá de las contraseñas, ir a otro tipo de autenticaciones con otros parámetros, como el doble factor de autenticación, biométricos, accesos condicionales..."



Toda esta información compone un Threat de Inteligencia "que es probablemente el mayor que puede existir actualmente en el mundo, por la

dimensión de la plataforma y la cantidad de señales que se pueden encontrar". Ese Threat de Inteligencia cuenta con una API muy elaborada para que los propios productos y servicios de Microsoft de esas cuatro categoría estén permanentemente chequeando y leyendo en tiempo real de esa información, "y tomando decisiones en tiempo real que son ajustadas y adecuadas a la amenaza que puede existir en el preciso momento, porque es en tiempo real. Y todos y cada uno de los servicios, están leyendo de esa información. Pero no solo eso, esa API se comparte para que nuestros socios y partners también generen otras soluciones de valor que puedan alimentarse de esa capacidad de Microsoft, porque pensamos que en la parte de seguridad sólo podremos tener éxito si somos capaces de colaborar".

Hablamos también con Héctor sobre el número de socios de la compañía que venden las soluciones de seguridad. Todos. "Todos los partners venden seguridad en la capa básica o en la más avanzada", dice Montenegro, y explica que en tanto en cuanto todos posicionan soluciones de cloud en el mercado, y todas las soluciones llevan implícitas opciones de seguridad de mayor o menor alcance en función de la categoría de la solución, es normal que todos tengan la seguridad como uno de sus activos. "Tenemos muy identificados los partners que aportan más en el negocio de la seguridad de Microsoft", dice el directivo de la compañía, que a riesgo de no nombrarlos a todos menciona a PwC, Deloitte, KPMG o Accenture.

Sobre la evolución del negocio de seguridad de la compañía, dice Héctor Sánchez Montenegro que con una inversión anual de mil millones, "lógicamente esperamos recuperar la inversión". Explica que las áreas de negocio más afectadas por el crecimiento en el área de la seguridad, y que van de la mano del crecimiento global, tienen que ver con el modern workplace, cuyo crecimiento ha sido en el último trimestre del 34%. "La cifra de crecimiento del negocio de seguridad no es muy diferente", reconoce, asegurando que "nuestro éxito en modern workplace va de la mano de nuestro éxito en seguridad, con una horquilla del +-5%, lo que supone que el crecimiento del negocio de seguridad pueda establecerse entre el 30-40%".

Enlaces de interés...

- Microsoft Security Blog
- Microsoft advierte de ciberataques contra las instituciones democráticas europeas
- Microsoft lanza un programa de Bug Bounty para Azure DevOps

Compartir en RRSS

smartLogin

wbsgo

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

¿Es fácil recobrar la confianza tras un gran fallo de seguridad?

El último gran error que ha atentado contra la privacidad de los usuarios de Internet ha sido el del FaceTime de Apple. Antes, Facebook, Hoteles Marriot, Yahoo!, Tesla, Telefónica o Equifax, por poner algunos de los ejemplos más sonados, también tuvieron fallos similares. ¿Se recupera una empresa de un golpe así? Hablamos con expertos en seguridad sobre ello.

Bárbara Bécares

Un chaval de solo 14 años descubrió a finales del mes de enero que una falla de seguridad existente en Facetime, una aplicación de telefonía con video para los dispositivos iPhone, iPad, Mac y iPod touch, permitía escuchar a otras personas en sin que estas llegasen a aceptar la petición de una llamada grupal. Un error muy grave en la privacidad de los usuarios de una de las más grandes y prestigiosas empresas del mundo: Apple.

En el momento del descubrimiento, Victor Chebyshev, analista de seguridad en Kaspersky Lab,

explicó que, según lo que se había reportado en los medios de comunicación, “parece difícil para un ciberatacante explotar este bug capaz de vigilar a sus objetivos, ya que la posible víctima recibiría una alerta de llamada entrante. El único escenario de riesgo se da cuando el objetivo usa el modo ‘silencioso’. En este caso, posiblemente se podría escuchar en secreto las conversaciones privadas de un objetivo”.

A raíz de esta historia, desde ITDigital Security, vamos a analizar cómo afecta a la fama de una empresa un fallo de este estilo y qué habría que hacer para sobrevivir en el mercado, en caso de que nuestra empresa pasase por un trago como este. De la mano de Panda Security, Forcepoint y Symantec, hacemos un repaso por otros casos protagonizados por grandes firmas y vemos si se puede uno recuperar de un escándalo así.

Un repaso a otras historias

No solo Facetime y Apple han pasado por un error que les ha puesto en evidencia ante el gran público. Recuerda Julia Barruso, Channel Account Manager Iberia en Forcepoint, que “ha habido numerosos casos y muy sonados como Facebook, Google+, Marriot, Equifax o Tesla”.

Si hablamos de los fallos de seguridad del año 2018, explica María Campos, KA & Telecoms Manager en Panda Security, que “quizás la odiada pole en este aspecto el pasado año, la alcanzase la cadena Marriot debido a la exfiltración de más de 500 millones de datos de huéspedes y clientes, seguida de cerca, entre otros, por el caso de Facebook y Cambridge Analytica con la ‘cesión’ de más de 90 millones de datos de usuarios con fines electorales”.

Si vamos a un año antes, 2017 “fue igualmente dañino con casos de mucho ruido mediático como el de Equifax, que por su magnitud (robo de datos personales de más de 140 millones de personas) se considera otra de las brechas de seguridad más dañinas de la historia reciente. Pensemos que, con los datos de cualquiera de estas exfiltraciones se pueden suplantar identidades tanto en el momento del incidente como en el futuro, en caso de que continúen invariables. No obstante, Yahoo! y sus más de 3000 millones de cuentas robadas del que ya nos enteramos años atrás, fue igualmente impactante” y, otros casos de magnitud igualmente enorme “han sido también los robos de datos de registros de bases de datos menos conocidas para el público en general (Exploit.in, Anti Public, etc) pero con miles de entradas”, continúa recordando María Campos desde Panda Security.

Desde Symantec, Ramsés Gallego Strategist & Evangelist de la firma recuerda que en el pasado

it whitepapers

COPIAS DE SEGURIDAD: UNA GUÍA DE APROXIMACIÓN PARA EL EMPRESARIO

Esta guía proporciona información detallada sobre los aspectos más relevantes de las copias de seguridad, para comprender tanto la importancia de su implantación en las empresas como las distintas soluciones aplicables dependiendo de nuestro modelo de negocio.

Debemos proteger nuestro principal activo, la información, ya que su pérdida podría interrumpir la continuidad de nuestro negocio, así como afectar a la imagen que proyectamos ante nuestros clientes y proveedores.

Si ya realizas copias de seguridad en tu empresa, pero quieres saber si estás siguiendo los procedimientos más adecuados o si todavía no has comenzado a realizarlas, ¡esta es tu guía!

2018, por ejemplo, la empresa de tratamiento de información Exactis sufrió el robo de 340 millones de registros personales que fue, en su momento, hace escasos meses, el de mayor volumen de la historia. Sin embargo, el mismo año, una empresa mediática como Facebook reconoció el acceso de terceros a más de 30 millones de cuentas y perfiles de usuario". Además de estos casos tan escuchados, explica Gallego que "la mayor brecha de datos personales de la historia se ha conocido en este 2019 en lo que se ha decidido llamar como Collection#1, con 773 millones de cuentas de correo y sus contraseñas accedidas de manera no controlada". Lo terrible de esto, relata el experto, "es que, además, parece ser que existen otras 'colecciones' (llamadas Collection #2-5) con 25 mil millones de entradas que, eliminando duplicados y errores pueden suponer 750 millones de credenciales completamente nuevas".

Si nos remontamos a años anteriores y a grandes ataques que formarán parte de nuestra historia, dice María Campos que "no podemos olvidar los mediáticos ataques de ransomware como WannaCry con impacto en cerca de 150 países e infraestructuras afectadas, como hospitales, Petya o Bad Rabbit que a través del cifrado de datos dejaban inservibles los terminales correspondientes hasta el replataformado de los mismos (o pago del rescate -al que muchos accedieron).

¿Cómo daña la reputación un gran fallo de seguridad cuando sucede en una gran empresa?

El pasado año Facebook sufrió un grave caso que expuso informaciones de millones de personas. Muchos de sus usuarios decidieron irse de una red social que, poco a poco va defraudando a más personas, precisamente por sus ataques a la privacidad. Pero, en general, miles de millones de personas siguen formando parte de la lista de clientes de la que es la mayor red social del mundo (más aún si tenemos en cuenta que WhatsApp e Instagram también está en su haber). ¿A cuántas personas conoce que hayan decidido dejar de usar Facebook tras conocerse el mencionado escándalo del pasado año? El hecho de saber que pueden perder nuestras informaciones y exponer nuestra privacidad, no parece asustar al grueso de la sociedad. Por ejemplo, probablemente los próximos productos y servicios de Apple mantengan sus altos precios a pesar de la gravedad de lo que acaba de suceder con Facetime.

Sin embargo, los expertos en seguridad insisten en que, realmente, un fallo en esta materia supone un precio de gran envergadura y en que la reputación

THE FACETIME BUG

CLICAR PARA VER EL VÍDEO

"Las repercusiones económicas son un hecho, pero aún peor es la pérdida de confianza que estas brechas han causado"

María Campos, KA & Telecoms Manager, Panda Security

de las compañías afectadas siempre está en juego. Ramsés Gallego recuerda que “hemos visto el valor bursátil de una entidad bajar drásticamente por un hecho así, la pérdida de imagen pública y la insatisfacción y pérdida de confianza de los usuarios”.

Cuando hablamos de compañías de gran tamaño, continúa Gallego, “si sufren un ataque masivo que, lamentablemente, tenga éxito, si bien es cierto que un buen número de usuarios se molestará y, quizás, dejan de utilizar sus servicios (temporalmente), no es menos cierto que lo que proponen sigue siendo válido para muchas personas en la sociedad -a veces, incluso necesario- y hablamos de un volumen ingente de consumidores que apenas puede tener un impacto ‘definitivo’ en la cuenta de explotación de la entidad”.

La cuestión es, sin embargo, si esa pérdida de confianza se mantiene en el tiempo o si, por el contrario, es sólo pasajera.

Julia Barruso, Channel Account Manager Iberia en Forcepoint, considera que “el tamaño de las empresas en este caso es irrelevante”, ya que “las repercusiones son las mismas para todas las compañías”.

¿Cuál es la diferencia, pues, para unas y otras? Opina la experta de Forcepoint que “para las firmas de menor tamaño el reto de volver a generar confianza puede llegar a ser mayor”.

Añade Ramsés Gallego desde Symantec que, mientras que “por una parte, la repercusión mediática es mayor, como no podía ser de otra manera”, para las empresas grandes, “su capacidad de ‘recuperación’ también es mayor” ya que tienen más opciones de poner “en marcha estrategias de mitigación que reducen el efecto y limitan, de alguna manera, la acción de la administración porque pueden demostrar que están trabajando en mayores y mejores contramedidas” para hacer frente a la situación.

> "Sugerimos tener un plan de gestión de crisis que debe contener nombres de personas que responderán ante los medios, qué comunicarán o cuáles son las medidas que se están tomando"
>
> Ramsés Gallego Strategist & Evangelist, Symantec

Y recuerda el especialista que “es cierto que una empresa de menor tamaño podría no recuperarse de la pérdida masiva de usuarios ya que su modelo de negocio está dimensionado para cierta volumetría... y la pérdida repentina de confianza de un elevado porcentaje de sus consumidores sí podría ser fatal”.

Desde Panda Security, María Campos anima a las empresas a estar preparadas. No solo a evitar los fallos, sino también a preparar una estrategia para ser capaces de hacer frente a la situación, en el caso de que se dé. “En la medida en que la empresa esté preparada para afrontar la gestión de un incidente de seguridad responderá de una forma más o menos rápida, ordenada y eficaz, minimizando las consecuencias del mismo”, dice la especialista.

De hecho, en el mencionado ejemplo de Facebook, la que sí perdió fue Cambridge Analytica que, como publicamos en nuestras páginas, se declaró en bancarrota (lo que en España llamamos concurso de acreedores).

Cómo reaccionar para que las consecuencias sean menos graves

Un factor que será de gran importancia para el resultado final al que pueda llevarnos un escándalo así es conseguir ser rápidos en la respuesta. En el caso de FaceTime, desde Kaspersky valoraron que “Apple respondiese rápidamente a la notificación

"El único elemento constante desde el inicio de la ciberseguridad son las personas. Las organizaciones pueden mejorar tanto su ciberdefensa como restaurar la confianza entendiendo mejor el comportamiento humano"

Julia Barruso, Channel Account Manager Iberia, Forcepoint

del error". Entre otros asuntos, la compañía con sede en Cupertino desactivó, en cuanto se conoció el problema, "la función de chat en grupo de FaceTime para proteger aún más a los usuarios ante cualquier posible abuso de privacidad".

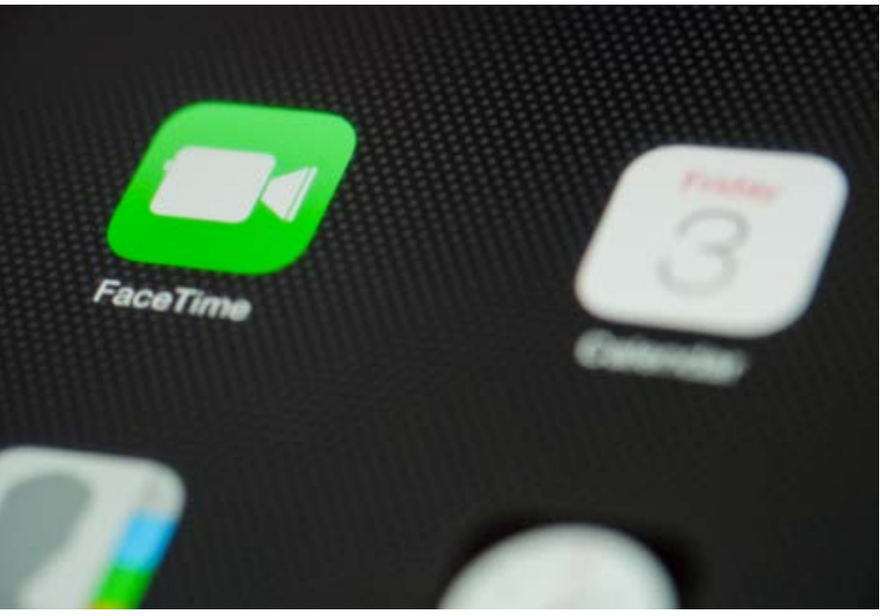
Por otro lado, Ramsés Gallego desde Symantec aconseja tener un buen plan de comunicación, efectivo, eficiente, honesto. "Sugerimos tener un plan de gestión de crisis -que no es habitual, desgraciadamente- que debe contener nombres de personas que responderán ante los medios, qué comunicarán cuáles son las medidas que se están tomando. Ese plan debe contener qué pasos se están siguiendo, cómo se está colaborando, si procede, con las Fuerzas y Cuerpos de Seguridad del Estado, etc. Para recuperar la confianza -que, recordemos es algo que debe ser ganado, algo que los usuarios entregan a sus proveedores y, en consecuencia, subjetiva en su percepción- la empresa debe recuperar el estado anterior al fallo (o mejorarlo) en cuanto a cómo estos perciben los esfuerzos en protección de los datos de sus clientes". Por ejemplo, se puede invertir en tecnología que refuerce la seguridad y la defensa de los sistemas o en mecanismos de monitorización y cifrado y trasladar esa nueva postura de seguridad a los clientes, de acuerdo con las palabras del experto.

"No nos cansamos de repetir la importancia de diseñar un buen modelo de prevención, detección, contención, respuesta y remediación, que permita en cada uno de los casos disminuir el gap entre "haberse visto afectado" y "darse cuenta de haberse visto afectado", continúa María Campos. Y Julia Barruso añade desde Forcepoint que una empresa debe ser capaz de conocer bien al ser humano. Tanto para prevenir, como para restaurar la confianza de las personas: "el único elemento constante desde el inicio de la ciberseguridad son las personas. Las organizaciones pueden mejorar tanto su ciberdefensa como restaurar la confianza entendiendo mejor el comportamiento humano", detalla la experta.

¿Hay elementos legislativos que nos protejan en España?

El fiscal general de Nueva York anunciaba a comienzos de este mes de febrero que investigaría la respuesta de Apple al mencionado error de su aplicación de videochat FaceTime, junto con el Comité de Energía y Comercio del Congreso de los Estados Unidos.

Explica Ramsés Gallego que, en un caso similar, en España el proceso sería más lento, aunque la Administración del Estado tiene herramientas para solicitar qué mecanismos de control tiene una compañía cuando ha sido penetrada por cibercriminales, especialmente por robo de información. "Con el fallo de FaceTime, la administración americana actúa, por una parte, de oficio y, por otra, porque ha habido -desde el primer día- una denuncia contra la compañía", concreta el directivo. "En España, si



bien es cierto que se podría actuar de oficio, dudo que ocurriera con la misma celeridad que en aquel país. Debería, por una parte, existir denuncia y pasar a demostrar de manera inequívoca que ha habido robo de información. Podría articularse que ha habido negligencia y dejadez en la construcción de la aplicación y, como resultado, un código que deja huecos/vulnerabilidades que pueden ser utilizadas por los criminales... pero perseguir eso con nuestra práctica judicial es difícil... aunque no imposible".

Y, cuando hablamos de legislación, no debemos olvidar que contamos ahora con nuevas leyes que rigen grandes países para la protección de los datos personales, como pueden ser el RGPD en Europa o el LGPD en Brasil y que han cambiado el panorama. Recuerda María Campos, directiva en Panda Security, que "si echamos la vista atrás creo que todos coincidiremos en que 2018 será recordado como el año en el que las brechas de seguridad en torno a la protección de datos alcanzaron una mayor dimensión debido a las nuevas regulaciones en este ámbito", y la experta menciona que estas nuevas regulaciones estuvieron "encabezadas sin duda por GDPR –pero que se ha ido replicando en distintas partes del mundo con características similares".

¿Por qué motivo? Como explica la directiva de la empresa de seguridad, la nueva norma obliga a comunicar dicha brecha en el momento del impacto, por lo que lo que hace años podía pasar desapercibido ahora se trata bajo un marco de mayor transparencia.

Estas regulaciones llevan a las empresas a tener que pagar multas por no haber protegido bien la seguridad de sus clientes. Pero, recuerda Campos que las repercusiones económicas son un hecho, pero "aún peor es la pérdida de confianza que estas brechas han causado".

La concienciación sobre la importancia de los datos en el último año, en gran parte gracias a normativas como GDPR en Europa, se ha convertido en un hecho, como recuerda Julia Barruso desde Forcepoint y, sobre este mismo tema, agrega la directiva de Panda Security que esta "concienciación en materia de implementación de medidas de seguridad, ayuda a generar una mayor cultura en ciberseguridad empresarial que exige, entre otras, la comunicación de las violaciones de brechas de seguridad en tiempo y forma".

Así, tenemos que "el nuevo reglamente GDPR obliga a las empresas a notificar la violación de la seguridad de los datos personales a la autoridad de control competente tan pronto se tenga conocimiento de que se ha producido y a más tardar en un plazo de 72 horas. Con este reglamento se ha extendido la obligación de notificar brechas de seguridad a todas las empresas que manejen datos de carácter personal en la Unión Europea, siempre que puedan verse afectados los derechos y libertades de las personas. Además, si de la brecha se derivasen perjuicios graves para los interesados, también habrá que comunicarles la incidencia directamente a ellos para que puedan tomar las medidas correspondientes", recuerda Campos.

Enlaces de interés...

- FaceTime sufre un fallo de seguridad que permite espiar a otras personas
- La Universidad de Valladolid hackeada
- Facebook anuncia medidas para recuperar la confianza de sus usuarios
- Una brecha de seguridad expone datos de empleados de la NASA
- Ocho meses de GDPR

Compartir en RRSS

Un ciberataque puede ser igual de letal para tu negocio. ¿No deberías tomar medidas para protegerlo?

Así es, un ciberataque puede tener graves consecuencias para tu empresa: pérdidas de información, espionaje industrial, paralización de la actividad, mala reputación, pérdidas de negocio, problemas frente a la ley…
Por eso en Sarenet, a través de nuestras **Soluciones de Seguridad Gestionada**, te facilitamos mecanismos de ciberdefensa que cubren todas las posibles superficies de ataque a las que estás expuesto. Con la tecnología más avanzada y técnicos especializados, que mantienen un servicio de vigilancia permanente y reaccionan eficazmente ante cualquier indicio de amenaza.

902 239 076 comercial@sarenet.es

sarenet
Conectamos con tu empresa

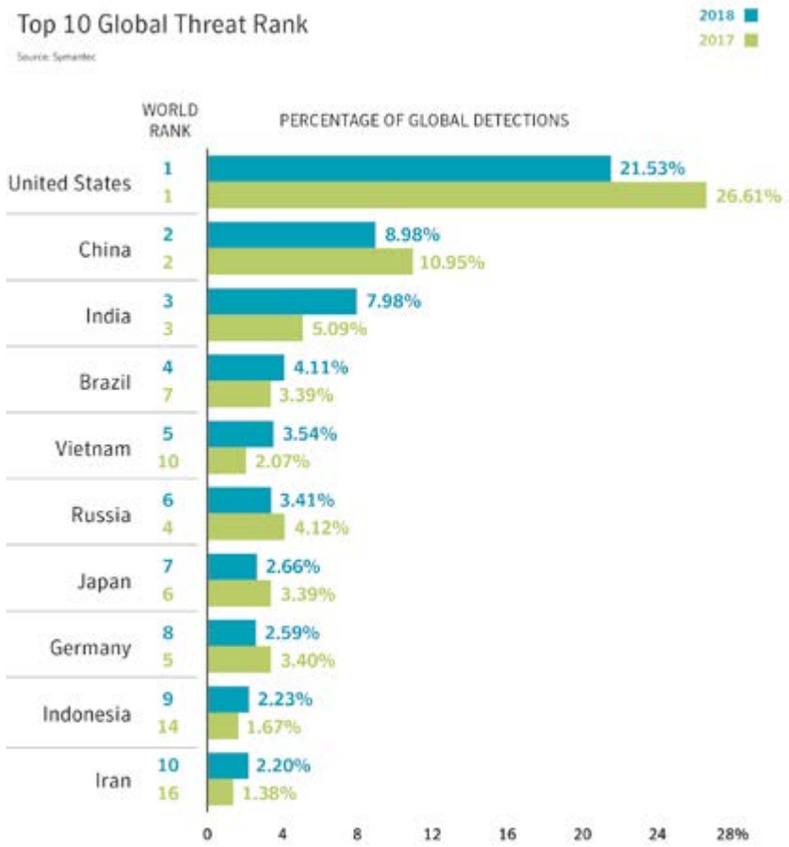
Los cibercriminales encuentran nuevos terrenos de juego

Presenta Symantec el vigésimo cuarto volumen de su ISTR, un informe sobre las amenazas para la seguridad de Internet que revela que los ataques son, en general, más ambiciosos, destructivos y sigilosos para las empresas. De ello hablamos con Ramsés Gallego, Security Strategies de la compañía, quien asegura que sí, que es cierto que lo que refleja el informe es que vamos a peor, que los cibercriminales "encuentran nuevos terrenos de juego, variaciones en la forma de atacar, innovación en el ataque".

El informe recoge que los ingresos procedentes del ransomware y el cryptojacking han disminuido, lo que ha llevado a los ciberdelincuentes a apostar por métodos alternativos, como el formjacking, para conseguir dinero.

Sobre el formjacking dice Ramsés Gallego que es digitalizar lo que ya se estaba haciendo cuando se clonaban tarjetas bancarias; "la gran tragedia es que lo han llevado al mundo virtual, de forma que cuando transaccionamos con algunas páginas web y damos todos nuestros datos, aunque sí se recibe lo que se ha comprado, la información está siendo enviada a otro lugar", explica Gallego, añadiendo que le parece terrible que el informe de Symantec haya detectado que, de media, unas 4.800 webs al mes, webs legales, se vean comprometidas con el formjacking.

España ocupa al octavo puesto en el ranking europeo de amenazas detectadas



Dice el ISTR 24 que aunque numerosos sitios web de pago online muy conocidos, incluyendo Ticketmaster y British Airways, fueron comprometidos con código de formjacking en los últimos meses, las tiendas de pequeño y mediano tamaño son, de largo, las más comprometidas. Según estimaciones conservadoras, los ciberdelincuentes podrían haber recolectado millones de dólares en el último año, robando información financiera y personal de los consumidores a través del fraude con las tarjetas de crédito y las ventas en la dark web. Solo 10 tarjetas de crédito robadas de cada sitio web comprometido podrían generar 2,2 millones de dólares cada mes, y una sola tarjeta de crédito alcanza un precio de 45 dólares en el mercado negro. Con más de 380.000 tarjetas de crédito robadas, solo el ataque a British Airways podría haber permitido ganar a los delincuentes 17 millones de dólares.

El ransomware y el cryptojacking descendieron en 2018. Explica Symantec en su informe que aunque en los últimos años, el ransomware y el cryptojacking, con los que los ciberdelincuentes tratan de robar potencia de procesamiento y uso de CPU a consumidores y empresas para minar criptomonedas, fueron los métodos más atractivos para los atacantes que querían hacer dinero rápido, 2018 trajo un descenso en la actividad. Dice Ramsés Gallego que la tendencia tiene que ver con la cotización de Monero, que es una de las criptodivisas utilizadas en las campañas de ransomware; “la pendiente de descenso de decrecimiento del ransomware es razonablemente similar al precio del dinero en el mercado de Monero. Esto quiere decir que si en enero de 2018 era muy lucrativo hacer ataques de ransomware y pedir rescate en esta criptodivisa, una vez que el precio en ese mercado ya no es tan lucrativo hay una disminución en los ataques de ransomware”, lo que lleva

Con más de 380.000 tarjetas de crédito robadas, solo el ataque a British Airways podría haber permitido ganar a los delincuentes 17 millones de dólares

al siguiente planteamiento: "…de ahí la necesidad de buscar un nuevo terreno de juego, como es el formjacking, ataques a la cadena de suministro, se siguen explotando las vulnerabilidades que existen en las plataforma comerciales, etc.". Concluye el estratega de Symantec asegurando que en muchas ocasiones "los ciberdelincuentes no tienen que inventar nada. Se aprovechas de los agujeros existentes".

Recoge el informe que aunque las infecciones de ransomware se redujeron un 20%, aún así, las empresas no deberían bajar la guardia, ya que las infecciones de ransomware en empresas crecieron un 12% en 2018, rompiendo la tendencia descendente general y demostrando que el ransomware es una amenaza vigente para las organizaciones. De hecho, más de ocho de cada diez infecciones de ransomware impactan en empresas.

En cuanto al cryptojacking, alcanzó su máximo a principios de año y se redujo en un 52% a lo largo de 2018. Incluso con los valores de las criptomonedas cayendo en un 90% y una significativa reducción de la rentabilidad, el cryptojacking continúa, no obstante, manteniendo su atractivo para los atacantes debido a su baja barrera de entrada, la carga mínima y el anonimato que ofrece.

Sobre el Spear phishing, una lacra que no tiene visos de descender, dice Ramsés Gallego que

¿Cuándo la seguridad se convirtió en ciberseguridad?

"No nos dimos cuenta", responde Ramsés Gallego a esta pregunta que el propio Security Strategies de Symantec planteaba no hace mucho en una de sus muchas conferencias.

¿En qué momento la seguridad empezó a ser ciberseguridad? ¿en qué momento los ataques empezaron a ser ciberataques? ¿en qué momento la resiliencia empezó a ser ciberresiliencia? ¿en qué momento la guerra empezó a ser ciberguerra? La respuesta a estas preguntas es que no lo sabemos porque no nos dimos cuenta, explica Gallego.

Todo empezó cuando conectamos los sistemas, cuando los datos empezaron a fluir hacia la nube, en la nube… ahora estamos en la etapa de madurez de internet "y el momento de la ciberseguridad aparece sin nosotros darnos cuenta". Añade el directivo que Symantec trabaja a cinco, siete años vista, intentando averiguar lo que va a ocurrir, pero que la pregunta nos la hemos hecho demasiado tarde. "Y el ISTR lo que hace es demostrar que los malos no van a parar, que esos cibercriminales serán malos, pero no son estúpidos y utilizan técnicas que les funcionan, e innovan".

Nos hacemos las preguntas demasiado tarde, insiste Ramsés Gallego. El ejemplo, la cantidad de controles de seguridad que puede pasar un juguete que se conecta a la red. Sabemos que el pelo no es tóxico, que no hay piezas pequeñas que puedan desprenderse y ser un peligro… "pero nadie ha pensado en los problemas relacionados con la ciberseguridad del juguete".

Sobre si la solución pasa por adoptar modelos de DevSecOps, dice Ramsés que le parece "fundamental", añadiendo que "los desarrolladores, que son excelentes profesionales" no suelen hacerse preguntas relacionadas con la seguridad de las aplicaciones, desde cómo se garantiza la seguridad del acceso, a quién puede manejar los datos.

it whitepapers

ISTR
VOLUME 24 SUMMARY

Resumen del ISTR 24, el informe de Symantec que ofrece información sobre la actividad global de amenazas, las tendencias cibernéticas, las motivaciones de los atacantes y otros acontecimientos en el panorama de amenazas en 2018.

El informe de este año, en particular, revela que el secuestro de formularios, o formjacking, se ha convertido en la amenaza revolucionaria de 2018. Esta amenaza mostró un crecimiento explosivo a fin de año, asegurando que seguiremos viendo su avance en 2019.

Si bien ya no es dinero fácil, el ransomware y el cryptojacking no han desaparecido. El ISTR muestra que con la disminución del valor de las criptomonedas, enriquecerse rápidamente a través del cryptojacking no es tan fácil como antes, y algunos atacantes han pasado a actividades más lucrativas.

aunque haya mejorado la concienciación, la superficie de ataque crece, y por tanto el volumen también. "El correo es casi una plataforma de colaboración en la que además del correo hay adjuntos…", lo que les convierte en un interesante objetivo para los ciberdelincuentes, que además hacen uso de amenazas combinadas: un correo electrónico, con un adjunto que es un PDF y en principio parece inofensivo y que te lleva a una página web que en realidad es la maliciosa, explica Gallego, añadiendo que eso significa que de nuevo hay que proteger en multivector, es decir proteger el correo, y además la navegación, y además proteger a qué nube te lleva.

El 52,9% del total de emails en circulación en España contiene spam

El ISTR 24 recoge que los ataques de phishing son dirigidos en su mayoría al pequeño comercio (1 de cada 488), fabricantes (1 de cada 2.048) y sector financiero y asegurador (1 de cada 2.742). Las empresas con entre 1501 y 2500 empleados son las más afectadas, ya que 1 de cada 2.153 correos contiene ataques de phishing.

Si hablamos de forma más genérica de los ataques de mail, el 52,9% del total de emails en circulación en España contiene spam. Por su parte, las amenazas de malware están presentes en 1 de cada 510 correos electrónicos y el phishing, en 1 de cada 3.680 emails (más del doble que el año anterior, cuando la proporción era de 1 de cada 6.929 emails). Por sectores, los más afectados por el spam son la construcción (66,4%), la fabricación (59,6%), el retail (59%), las administraciones públicas (58,8%) y las entidades financieras y aseguradoras (54,2%). El porcentaje más alto se da en las compañías con entre 501 y 1000 empleados, en las que el 58,5% del correo es spam.

Los smartphones podrían considerarse el mayor dispositivo de espionaje creado hasta la fecha

También recoge el informe datos sobre el IoT asegurando que el perfil de los ataques IoT está cambiando radicalmente ya que no sólo se centran en routers y cámaras conectadas, ya que casi todos los dispositivos IoT, incluidas las bombillas inteligentes o los asistentes de voz han demostrado ser vulnerables y crean puntos de entrada adicionales para los atacantes.

Asegurando que con sus cámaras, micrófonos y localizadores los smartphones podrían considerarse el mayor dispositivo de espionaje creado hasta la fecha, la investigación de Symantec dice que el 45% de las apps de Android más populares y el 25% de las apps de iOS más descargadas solicitan la información de ubicación; el 46% de las apps más populares de Android y el 24% de las de iOS solicitan permiso para acceder a la cámara del dispositivo, y las direcciones de correo electrónico se comparten con el 44% de las principales apps de Android y el 48% de las apps más populares de iOS.

Enlaces de interés...

- 2019 Internet Security Threat Report – ISTR24
- Una oleada de ataques DNS afecta a entidades de todo el mundo
- Los ataques más extendidos están dirigidos y bien planificados
- El volumen de ataques DDoS superiores a 10Gbps se duplicó en 2018

Compartir en RRSS

CURSO CYBERSECURITY FUNDAMENTALS

ABIERTO PLAZO DE MATRICULACIÓN

PLAZAS LIMITADAS

INICIO 8 DE FEBRERO DE 2019

DCNC Sciences

Universidad Rey Juan Carlos

www.master-dcncsciences.com

Los ‘yahoo boys’ crecen:

del spam de las cartas nigerianas a la ingeniería social

Los estafadores nigerianos, más conocidos como ‘Yahoo Boys’, han evolucionado del envío masivo de spam fraudulento al negocio de robo de datos bancarios, suplantación en redes sociales, clonación de webs y el compromiso de mails corporativos. Nueve de cada diez grupos criminales dedicados a los ataques BEC operan desde el país africano.

Jaime Velázquez

Todo aquel que tenga un correo electrónico y mire en su bandeja de ‘spam’ encontrará decenas de mensajes procedentes de una viuda de un jefe de Estado africano o de un enigmático hombre de negocios reclamando desesperadamente ayuda para la transferencia de enormes sumas de dinero hacia mercados fiscales más estables en Europa o Estados Unidos.

Lo único que uno debe hacer para obtener un porcentaje de esa fortuna es colaborar en la transacción, facilitando sus datos personales y bancarios. Y pese a las faltas de ortografía y lo inusual de la oferta, funciona. Los nigerianos son los reyes del ‘spam’ y han explotado la fórmula con numerosas variantes como los anuncios de ‘romance’, donde

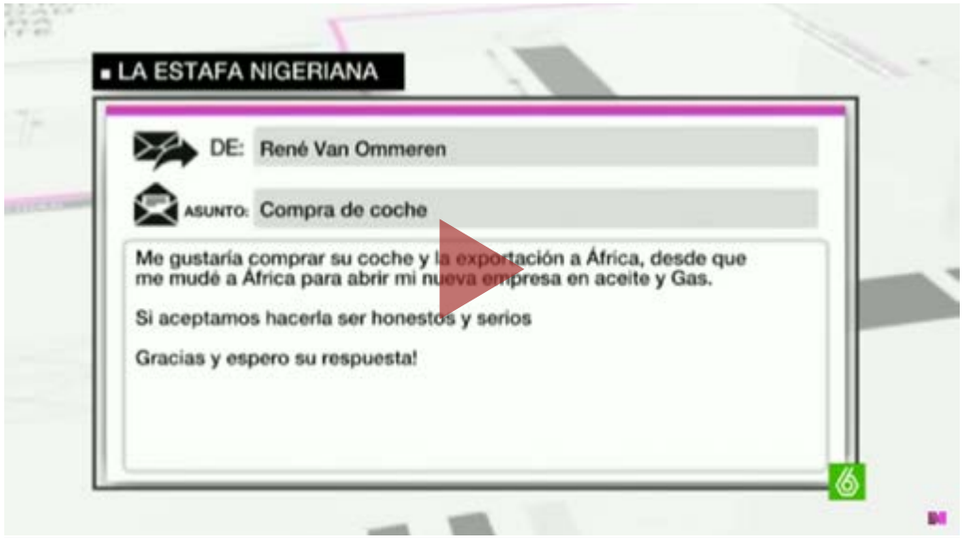
una atractiva mujer reclama dinero para sus estudios o una operación quirúrgica, y nuevos escenarios como la guerra de Siria y Afganistán.

El timo alcanzó su máxima popularidad en la década del 2000 y fue bautizado como 'las cartas nigerianas' porque la mayoría de ellos procedían de este país africano. El fraude se inició en realidad en los noventa, antes incluso de la popularización de internet, y sólo hizo más que aumentar con los envíos electrónicos masivos.

Dos décadas después, las bandas organizadas asentadas en África occidental han evolucionado también a nuevas formas de fraude informático, multiplicando sus ingresos y magnificando los daños causados por sus ataques.

Nigeria se encuentra en la lista de los países donde más ataques informáticos se generan –ocupó el puesto número tres en el informe anual del FBI de 2013-, y según los últimos datos procedentes de diversas compañías de seguridad, continúa jugando un papel protagonista en los ataques a escala mundial.

Sus actividades se extienden ahora a la clonación de páginas web de entidades financieras, a la suplantación en las redes sociales, al robo de datos



ASÍ FUNCIONA LA "ESTAFA NIGERIANA" EN INTERNET

CLICAR PARA VER EL VÍDEO

"Las bandas nigerianas han sabido aplicar lo aprendido con los timos de spam para lograr ser tremendamente efectivos en la técnica del BEC"

Zeki Turedi, estratega tecnológico de CrowdStrike

personales, el 'phishing', el malware, y los más novedosos ataques dirigidos de 'spear fishing' a través de ingeniería social.

De los viejos timos dirigidos a individuos incautos que se creían historias inverosímiles de príncipes nigerianos y bellas mujeres rusas, los estafadores nigerianos han pasado a centrar sus objetivos en empresas y corporaciones mediante el compromiso de correos corporativos (BEC).

"Todavía hay muchos ataques dirigidos a individuos particulares, pero en general, han aprendido que los grandes beneficios se obtienen cuando tu víctima es una gran corporación", explica Zeki Turedi, estratega tecnológico de CrowdStrike.

"Las bandas nigerianas han sabido aplicar lo aprendido con los timos de spam para lograr ser tremendamente efectivos en la técnica del BEC. No solo en su habilidad para engañar a las víctimas, sino también en su capacidad para mover y blanquear el dinero procedente del fraude", añade Turedi. "En lo que se refiere a BEC, podemos afirmar que Nigeria es básicamente el líder mundial".

Una lista de 50.000 correos corporativos

Según una investigación del equipo Unit 42 de la firma Palo Alto Networks, que analizó las activida-

"Cualquiera que tenga una experiencia previa en phishing puede realizar ataques BEC"

Eusebio Nieva, director técnico de Check Point España

des del grupo nigeriano conocido como Silver Terriers, identificó un total de 300 actores asociados a medio millón de ataques, con 15 herramientas distintas de malware para llevar a cabo tareas de compromiso de correo. "Sólo durante el año pasado –afirma la compañía en su informe de 2018- han emprendido 17.600 ataques al mes, lo que supone un aumento del 45% con respecto al ejercicio anterior. La mayoría de estas acciones iban dirigidas contra compañías más que contra individuos".

En otra investigación separada, la empresa especializada en seguridad de correo electrónico Agari, siguió los pasos de otra banda nigeriana con ramificaciones en el Reino Unido y Estados Unidos. Los cibercriminales tenían en su poder 50.000 direcciones de correo electrónico pertenecientes en su mayoría a CFOs y CEOs de compañías pertenecientes a diversos sectores; desde pequeñas empresas a grandes corporaciones, los principales bancos a nivel mundial, entidades de crédito y agencias inmobiliarias de más de 80 países, entre ellos España.

"Agari ha cruzado cuentas de correo con perfiles de redes sociales y otros registros personales para extraer una imagen real de la identidad real de los atacantes. Parece que nueve de cada diez grupos criminales dedicado al envío de correos operan desde Nigeria", afirma Agari.

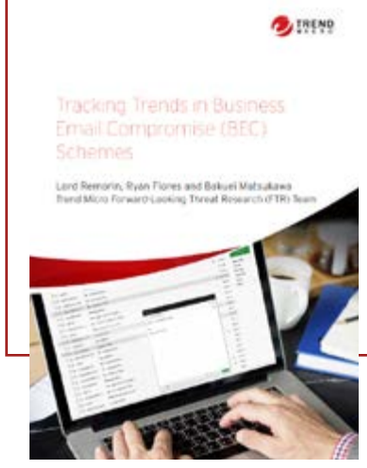
"Como si de una empresa de marketing se tratara, London Blue utilizó servicios comerciales de análisis de datos, entre ellos una empresa de San Francisco, para generar 'leads', seleccionar sus objetivos y emprender sus campañas de phishing y BEC", añade la firma.

Y su tasa de éxito es elevada. Tres de cada cien víctimas responden al primer correo enviado por los criminales, y de ellos, casi cuatro acaban por morder finalmente el anzuelo. Eso supone 3,7 casos de éxito por cada mil mails. De esta manera, los ataques BEC ocasiona-

TENDENCIAS EN LOS ATAQUES BEC

Trend Micro desvela en este documento no sólo algunas de las cifras que generan los ataques BEC, o de Business Email Compromise, sino los cinco tipos de ataque que hay o las técnicas más utilizadas, ofreciendo algunas guías para hacer frente a este tipo de ataques.

En mayo de 2017, la Oficina Federal de Investigaciones (FBI) publicó un estudio que indica que los ataques Business Email Compromise (BEC) se han convertido en una industria de 5.300 millones de dólares. En 2018, Trend Micro predijo que la cantidad superará los 9.000 millones. Esta creciente popularidad de BEC entre los ciberdelincuentes se puede atribuir a su relativa simplicidad: requiere pocas herramientas especiales o conocimientos técnicos para lograrlo, en lugar de eso requiere una comprensión de la psicología humana y un conocimiento de cómo funcionan las organizaciones específicas.



¿POR QUÉ LOS TIMADORES NIGERIANOS NO OCULTAN SU PROCEDENCIA?

Pese a que los hackers nigerianos se han evolucionado hacia fraudes electrónicos más sofisticados, las mafias continúan utilizando la clásica técnica de las 'cartas nigerianas': mensajes de correo masivo donde los cibercriminales tratan de engañar a individuos incautos para que les envíen dinero o compartan sus datos bancarios.

1,57 personas de cada cien acaban por morder el anzuelo en los correos de 'romance', donde los estafadores se hacen pasar por una mujer en busca de relaciones, pero según las investigaciones de CrowdStrike, las bandas utilizan este tipo de spam como apoyo a sus ataques BEC. "El FBI considera los timos de 'romance' como un sistema secundario asociado al BEC, puesto que las víctimas de este fraude son utilizados como 'mulas' para cobrar dinero o facilitar las transferencias procedentes de emails corporativos", asegura la firma de ciberseguridad.

¿Pero por qué los timadores, pese a la mala fama del país africano insisten en decir que son de Nigeria? ¿Por qué envían correos electrónicos con una ortografía y una sintaxis tal que les ha hecho merecedores del Premio Anti-Nobel de Literatura de 2005? Un estudio publicado por Microsoft Research tiene la respuesta.

Según Microsoft los estafadores usan patrones matemáticos y datos históricos para determinar el perfil de las personas que realmente acaban por caer en la trampa. Al introducir deliberadamente errores ortográficos y gramaticales en el mail, eliminan a aquellos de mayor nivel educativo que lo identifican inmediatamente como un fraude. Así evitan perder tiempo con gente que al final no va a entregar el dinero.

Nigeria es conocida en internet por ser la base de un gran número estafadores. Si alguien considera que el mensaje es auténtico, es una prueba de su desconocimiento y experiencia en la Red. La elección de países africanos o en conflicto, que a menudo son vistos en Europa y EEUU como un foco de corrupción, contribuye a que las víctimas acaben por creer que las estrambóticas ofertas de traspaso de fondos o entrega de imposibles herencias son reales.

ron unas pérdidas globales de 12.500 millones de dólares en los últimos cinco años, según datos del FBI.

Pese a no utilizar técnicas avanzadas, las bandas nigerianas utilizan métodos muy extendidos y sencillos, lo que les permite contar con un enorme ejército de hackers a su disposición. "Cualquiera que tenga una experiencia previa en phishing puede realizar estos ataques –explica Eusebio Nieva, director técnico de la firma Check Point España-. En algunos casos utilizan cosas tan básicas como key loggers que compran directamente en el mercado negro".

"Otras veces –continúa Nieva-, ni siquiera usan ningún tipo de software; simplemente se hacen pasar por el director de la compañía o alguien con autoridad. Esto hace que sea complicado que los programas de defensa identifiquen los correos. Pero ya existen sistemas inteligentes de spam o sistemas que localizan dominios similares al de la empresa que permiten identificar este tipo de emails".

"Los Yahoo Boys tienen su propio argot, les encanta aparentar, conducir coches tuneados y cambiarlos regularmente"

Profesor Joshua Oyeniyi Aransiola

Además de programas de detección, el experto de Check Point recomienda ante todo proteger los procesos de negocio de la compañía, "con sistemas de doble autenticación, u horarios determinados para transacciones, porque en muchos casos los cibercriminales reclaman las transacciones con urgencia".

El territorio de los 'Yahoo Boys'

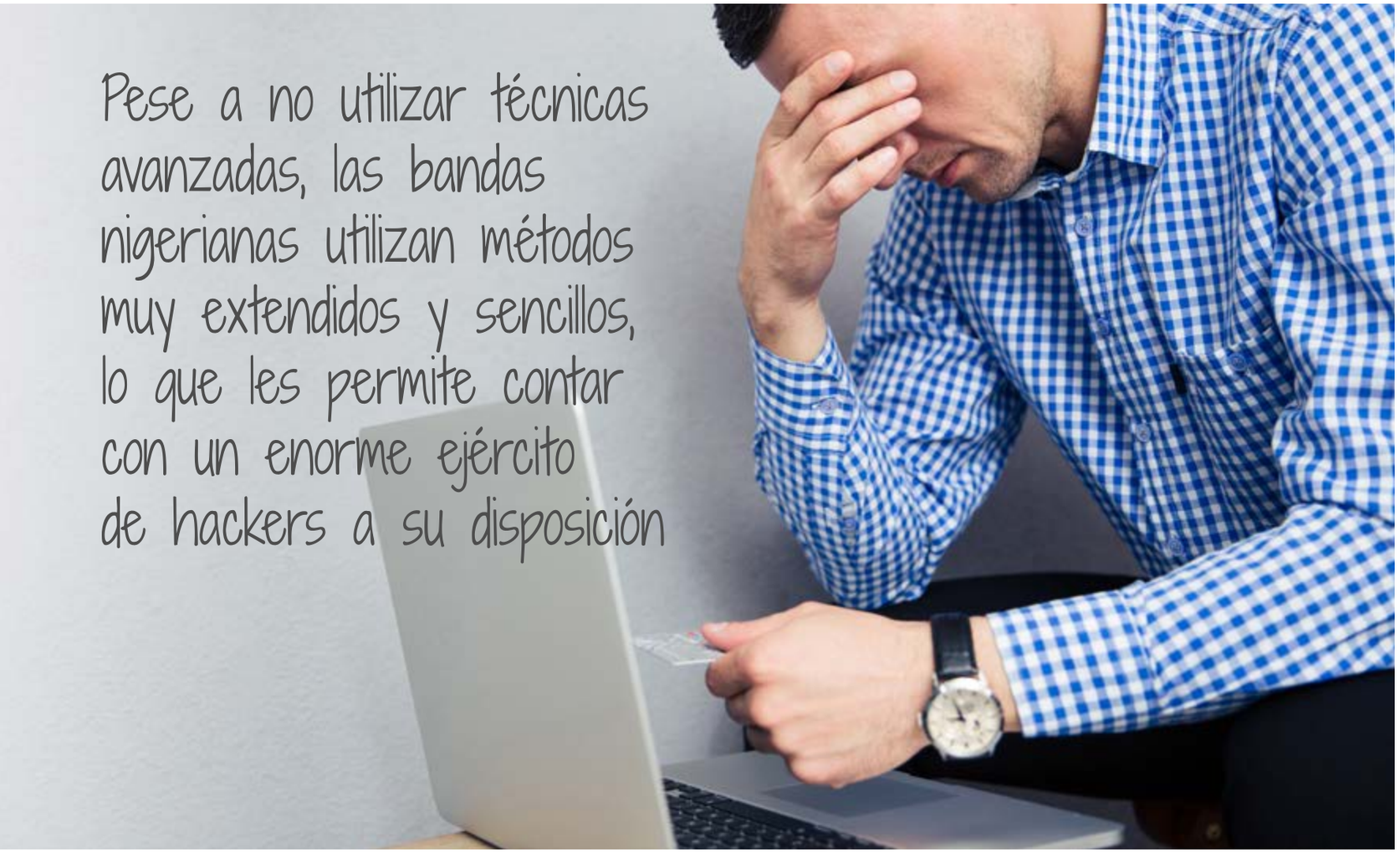
Amparados por la falta de legislación en ciberseguridad y la falta de recursos de las autoridades, los criminales han encontrado en África un refugio ideal donde desarrollar sus actividades. Y la expansión del acceso a internet en el continente sólo aumentará su atractivo. La región está demostrando ser un entorno muy confortable para que las mafias se instalen, operen y lancen sus ataques, asegura la firma norteamericana Trend Micro.

Los soldados africanos del cibercrimen son los 'Yahoo Boys', jóvenes de entre 22 y 29 años, desempleados y con escasa formación, que con programas maliciosos rudimentarios –y mucho ingenio- son capaces de cobrarse botines sustanciosos. Actúan a menudo desde cibercafés, cuentan con amigos en las fuerzas de seguridad o en las oficinas de la banca, y tienen contactos con las redes internacionales del hampa.

Y no ocultan su nivel de vida. "La mayoría están en páginas de contactos y compran y venden con identidades falsas. Los Yahoo Boys tienen su propio argot, les encanta aparentar, conducir coches tuneados y cambiarlos regularmente", según recoge un estudio realizado por el profesor Joshua Oyeniyi Aransiola, de la universidad nigeriana de Obafemi Awolowo, que entrevistó a 40 de estos gángsters del cibercrimen. "Visten a la última y llevan las joyas más caras. Salen a clubs y son famosos por sus fiestas con chicas de alterne".

"Los jóvenes criminales nigerianos, normalmente estudiantes universitarios, comienzan con los timos tradicionales de spam. Eventualmente, los novatos son 'ascendidos' para su participación en los fraudes de BEC", explica Zeki Turedi, estratega tecnológico de CrowdStrike.

En la parte alta de la jerarquía se encuentran los llamados "Next Level cybercriminals" –cibercriminales de siguiente nivel-, que al contrario que los Yahoo Boys, no hacen exhibición de su riqueza y tratan de presentarse como miembros respetables de su comunidad. "Los next level cybercriminals tienen más formación técnica, compran software y contratan servicios de cifrado en foros clandestinos, y tienen grandes habilidades y recursos para el lavado de dinero", relata Trend Micro en su informe 'La ciberdelincuencia en África occiden-



Pese a no utilizar técnicas avanzadas, las bandas nigerianas utilizan métodos muy extendidos y sencillos, lo que les permite contar con un enorme ejército de hackers a su disposición

Enlaces de interés...

- Ataques BEC, ¿sabes lo que son?
- Una nueva táctica de ataques BEC busca robar las nóminas de los empleados
- Tendencias en los ataques BEC
- Las pérdidas por ataques BEC alcanzan los 12.000 millones de dólares

tal: preparada para el mercado clandestino', elaborado en colaboración con la Interpol.

"Mantienen cuentas bancarias y contactos en el exterior y hombres de la organización desplegados en las regiones donde se producen los ataques. Los datos de la Interpol muestran que estas organizaciones se expanden en el exterior. Se trata de ciudadanos africanos que han migrado a los países objetivo", añade el informe de Trend Micro.

En un país donde la mitad de la población vive aún bajo el umbral de pobreza y el 50 por ciento de los jóvenes están desempleados, el cibercrimen es un reclamo tentador para la juventud, aunque el fraude informático haya dañado la imagen del país.

Algunas páginas bloquean las IPs nigerianas, y páginas como Paypal no permiten enviar dinero al Estado africano. Nigeria es la economía más grande de África, uno de los principales productores de petróleo del continente y un mercado emergente con un fuerte crecimiento económico. Existen oportunidades financieras e inversores legítimos, aunque muchas de sus ofertas de negocio, por culpa de los 'Yahoo Boys' acaben en la bandeja spam.

"Las operaciones internacionales de estas bandas suponen un problema no sólo para Nigeria –concluye Zeki Turedi, de CrowdStrike-. Las fuerzas del orden de múltiples países deben ser capaces de comunicarse e intercambiar información para parar y detener de manera rápida a estos criminales. Por desgracia, los cibercriminales son capaces de esconderse entre los pliegues de la burocracia internacional".

Compartir en RRSS

¡AYÚDANOS A DEFINIR EL FUTURO DIGITAL!

Participa en nuestra encuesta itTRENDS

¿Qué valor tienen los datos
y las aplicaciones en tu empresa?
¿Cómo se construyen y tratan?
¿Bajo qué modelo?

PARTICIPA

La Seguridad Gestionada o el Caos

El número de amenazas crece al mismo ritmo que el número de dispositivos y elementos a proteger en las empresas. Además, las amenazas son tan sofisticadas como complejas las infraestructuras a securizar. Ha llegado el momento de contar con el apoyo de un proveedor de servicios de seguridad gestionada.

Normativas, ataques sofisticados, tendencias como Bring Your Own Device o la necesidad de gestionar más soluciones de seguridad para hacer frente a las nuevas amenazas, nos lleva a recurrir a servicios gestionados. Por todo ello, las empresas cada vez recurren a proveedores de servicios de seguridad gestionada, o MSSPs, que les ofrecen la experiencia y el conocimiento de la gestión de amenazas que podría faltar internamente, así como servicios de supervisión y administración de la seguridad fuera de las horas normales de funcionamiento.

IT Digital Security se ha reunido con empresas líderes del sector para conocer de primera mano cuál es la situación del mercado, cuál es el perfil de un cliente de servicios de fseguridad gestioandos o cuáles son sus ventajas. De forma que Sarenet, Trend Micro, Panda Security, Sophos y S21sec nos

"Las amenazas de seguridad se van extendiendo y se deben abordar de una forma más proactiva"

Juan José Rey,
Director de Ventas Madrid, Sarenet

ayudarán a comprender el valor agregado que ofrecen estos servicios gestionados.

Sarenet

¿Qué ventajas lleva adoptar este tipo de servicios gestionados? Juan José Rey, responsable de ventas de la zona centro de Sarenet, recuerda que hay mayor concienciación, a la vez que las amenazas de seguridad se van extendiendo y se deben abordar de una forma más proactiva. "Hemos pasado de unas redes simples donde había conectados PC, impresoras y algún servidor, a redes heterogéneas complejas, con gran cantidad de dispositivos, a veces ajenos a la organización", como pasa con el IoT. Sarenet ve que el mercado español va madurando, aunque aún está en una fase de adopción. Sin embargo, "este será el año para los servicios gestionados", dice Rey.

Sarenet propone "elevar una capa de seguridad a todos los niveles". El camino que sigue la información de una empresa va desde el puesto de trabajo de los empleados, hasta la red de Internet. Históricamente, se ha definido un punto frontera donde se colocaba el firewall para detectar las posibles amenazas. Un cortafuegos que crea una frontera desde la red cliente hasta la pública, que Sarenet ofrece de la mano de Fortinet y que es su servicio más demandado. Pero yendo más lejos, se pueden ofrecer mayores capacidades, como operadores, ofreciendo una capa adicional de seguridad. En esa parte exterior, hay grandes amenazas: bien de tráfico, o bien de denegación de servicio. Nos comunicamos con Internet a través de dos formas: de los grandes proveedores de tránsito y de los operadores de peering. "Al cliente le daremos la posibilidad de colaborar con ese borde exterior. Así podrá ver el tráfico que se mueve alrededor de su red. Y si encuentra algo anómalo, podrá bloquear esos ataques", dice Rey.

Para la red privada virtual y su protección, la labor de Sarenet es llegar al domicilio del cliente, como operador multicareer. "Es positivo combinar dos tecnologías y dos careers distintos. Se puede controlar el flujo MPDS, y una vez desplegada la VPN, se ofrece al cliente la posibilidad de realizar una gestión proactiva del flujo de tráfico entre sus sedes. Y se muestra la interacción entre las diversas oficinas del usuario. De la misma forma que el cliente puede hacer en el borde exterior, aquí puede ver el tráfico y controlar o limitar lo que no desea", explica el directivo. Sarenet propone la segmentación de la LAN del cliente, teniendo en cuenta el Internet de las Cosas, controlar el acceso a la Red (para ello, dice Juan José Rey, es necesario asesorar respecto

de cómo asesorar al cliente respecto a cómo gestionar el acceso a informaciones corporativas, con dispositivos ajenos a la organización).

Trend Micro

José de la Cruz González, Tecnhnical director Iberia para Trend Micro, recuerda que “a día de hoy, las empresas se enfrentan a mayores retos de seguridad que va desde el malware tradicional (ransomware, criptolockers, spam, phishing…) hasta todas las vulnerabilidades que han ido surgiendo. Esto hace que los métodos tradicionales no sean suficientes para las vulnerabilidades a las que nos enfrentamos ahora. Otro reto es la normativa: no solo GDPR, sino las que hay en los diversos sectores en los que pueda trabajar una compañía. Y, además, las empresas necesitan protegerse de una forma que sea económicamente viable.

Para mitigar todos estos riesgos a los que nos enfrentamos hay dos grandes planteamientos, según el directivo de Trend Micro: Desde el punto de vista de la red, se pueden monitorizar los protocolos en nuestra red y analizar el comportamiento y detectar los ataques, aunque también puede ser demasiado complejo y a veces complicado determinar el origen; y otro planteamiento es el ‘Endpoint Detection and Response’ que permite realizar un análisis desde la raíz y nos da mucha información del comportamiento del usuario o machine learning, aunque se necesita de un personal especializado, ya que es muy complejo, y esto supone un elevado coste.

Un ataque se divide en cuatro fases: protección (antes de que llegue al entorno), aquí se usan tecnologías como análisis de reputación web, antimalware tradicional…; detección, cuando se quiere frenar un ataque que aún no ha dañado el sistema y para lo que hay herramientas como machine learning, análisis de comportamiento…; la respuesta, que es cuando la amenaza ya ha conseguido entrar al sistema y en ese momento, se puede enviar el endpoint desinfectado para poder limpiarlo, meter en cuarentena las amenazas…; y la investigación, fase que requiere una mayor

"Un ataque tiene cuatro fases: protección, detección, respuesta e investigación"

José de la Cruz,
Director Técnico, Trend Micro

"Hay que tener cuidado con los escenarios americanos, porque si un tercero se quiere llevar un dato no tienen que pasar por los mismos canales por los que se pasan en Europa"

Pedro Viñuales, VP Global Presales Key Account, Panda Security

inversión ("ya hemos tenido el problema y ahora se debe investigar qué ha pasado para evitarlo la próxima vez").

Trend Micro incorpora las tres primeras fases automatizadas y, si el cliente tiene el tiempo, el dinero para invertir y el interés, se le ofrece la cuarta, la de la investigación con personal experto. No son tecnologías que actúan por separado. Todas ellas se coordinan. Desde los antivirus, que dice José de la Cruz, que es necesario para ataques automatizados, hasta tecnologías muy desarrolladas que, todas ellas combinadas, hacen frente a las amenazas actuales. Trend Micro considera que, combinando todos los productos se crea la seguridad conectada capaz de confrontar las amenazas actuales. Y bajo esta idea surgió su servicio Managed Detection and Response, que implementa automatización (con inteligencia artificial) y sus ingenieros expertos, en caso de que los clientes contraten este servicio.

it whitepapers

INFORME
DE CIBERAMENAZAS
Q4 2018

Publica Positive Technologies un nuevo informe de amenazas que recoge, entre otras cosas, que el objetivo del 48% de los ciberataques que se produjeron en el cuarto trimestre del año pasado buscaban el robo de datos.

También recoge Positive en su informe que el número de ciberincidentes creció un 11% en el último trimestre de 2018 en comparación con el mismo periodo de hace un año, y un 7% más respecto al trimestre anterior.

Panda Security

Pedro Viñuales. VP Global Presales en Panda Security, recuerda que la empresa española, desde el punto de vista de la seguridad, cuenta con varios retos: transformación digital, la dispersión del entorno, que cada vez está más distribuido, la movilidad de su parque de usuarios y las amenazas que cada vez son más avanzadas. Y a estos retos hay que darles respuesta desde los proveedores de servicios y los fabricantes. Las amenazas ya no intentan infectar el PC con software malicioso, ahora roban las credenciales y se adentran en los equipos de personas y empresas para robar lo que les conviene, como explica Viñuales. Y Panda cuenta con su programa de inteligencia colectiva de amenazas que usa la nube para ser capaz de detectar esos comportamiento anómalos en el uso de un sistema. Así, cuenta con la inteligencia de todos los clientes para transportar esa telemetría que se concentran en sus plataformas SaaS y sus herramientas de Machine Learning, y respondiendo a ese punto de valor añadido. Es la inteligencia colectiva recolectada en siete años en la nube, de la mano del equipo de analistas de seguridad.

"La formación del usuario es una capa adicional de seguridad"

Iván Mateos, Sales Engineer, Sophos

Las herramientas cloud de Panda dan capacidades a un proveedor de servicios que quiera realizar su actividad. En base a eso hay que articular una plataforma, de modo que un proveedor de servicios pueda ofrecer lo que el cliente necesita siendo competitivo en costes. Explica el directivo de la firma española que, por muy bueno que sea un servicio, si el coste no es competitivo, la oferta tampoco lo es. Y Panda lo que ofrece a sus socios es una oferta que no requiera un gasto para esos proveedores, los cuales tienen que darle el valor añadido, dándoles la flexibilidad de conectar sus propios servicios.

Recuerda Viñuales que es "muy importante tener claro dónde estamos cuando hablamos de que 'Tus datos están en Europa'" y añade que "hay que tener cuidado con los escenarios americanos, porque si un tercero se quieren llevar un dato no tienen que pasar por los mismos canales por los que hay que pasar en Europa, y ahí Panda quiere marcar la diferencia, ya que su información se guarda aquí, donde la normativa es más estricta".

Sophos

¿Qué tipo de clientes adopta servicios cada vez más imprescindibles? Dice Iván Mateos, ingeniero de preventas de software de Sophos que "los clientes se dan cuenta de que por el hecho de abrir su puerta a Internet tienen un riesgo, y eso afecta al servicio que ellos puedan ofrecer y, la suma de estas dos pone en juego su reputación". Cuando se dan cuenta todo lo que hay en juego, es cuando quieren un entorno de seguridad.

Sophos propone en su oferta su ecosistema de seguridad sincronizado con un porfolio que se gestiona desde una sede central, en donde se reúnen sus nueve soluciones de manera agrupada para hacer más sencilla la tarea. La interfaz mantiene una estructura similar, independientemente del servicio que se use, lo que facilita su gestión,

explica Mateos. Un ejemplo de estas soluciones es FishThreat, que busca que los usuarios aprendan a usar las tecnologías de forma segura. “El phishing es una enorme amenaza”, recuerda el directivo, que explica que Sophos usa el Malware as a Service o el Phishing as a Service para ofrecer una solución de simulación que se ha bautizado como FishThreat y que ofrece formación continua, con una serie de ataques que se sube al sistema del cliente, junto con módulos de formación para que el usuario aprenda qué es phishing y qué no lo es y cómo hacerles frente.

La formación es una “capa adicional de seguridad” y Sophos los hace parte de la estrategia para mantener esta. Y así, los usuarios formados, podrán también usar las soluciones que la empresa tiene para mantener sus equipos seguros. La empresa española cada vez está más interesada en poder formar a sus empleados en seguridad. “Las empresas cuando no pueden recurrir a un departamento de IT, siguen queriendo soluciones de gran calidad y alto nivel” pero que puedan ser sencillas de usar por los empleados.

S21sec | Nextel

Jorge Hurtado, vicepresidente de servicios gestionados de S21sec, recuerda que hace apenas diez años las empresas eran “un castillo fortificado”, que intercambiaban muy poca información con el exterior, con un responsable de seguridad dentro de la empresa y se sentían completamente protegidas. El responsable de tecnología decía qué se podía llevar a cabo en el negocio y qué no. Pero eso ha cambiado. Ahora el departamento tecnológico debe

recoger las demandas que llegan desde el negocio y adaptar la seguridad en función de eso, como explica Hurtado, que recuerda que la transformación digital ha sido uno de los asuntos que ha modificado esa ciberseguridad que conocíamos, de la mano de novedades como el cloud, IoT, movilidad, redes sociales, Big Data y que todas ellas han traído nuevas implicaciones en seguridad.

Al mismo tiempo, mientras que hace unos años los atacantes eran actores concretos, a veces con cierto afán de notoriedad o lucro, normalmente organizaciones unipersonales, ahora las amenazas llegan desde entidades gigantes criminales, que en ocasiones mueven miles de millones de euros, o que son hacktivistas muy organizados que hacen necesaria mucha mayor seguridad. También tenemos ahora los gobiernos y las agencias de espionaje vinculadas a gobiernos. Así, las empresas se encuentran con que hacen frente a amenazas que cuentan con enormes recursos, tanto económicos,

"Ahora la seguridad se enfrenta a organizaciones criminales que mueven miles de millones de euros, hacktivistas bien organizados y agencias de espionaje de gobiernos"

Jorge Hurtado, VP Managed Services, S21sec

Compartir en RRSS

como tecnológicos, además de las personas expertas que forman parte de sus filas. “El tiempo entre que se produce una brecha y esta se detecta ha aumentado, por lo que los atacantes se sienten más cómodos y sus ataques son más rentables”, dice el directivo. También tenemos que las regulaciones han cambiado: GDPR, NIS, Regulaciones específicas para el sector bancario, Esquema Nacional de Seguridad, PSD… y estas deben aplicarse a los sistemas de seguridad. Finalmente, los usuarios, “el eslabón más débil”, son otro gran cambio. Es muy difícil encontrar expertos en seguridad que conozcan bien la situación para poder hacer frente a los desafíos.

Hoy en día, hay que cubrir las funciones de detección, respuesta y recuperación, frente a los ataques. La falta de talento requiere de servicios gestionados. Las empresas que ofrecen estos servicios son expertas. Al mismo tiempo, el costo es más asequible a la hora de contratar firmas externas, a la vez que se ofrece un mayor nivel de protección y una gran capacidad de respuesta. S21sec cuenta con dos servicios en este campo: SOC, que externaliza las operaciones de seguridad (supervisión de la operación del cliente para detectar si le está pasando algo, analizar y gestionar cualquier incidencia, además de conocer qué carencias tienen sus empresas en cuanto a seguridad); y Threat Intelligence, que monitoriza actividades fraudulentas, tanto internamente, como si está entrando malware de fuera, además de poder conocer si algún grupo hacktivista tiene a esta empresa entre sus objetivos.

Enlaces de interés...

- Consejos para los proveedores de servicios gestionados..., y especialmente para los de seguridad
- Los servicios de seguridad gestionados en EMEA se duplican
- Sophos adquiere la compañía de seguridad endpoint DarkBytes
- Nueva versión de la solución de seguridad para IoT de Trend Micro
- Bajo GDPR España ha notificado 670 brechas de seguridad
- Ocho meses de GDPR

#ITWebinars

Tecnologías para dar al dato el protagonismo que merece

Registro

MARZO

La seguridad gestionada o el caos

Registro

www.ittelevision.es

it televisión

Compartir en RRSS

Backup y continuidad de negocio, ¿estás preparado?

Parece obvio pensar que las empresas tienen planes de backup, disaster recovery y continuidad de negocio. Pero lo obvio deja de serlo cuando un informe tras otro indica que la mayoría de los responsables de TI no están seguros de la habilidad de sus organizaciones para recuperarse de una incidencia o un ataque.

El impacto de la adopción de servicios de cloud, las nuevas regulaciones de protección de datos o la amenaza del ramsonware han introducido nuevas dimensiones en el concepto tradicional de backup, no sólo como una manera de proteger los datos, sino también como herramienta indispensable para garantizar la actividad de la empresa en caso de ataque.

Para analizar los retos este sector en transformación IT Digital Security reunió en sus #DesayunosITDS a los expertos Ignacio Gilart, CEO de WhiteBearSolutions; Alexis de Pablos, Director Técnico de Veeam Iberia; Germán Zurro Valdez, ejecutivo de cuentas de Rubrik, y Chuck Cohen Managing Director de Ireo, distribuidor exclusive de StorageCraft en España.

¿Están preparadas las empresas españolas? ¿Podemos dar por hecho que la empresa española cuenta con políticas de backup y recuperación? Según nuestros expertos la concienciación por parte de las empresas ha mejorado, especialmente en las grandes corporaciones, aunque aún queda trabajo por hacer.

"El cliente muchas veces no es consciente de la importancia de la continuidad de negocio"

Chuck Cohen Managing Director de Ireo, distribuidor de StorageCraft en España

"Desde el punto de vista de la obligación de tener un backup entendemos que sí que lo hacen; desde el punto de vista de que realmente funcione… depende un poco de qué tipo de compañía estamos hablando –aseguró Ignacio Gilart, CEO de WhiteBearSolutions -. Cuanto más grande es una organización y más sujeta ésta a normativas y regulaciones, mejor hace los deberes, pero cuando vas hacia abajo vamos viendo carencias, especialmente en la micropyme y la pyme, donde se cumple esta obligación, pero cuando llega el día de recuperar un dato resulta que la herramienta no funcionó como debía funcionar o los procedimientos han fallado".

"La parte más positiva es que estamos pensando no solamente ya en el backup como una segunda alternativa, sino como una parte complementaria a lo que es la disponibilidad en general", apuntó Alexis de Pablos, director técnico de Veeam Iberia.

Frente a grandes retos, grandes soluciones

Como es habitual, al finalizar el debate pedimos a nuestros expertos que expongan sus propuestas, en esta ocasión para securizar los sistemas y redes de operaciones industriales.

Ignacio Gilart: Nuestra propuesta desde hace muchos años está basada en un modelo de prestación donde intentamos ser una suite de tipo generalista para abarcar el mayor conjunto de plataformas posibles que nos podemos encontrar en los clientes. Luego en aquellas que particularmente tengan una mayor relevancia por implantación en el mercado, nos focalizamos si cabe más, y tener herramientas más sofisticadas.

Por otro lado tratamos también de desligar un poco el modelo tradicional de adquisición de licencias-soporte. Nosotros somos soporte puro. Concentramos todos los servicios de tal manera que cuando el cliente adquiere un producto nuestro lo que está adquiriendo es ese servicio, no sólo la plataforma, de manera que cuando tenga ese problema que me va a surgir seguro como en cualquier plataforma, pues haya detrás una compañía muy solvente para prestar ese servicio. Y luego democratizar un poco el uso de la tecnología; llegar a esas startups que tienen capacidad tecnológica para desplegar una serie de plataformas y poder tener una solución lo más completa a un coste razonable.

Alexis de Pablos, **Veeam Iberia:** Estratégicamente va muy ligada a lo que es la protección de del servicio. Lo que nos interesa por supuesto es copiar el dato, no es sólo el objetivo, el objetivo es la restauración y ahí es donde viene nuestra segunda derivada que es la disponibilidad. La posibilidad de recuperar el servicio en cualquier entorno de forma óptima y en muchas ocasiones apoyándonos en herramientas de terceros. Evidentemente, los entornos cada vez están más dispersos hay cargas de trabajo distribuidas en distintas plataformas y lo que se trata es de utilizar una solución única que nos permite hacer una recuperación sencilla y fácil de cualquier entorno.

Germán Zurro, **Rubrik:** Lo que proponemos es una solución de gestión del dato, de tipo convergente, para que la gente no tenga que seguir invirtiendo tanto en la gestión de infraestructuras y en gestión de sistemas, sino que vayan más la capa servicio. Copiamos el dato para extraer el metadato y en base a eso, ofrecerles diferentes servicios, muy orientado a que la gente explote es esos servicios y esos metadatos. Una vez que tenemos una copia y esos servicios podemos dar otras vertientes, como el recovery instantáneo, la interacción con el cloud, orquestación de aplicaciones, disaster recovery y por supuesto seguridad.

Chuck Cohen, **StorageCraft:** Como su nombre indica, Storagecraft tienen algo que ver con almacenamiento integrado con backup. Es cierto que es la parte de backup es mucho más conocida, pero en cuanto almacenamiento tenemos la nueva generación almacenamiento, escalable en caliente para los clientes que necesitan controlar los datos desestructurados, y en el área de backup cubrimos todos los escenarios; desde los entornos virtuales hasta entornos físicos y heterogéneos. También ofrecemos programas para proveedores de servicios bajo un modelo de pago con facturación mensual, que es lo que más se está vendiendo en España.

El backup está cubierto en la empresa española, asegura Germán Zurro, añadiendo que en Rubrik "plateamos partir del backup para ofrecer otros servicios, como la gestión del dato y del metadato para ir hacia la integración con la nube, integración de procesos, automatización, porque es ahí donde tenemos que llevar la continuidad de negocio".

Porque el backup no sólo tiene el objeto de poner a salvo los datos, sino también garantizar la continuidad de negocio. "Hablamos cada vez de continuidad de negocio –explicó Alexis de Pablos-. La idea es cada vez más la disponibilidad. Estamos incorporando nuevos elementos dentro de lo que son los data center o centros de cloud. El objetivo en sí del backup no es la copia, sino el poder restaurar en tiempo y forma".

"El cliente muchas veces no es consciente de la importancia de la continuidad de negocio –añadió Chuck Cohen, Managing Director de Storagecraft. Es un servicio con una gran oportunidad de negocio. No es solo cuestión de tener una herramienta, sino el servicio en sí". En este mismo sentido, Ignacio Gilart aseguró que "las organizaciones cada vez están más obligadas con la transformación digital. La continuidad es inherente. Tengo que saber qué tipo de disponibilidad tiene que tener cada dato y en cuanto tiempo tengo que responder a una amenaza que pueda comprometer mi negocio".

Las nuevas normativas, especialmente las referentes a protección de datos, como GDPR, han contribuido a aumentar la concienciación por parte de las empresas en esta materia. "En ciertos campos hemos notado que los clientes preguntan si nuestros data centers están en Europa o no. Se nota que los clientes están pensado en más cosas que si puedo marcar la casilla de si tengo backup o no. Lo importante es la concienciacia de que tengo que proteger mis datos", apuntó Chuck Cohen.

"En cualquier cosa que tenga que ver con tecnología y seguridad afectan las normativas –añadió Gilart -. Puede haber regulaciones, como la GDPR, que genera retos para los fabricantes. Si alguien me dice que tengo que eliminar todos sus datos, yo puedo eliminarlos de las fuentes primarias, pero ¿cómo los elimino del backup histórico? Hay tecnologías para poderlos integrar a través de operatividad con sistemas de

BACKUP Y CONTINUIDAD DE NEGOCIO, ¿ESTÁS PREPARADO? **CLICAR PARA VER EL VÍDEO**

"El objetivo en sí del backup no es la copia, sino el poder restaurar en tiempo y forma"

Alexis de Pablos, Director Técnico de Veeam Iberia

"No vemos GDPR como un motor de negocio, sino como un facilitador"

Germán Zurro Valdez, ejecutivo de cuentas de Rubrik

gestión, o automatizar la tarea como tal, pero plantea retos".

Desde Rubrik no ve GDPR como un motor de negocio, "nadie me llama porque tenga que cumplir con la normativa", pero sí en un facilitador para posicionar las soluciones.

De la misma forma, el auge del ramsomware, especialmente el reciente ataque de WannaCry, ha contribuido a aumentar la conciencia en las empresas de la necesidad de contar con un backup y servicios que garanticen la continuidad.

"Empezaron a darle valor –relató Germán Zurro, ejecutivo de cuentas de Rubrik-. No sólo por daño del dato, sino el daño como marca". Además, "se ha visto que tener un backup en local no es suficiente, porque el ramsomware pueden encriptar mi backup –añadió Chuck Cohen, por lo que hay que tener también una copia en remoto".

Pero los grandes desafíos del sector han venido por la expansión del Big data y la universalización de los servicios en la nube.

"Los datos crecen exponencialmente, y por tanto aumenta la demanda de recursos (para las empresas de backup) –apuntó Gilart. Un sistema de big data, cuando tiene una corrupción, georreplica la corrupción, con lo cual el backup es un buen elemento para volver a un punto atrás. Y también depende un poco de la validez de esos datos en el tiempo y como la tecnología de backup se integre con los sistemas nativos. Es una combinación de la tecnología de backup con elementos de infraestructura que alojan ese big data".

OCHO MESES DE GDPR

El 25 de mayo de 2018 GDPR se convirtió en una regulación de obligado cumplimiento que cambió fundamentalmente el perfil de riesgo para las organizaciones que sufren una violación de datos personales.

En virtud de GDPR, las violaciones de datos personales que puedan generar un riesgo de daño a las personas afectadas deben notificarse a los reguladores de datos. Cuando dicha conlleve un alto riesgo de daño, las personas afectadas también deben ser notificadas.

Este informe analiza de cerca la cantidad de infracciones notificadas a los reguladores y las primeras multas emitidas bajo el nuevo régimen GDPR para el período comprendido entre el 25 de mayo de 2018 y el Día Internacional de Protección de Datos el 28 de enero de 2019.

Alexis de Pablos, por su parte, aseguró que desde su firma están “impulsando mucho las tecnologías de poder rearmar los sistemas de big data. Que en caso de tener que rearmar o replicar esos sistemas, que tengamos herramientas para hacerlo, y hacerlo en tiempo”.

Para Germán Zurro una de las soluciones es la gestión del metadato. “No sólo debemos hacer una copia, sino que se extraiga el metadato, de tal forma que puedas llegar a interactuar con estas tecnologías y cumplir mejor las normativas, porque no estás moviendo el dato de lugar, que es donde reside el dato del ciudadano, sino que estás gestionando el metadato que es menos crítico en lo que a violación de protección de datos se refiere”.

Enlaces de interés...

- Carbonite compra Webroot por 618 millones de dólares
- El mercado de dispositivos de backup vuelve a la senda del crecimiento en Europa
- Pistas para elaborar un buen plan de continuidad
- Copias de seguridad: una guía de aproximación para el empresario

"Un sistema de big data, cuando tiene una corrupción, georreplica la corrupción, con lo cual el backup es un buen elemento para volver a un punto atrás"

Ignacio Gilart, CEO de WhiteBearSolutions

Los sistemas de almacenamiento en la nube han sido “un punto muy interesante para el backup, porque podemos enviar los datos a un cloud que no se encuentra en tus dependencias físicas –explicó Alexis de Pablos-. Nosotros tratamos de proteger tanto los entornos on premise como cloud; que todos los entornos interactúen”.

“Estoy en contra de usar la palabra cloud, porque nada se puede guardar en una nube, húmeda y gaseosa –bromeó Chuck Cohen-. Se guarda en los data center. Cuando tenemos una solución de backup, tenemos que guardar el backup en la red local y luego replicarlos fuera por si hubiera un desastre en la red local, pero no tiene por qué ser en Amazon, o Google, puedes guardarlos en otros lugares, para estar en todo momento en control de dónde se guardan tus datos”.

it User
TECH & BUSINESS

¿Eres el que más sabe de tecnología?

¡Participa!

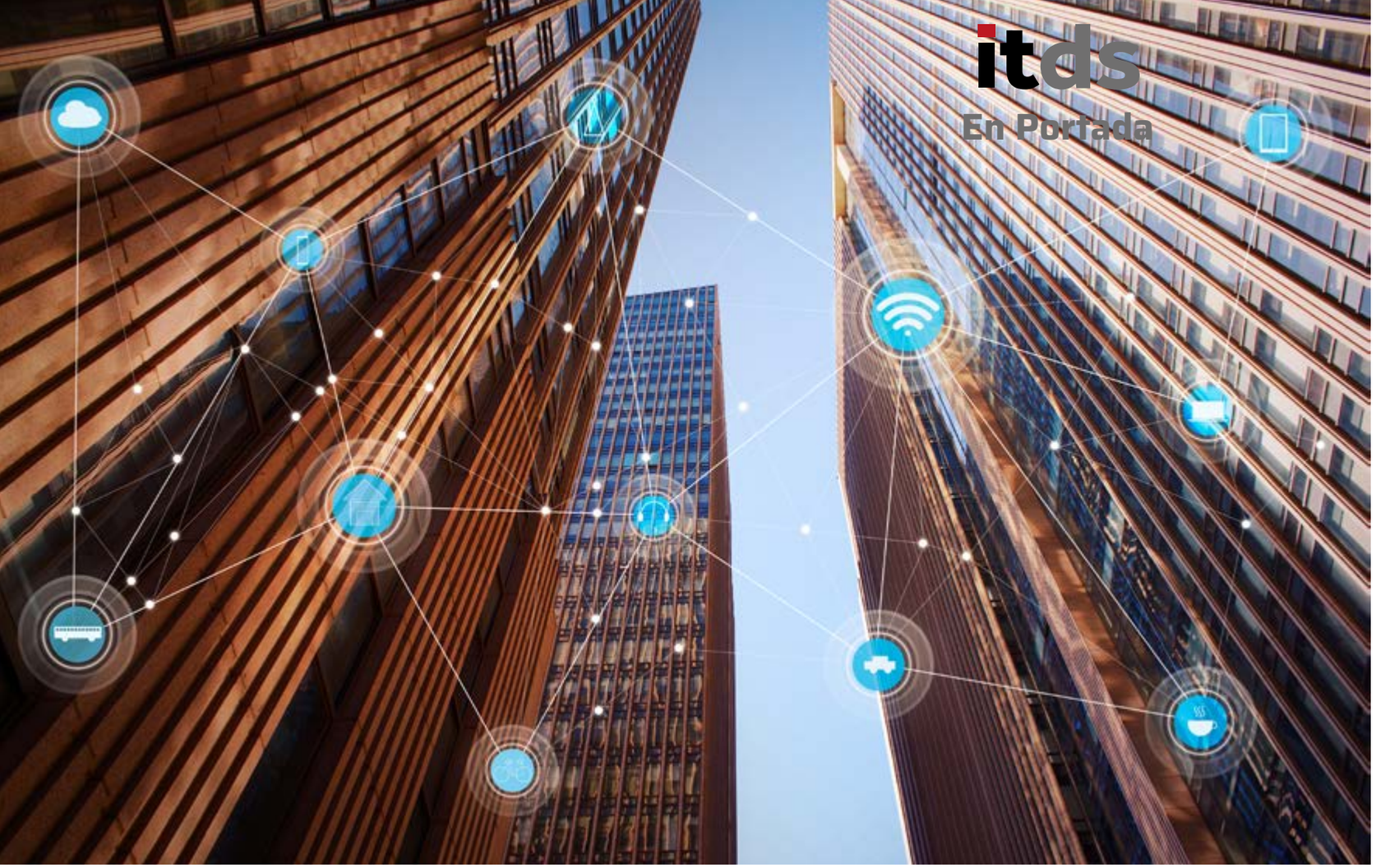
DELL

Windows 10 Pro

itExpert

NAC,
visibilidad y control para tu red

Las tecnologías NAC, o de control de acceso a la red, han evolucionado mucho desde aquellos primeros tiempos en los que sólo estaban centradas en la autenticación y autorización de los endpoints para tener cierto control sobre el BYOD y los accesos de terceros, entre los que se incluyen tanto a partners como colaboradores o invitados. La explosión del IoT está dando un nuevo impulso a este mercado, que según Research Markets crecerá un 27,23% anual entre 2018 y 2022.



"Hasta ahora la tecnología NAC se limitaba a controlar quién entraba a nuestras redes y eran un modelo muy estático de acceso"

David García Cano, Cyber Security Sales Manager para el Sur de Europa

Aunque los firewalls y las soluciones de gestión de dispositivos móviles pueden ayudar, cuanto se trata de tener la suficiente visibilidad sobre el dispositivo y usuario que se quiere conectar a la red para determinar pueden hacer, o hasta dónde, estas soluciones se quedan cortas.

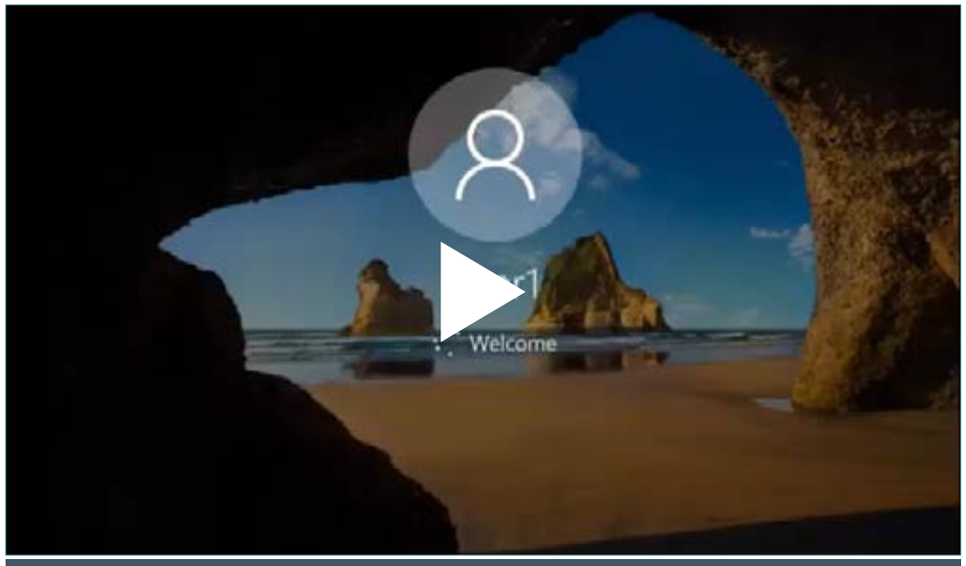
La virtualización, los servicios cloud, la movilidad, incluso los switches… hacen que la tarea de identificar y securizar los endpoints fuera misión imposible. Las primeras tecnologías NAC se dedicaban a autenticar y autorizar a los endpoint, sin más; impedía el acceso de ordenadores infectados a las redes corporativas para evitar que ser extendiera el malware.

Le siguió una segunda generación que añadió flexibilidad a la ecuación permitiendo establecer diferentes políticas en base a la localización de los usuarios o la gestión de riesgos para llegar, poco a poco a donde nos encontramos ahora, una tecnología NAC preparada para el reto del BYOD y del IoT; una tercera generación que permite alcanzar la máxima visibilidad de las redes y de los dispositivos personales pudiendo establecer políticas granulares basadas en el quién, el qué, el dónde y el cuándo.

Retos que solucionan los NAC

No se puede proteger lo que no se puede ver. Es una máxima que se repite a diario y que alcanzó su cota cuando la adopción de dispositivos móviles desbordó las previsiones de los responsables de TI de las empresas. Ya no se trataba de gestionar los PCs de los empleados, sino sus portátiles y sus móviles, todos ellos capaces de acceder a los recursos de las empresas. El IoT no ha hecho sino potenciar el problema. Lo cierto es que los equipos de seguridad deben ser capaces de ver toda la infraestructura de red en sus diferentes localizaciones, incluido en el borde. Aún ahora hay una desconexión entre la seguridad del endpoint y la seguridad de la red, de forma que no se comparte información en tiempo real y no se responde de forma coordinada a las amenazas.

De forma que una respuestas automatizadas ante las amenazas es otro de los retos que las tecnologías NAC ayudan a gestionar. Además, añade automatización a los flujos de trabajo. Es decir, procesos como los de aprovisionamiento si pueden automatizar, en lugar de hacerse de manera ma-



nual; no sólo se ahorra tiempo, sino que reduce la posibilidad de errores humanos que pueden generar riesgos o reducir la eficiencia general de las operaciones de seguridad.

Explica David García Cano, Cyber Security Sales Manager para el Sur de Europa de Aruba, que cada vez son más frecuentes los ataques internos (Insider Threats) así como la proliferación del IoT, y que esto lleva a que sea esencial saber en todo momento qué está conectado a nuestros sistemas (Identificación) para poder aplicar políticas de seguridad específicas y personalizadas (Protección), identificando el comportamiento anómalo que se pueda dar, premeditado o no, (Detección) y automatizar la respuesta para frenar este tipo de ataques internos no vistos hasta la fecha (Respuesta Automatizada).

Apunta Rafael Cuenca, Regional Channel Manager de Pulse Secure que en el entorno de redes híbridas en el que nos movemos, donde no sólo se conectan dispositivos de todo tipo, “incluidas aplicaciones, API´s, algoritmos… el control de acceso a la red (NAC) proporciona visibilidad y capacidad de gestión de acceso a esos usuarios/dispositivos/aplicaciones/‘cosas’ a través de la aplicación de las políticas de seguridad tanto en redes fijas como inalámbricas”.

Las soluciones tradicionales, como los firewalls o IDS, se centran en asegurar el perímetro de la red, mientras que el propósito de un NAC es asegurar y controlar la propia red de acceso y todos los dispositivos que residen en ella.

> "Las soluciones tradicionales, como los firewalls o IDS, se centran en asegurar el perímetro de la red, mientras que el propósito de un NAC es asegurar y controlar la propia red de acceso y todos los dispositivos que residen en ella"
>
> Ángel Arias Baelo,
> Aerohive Senior Sales Engineer

Evolución del NAC

Ya hemos mencionado que las soluciones de control de acceso a red están evolucionando hacia la automatización y la orquestación de la seguridad (SAO) para la seguridad de la red integral.

Dice Ricardo Hernández, Sales Manager de ForesCout para el mercado de Iberia, que entre las principales mejoras del mercado NAC en los últimos años destaca “particularmente” la capacidad de reconocer, clasificar y evaluar cualquier tipo de dispositivo, a lo largo de cualquier tipo de red, Campus, Data Center, Cloud u OT, sea este del tipo que sea, tradicional, móvil, IoT u OT sin necesidad de desplegar agentes ni suplicantes,

it whitepapers

ASEGURANDO LA ECONOMÍA DIGITAL: REINVENTANDO EL INTERNET DE LA CONFIANZA

En 2007, había 1.200 millones de usuarios de Internet, cifra que diez años después creció hasta los 4.200 millones, más de la mitad de la población mundial. La cantidad de dispositivos conectados a la IoT probablemente alcanzará los 25.000 millones para 2021, y para 2024, las redes 4G-LTE darán cobertura al 90% de la población, mientras el 5G lo hará al 40%.

A pesar de ello, sin confianza el futuro de nuestra economía digital y su potencial casi ilimitado están en peligro. Los esfuerzos parciales para abordar los problemas de ciberseguridad, incluidos los defectos inherentes de Internet, las vulnerabilidades de Internet de las cosas (IoT), la veracidad de la identidad y los datos y el aumento de la fragmentación digital, se han quedado cortos.

sin necesidad de utilizar el protocolo 802.1X, la monitorización continua, no sólo en el momento de acceso a la red, así como la integración con otras soluciones de seguridad e IT que permiten orquestar respuestas automáticas antes situaciones de riesgo o incidentes son para nosotros las más importantes".

La mayor parte de las soluciones NAC han evolucionado para incluir una funcionalidad más completa y mejorada más allá de las características de control de acceso originales del NAC tradicional, asegura Ángel Arias Baelo, Aerohive Senior Sales Engineer, añadiendo que muchas de las soluciones NAC de hoy en día incluyen características para integrar sin problemas cientos y miles de dispositivos, incluyendo BYOD, IOT, también con tecnologías como la creación de perfiles de dispositivos que pueden identificar automáticamente la marca y el modelo de un dispositivo, y luego incorporarlo basándose en el conocimiento del tipo de dispositivo. "La gestión de los invitados y los controles de salud de los dispositivos, también conocidos como posture assessments (evaluaciones de postura), son compatibles con muchas soluciones NAC avanzadas. Otra mejora es el impulso hacia la gestión de la nube, que aumenta considerablemente la eficiencia operativa, ya que permite una gestión centralizada y coherente de todos los sitios corporativos", apunta el ejecutivo de Aerohive.

Más del 25% de las organizaciones utilizan entre 11 y 20 proveedores de seguridad y un 16% usan entre 20 y 50 proveedores

Qué impulsa el mercado NAC

Cinco son los factores que Aruba identifica como impulsores del mercado NAC. El primero es la

"Las soluciones NAC son capaces, a nivel de red, de detectar y aplicar políticas de seguridad sobre dispositivos conectados, incluso aunque sean imposibles de administrar"

Rafael Cuenca, Regional Channel Manager de Pulse Secure

necesidad de mayor visibilidad de lo que está conectado a la red, sabiendo en todo momento el comportamiento de los dispositivos conectados, no solo en el momento del acceso. El segundo gran impulsor es la automatización y dar una respuesta coordinada ante incidentes a través de la integración nativa con terceros de seguridad (SAO, Automation and Orchestation). Habla también Aruba de la mayor presencia de dispositivos IoT conectados a las redes corporativas sin ningún tipo de control, el proporcionar nuevos mecanismos de autenticación simplificados, pero mucho más seguros: Single Sign On y acceso seguro (preferiblemente basado en certificados, EAP-TLS), y por último nueva legislación y cumplimiento normativo que exigen controles y planes de acción en el control de acceso a las redes corporativas heterogéneas (LAN, WLAN y VPN).

Dice Ángel Arias, de Aerohive, que la explosión del BYOD y, más recientemente, IOT ha sido uno de los principales impulsores del crecimiento de este mercado. Añade que muchas organizaciones protegen los dispositivos cableados, además de los dispositivos inalámbricos en los que se enfocaron tradicionalmente, debido a que "existe un creciente reconocimiento del que los dispositivos cableados no protegidos o los puertos Ethernet no protegidos presentan un riesgo de seguridad significativo". Y no hay que olvidar que las amenazas de seguridad de TI, los ataques a la red y las vulnerabilidades de los dispositivos siguen creciendo de manera exponencial, y muchos atacantes se enfocan en los dispositivos para obtener acceso a la red; "las soluciones de NAC proporcionan seguridad donde los dispositivos se conectan, es decir, en la capa de acceso, y cada vez más organizaciones se dan cuenta de que es precisamente aquí donde tienen brechas de seguridad".

Para Rafael Cuenca, de Pulse Secure, el mayor impulsor para la adopción de NAC es el creciente número de dispositivos que se conectan a las redes corporativas y que no siempre están bajo el control de la organización, "de tal manera que un problema de actualización, mala configuración o simplemente desactualización del Sistema de seguridad en el dispositivo puede generar una brecha de seguridad en la organización, poniendo en riesgo la integridad de esta".

Perímetro definido por software, ¿el nuevo NAC?

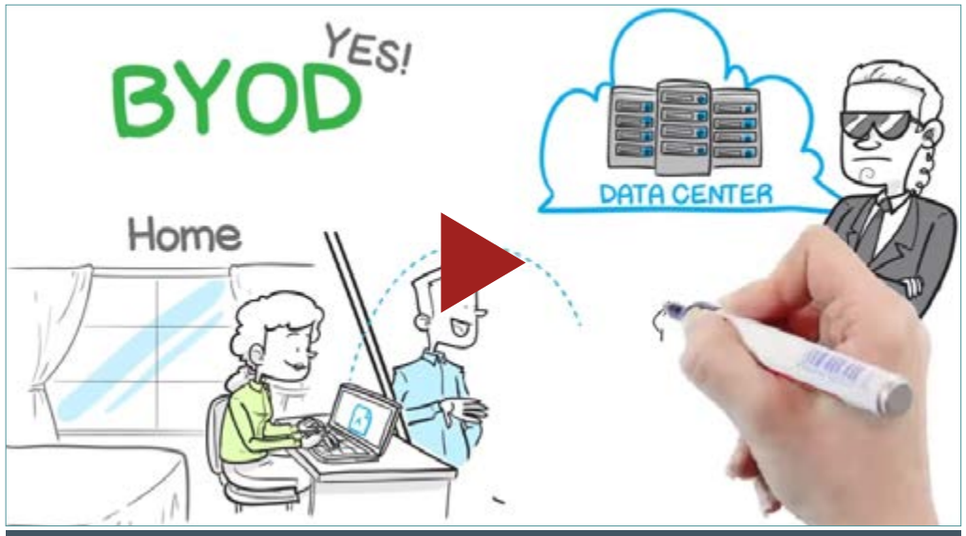
Hace algunos años que se habla del perímetro definido por software, o SDP, como el nuevo NAC. Y eso es lo que hemos planteado a nuestros expertos. He aquí sus respuestas:

David García Cano, Cyber Security Sales Manager para el Sur de Europa de Aruba. Creo que no se resolvería el problema ni mejoraría los sistemas de seguridad de los clientes. Las soluciones de NAC intentan resolver los problemas internos a las redes y gestionar todo el acceso, que no necesariamente tiene que pasar por el perímetro (movimiento Norte-Sur). Son soluciones totalmente complementarias, y que con entornos como el que propone Aruba, pueden convivir e integrarse nativamente para poder dar respuesta a problemas más complejos de una manera automatizada e integrada.

Ángel Arias Baelo, Aerohive Senior Sales Engineer: La aproximación del NAC es totalmente distinta a las soluciones por software, ya que el propósito de un NAC es asegurar y controlar la propia red de acceso y todos los dispositivos que residen en ella y las soluciones basadas en software normalmente necesitan la instalación de un agente software en el dispositivo lo que se hace inviable para dispositivos de invitados o IoT.

Rafael Cuenca, Regional Channel Manager de Pulse Secure: Se podría considerar que la arquitectura de Software Defined Perimeter (SDP) ofrece mejoras sobre las soluciones NAC existentes. En términos simples, la arquitectura SDP se basa en el modelo Zero Trust de “nunca confiar, verificar siempre” permitiendo el acceso seguro directo entre el usuario y su dispositivo a la aplicación y al recurso, sin importar la infraestructura subyacente. SDP separa la autenticación de los usuarios, los dispositivos y su estado de seguridad, de la asignación de un túnel seguro entre la entidad y la aplicación o los datos de destino. Los usuarios conectados a través de un proceso basado en SDP solo podrán ver y acceder a los recursos que se han definido en una política administrada centralmente, mientras que todo lo que no esté definido en esta política de acceso no será visible. La principal ventaja de SDP sobre NAC es que es más eficaz y fácil de administrar en entornos mixtos en los que la TI se distribuye en entornos on-premise, hosted, cloud y Saas.

Ricardo Hernández Calleja, Sales Manager Spain & Portugal de ForeScout: Creo que aquí hablamos de soluciones distintas, tanto porque las soluciones de Visibilidad y Control de dispositivos han evolucionado mucho desde los tiempos del NAC tradicional, como por las capacidades que tienen de cubrir cualquier tipología de red, sea esta Campus, Data Center, Cloud u OT. Creo que las soluciones de perímetro definido por software son complementarias en una de estas tipologías de red, y pueden trabajar conjuntamente para implementar un nivel de seguridad y control de acceso coherente y unificado a lo largo de toda la red. No considero que una tecnología sea sustituta de otra, sino que pueden trabajar juntas y complementarse en distintos casos de uso para fortalecer la protección en donde sea necesario.



Añade Ricardo Hernández que la cloudificación de las redes, con múltiples opciones conviviendo de nube pública, privada, SDN, SDDC… hace que sea cada vez más necesario extender la visibilidad y el control a estos entornos tan ágiles y cambiantes. “Por último, la interconexión de redes OT ha abierto un nuevo vector de riesgo, especialmente crítico por el tipo de infraestructuras e industrias a las que afecta y que tiene una idiosincrasia y particularidades específicas que requieren de un enfoque diferente y unificado que pueda cubrir estas redes sin afectarlas, algo que nuestras soluciones ayudan a proveer”.

NAC en un mundo de IoT

“El IoT es una pesadilla para los departamentos de IoT”, dice Ángel Arias, de Aehorive. Hasta aquí ha quedado claro que el Internet de las Cosas es uno de los grandes impulsores de la demanda de soluciones NAC. Pero la relación entre ambos va mucho más allá, porque en realidad los NAC son herramientas imprescindibles de este tipo de entornos.

Para Ricardo Hernández, de ForeScout, el papel que juegan los NAC en un entorno IoT es fundamental. Explica que este tipo de dispositivos tienen una capacidad de proceso limitado y necesitan soluciones para securizarlos que no impliquen ningún tipo de agente o software instalado en los mismos y que puedan usar la red para asegurar su acceso y seguridad sin afectar a su operatibilidad. “Tenemos un ejemplo muy claro con los dispositivos médicos, que no pueden ser afectados de ninguna manera por escaneos activos, agentes instalados, etc., puesto que son críticos y cualquier impacto en su operación puede afectar a vidas humanas, pero también su seguridad es fundamental y la única forma viable de protegerlos sin afectarlos es a través de soluciones de Visibilidad y Control de dispositivos que utilicen a la red para defenderlos y aislarlos de accesos peligrosos pero sin modificarlos ni afectar a su operación”, dice Hernández.

Explica David García Cano, de Aruba, una solución NAC avanzada podrá permitir a los clientes conocer qué estos dispositivos -que no están concebidos para ser seguros, están conectados a las redes, pero además podrá securizarlos de manera totalmente personalizada en función del tipo de dispositivo del que se traten. Dice el directivo que, hasta ahora, o se aplicaban políticas laxas para dar

"Una solución NAC permite asegurar y controlar el acceso a la red, tanto de equipos corporativos, como de invitados o socios que deban acceder temporalmente a sistemas y redes específicas"

Ricardo Hernández, Sales Manager Spain & Portugal de ForeScout

"Este tipo de tecnologías NAC abarcan cualquier tipo de cliente que se preocupe por securizar lo que está conectado a sus redes corporativas"

David García Cano, Cyber Security Sales Manager para el Sur de Europa

conectividad a cualquier cosa que pudiera llegar a la red, o se establecían políticas restrictivas que ponían en compromiso la experiencia de usuario; "Ni lo uno ni lo otro, lo más adecuado es establecer políticas totalmente personalizadas, pero para eso es necesario previamente identificar todos los dispositivos existentes, incluido el IoT para establecer políticas de protección a medida y en tiempo real. Además, esta política debe seguir al dispositivo y la solución NAC debe permitir asignarla dinámicamente en función del perfilado del dispositivo IoT en cuestión. Si este cambia, el sistema también enviará una política diferente según lo que se haya conectado posteriormente, haciendo un acceso adaptativo y en tiempo real también para este tipo de dispositivos".

Coincide Rafael Cuenca, responsable de canal de Pulse Secure, al afirmar que, para mejorar la seguridad, las organizaciones están recurriendo a soluciones NAC que son capaces, a nivel de red, de detectar y aplicar políticas de seguridad sobre dichos dispositivos, incluso aunque sean imposibles de administrar, restringiendo su acceso a la red y recursos, redirigiéndolos a áreas aisladas en las que no puedan comprometer la seguridad de la organización.

Perfil de cliente

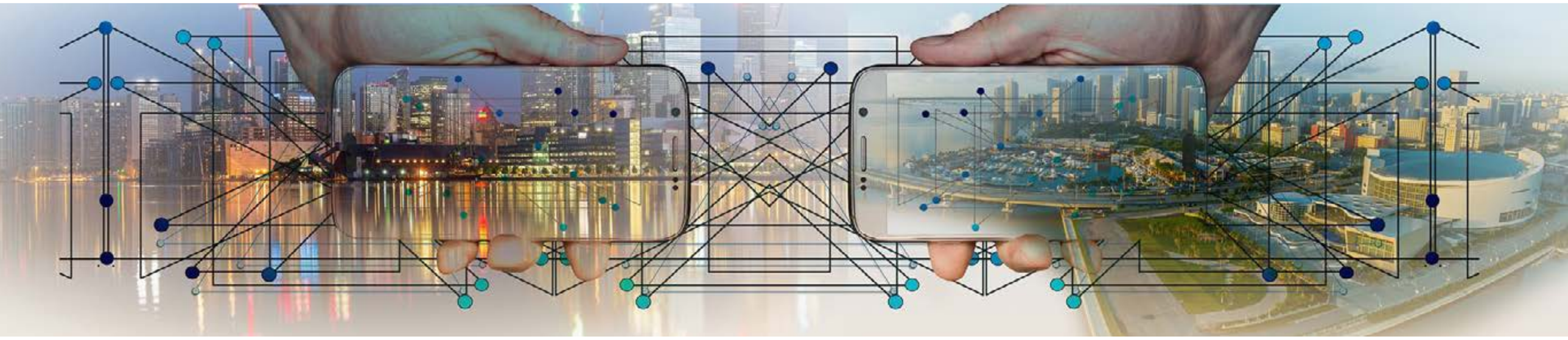
¿Grandes o pequeñas? ¿con más o menos pasión por el cloud? Preguntamos a los expertos quién es el cliente tipo de una solución NAC. "Cualquiera que se preocupe por securizar lo que está conectado a sus redes corporativas", asegura García Cano. Añade que, ante presupuestos ajustados, puede consumirse en modo as-a-Service, además de ofrecer "mecanismos de financiación que ayudan a democratizar la tecnología para que clientes con menos capacidad presupuestaria, puedan dotar de una mayor seguridad a sus redes corporativas".

Dice Rafael Cuenca que la tecnología NAC ha sido adoptada por todo tipo de organizaciones, aunque los sectores con mayor nivel de adopción son principalmente las Administraciones Públicas, el Sector Financiero, el sector Salud y en general toda la industria o negocio sujeto a regulación. "Los proveedores de servicios también figuran como early adopters de

la tecnología NAC, especialmente cuando ofrecen servicios críticos para los sistemas de información de terceros", añade el directivo d Pulse Secure.

Dice también el directivo de Aruba que los tipos de clientes que requieren de soluciones NAC han crecido en los últimos años acompañados de las nuevas normativas, así como del aumento de la concienciación de la seguridad. "Vemos un incremento en los niveles de seguridad en las corporaciones", añade que en determinados entornos en los que no se permite acceso a ningún dispositivo y se han incorporado soluciones de control de accesos "han visto que pueden además cubrir nuevas áreas que no tenían previstas con la misma herramienta gracias a las integraciones con terceros y el ecosistema abierto con la mayoría de fabricantes de seguridad que ya existían en su entorno, haciendo que el modelo de seguridad pase a ser un modelo más automatizado en la respuesta y en la compartición del contexto, dejando el modelo estático y de silos que hasta ahora había sido lo habitual en la mayor parte de las organizaciones".

Por cierto, que otro punto clave que según David García Cano demandan los clientes para este tipo de sistemas de seguridad, es "que sean soluciones fuera de banda para simplificar los despliegues en entornos multisede. Nuestra solución (ClearPass) permiten centralizar las políticas de seguridad y desplegar la solución en todas las sedes remotas sin necesidad de centralizar el tráfico (SPAN) ni de requerir sondas locales, haciendo que la gestión y la inversión sea mucho más eficiente para los clientes. El utilizar protocolos estándar simplifica este aspecto y lo hacen una solución perfecta para este tipo de despliegues".



> La tercera generación de NACs permite alcanzar la máxima visibilidad y establecer políticas granulares basadas en el quién, el qué, el dónde y el cuándo

Y asegurando que la tecnología de ForesCout "permiten adaptarse a requerimientos y tamaños diferentes y sacar rendimiento de la solución en situaciones distintas", dice Ricardo Hernández que la tipología de un cliente de una solución NAC es muy variada; "tenemos clientes que son grandes corporaciones con necesidades de seguridad e interoperabilidad muy alta, con equipos de operación y respuesta ante incidentes y también pequeñas empresas con necesidades muy concretas y equi-

"La explosión del BYOD y, más recientemente, IOT ha sido uno de los principales impulsores del crecimiento de este mercado"

Ángel Arias Baelo, Aerohive Senior Sales Engineer

pos IT muy limitados que necesitan optimizar esos recursos y automatizar al máximo los procesos para liberar a sus equipos IT", añade.

Casos de uso

"OnBoarding, Gestión de invitados y BYOD, autenticación corporativa con 802.1X, definición y aplicación de políticas granular para el acceso a la red, seguridad IOT y otros" son los casos de uso típicos de una solución de control de accesos, asegura Ángel Arias Baelo, de Aerohive.

Habla Rafael Cuenca de implementar el NAC "junto tecnologías de redes privadas virtuales (VPN) para detectar, clasificar y monitorear automáticamente los dispositivos administrados, IoT y otros dispositivos no administrados que se conectan a la red corporativa", y añade que mientras que las soluciones de control de acceso supervisan los cambios de estado de perfil y seguridad de los dispositivos, la VPN garantiza que la comunicación entre dispositivos y aplicaciones utiliza un canal privado y cifrado. La tecnología NAC, asegura Cuenca, se implementa ampliamente en áreas altamente reguladas, infraestructuras críticas como, por ejemplo, proveedores de energía, para garantizar que no se conecten dispositivos no autorizados a la red y para permitir una conectividad segura, especialmente desde sitios administrados de forma remota.

Dice Ricardo Hernández que teniendo en cuenta del NAC es uno más de los casos de uso típicos de una solución de visibilidad y control de dispositivos, los principales casos de uso que se identifican en los clientes son:

- **Cumplimiento de Dispositivos.** Asegurar que los equipos que se conectan cumplen con unas características (presencia de aplicaciones, parches, agentes de seguridad, etc.) y si no es así, gestionar su remediación de forma automática, limitando su acceso a la red mientras se resuelve, para una vez hecho esto permitir su acceso normal.

- **Gestión de activos:** Permite tener una foto en tiempo real de los equipos y sus características, a fin de conseguir un inventario de activos y poder interactuar con soluciones ITSM o CMDB para mantenerlas actualizadas y con información detallada de los dispositivos corporativos.
- **Segmentación de red:** Asegurarse que el acceso a la red es el correcto en función de quien se conecta, desde donde, con que dispositivo y cuál es el estado de dicho dispositivo. Esto nos permite realizar una segmentación dinámica y adaptada a las situaciones cambiantes de nuestro negocio.
- **NAC:** Ya comentado, nos permite asegurar y controlar el acceso a la red adecuado, tanto de equipos corporativos, como de invitados o socios que deban acceder temporalmente a sistemas y redes específicas, así como controlar que no halla equipos rogue o atacantes accediendo a la red.
- **Respuesta ante incidentes:** Orquestar diferentes soluciones (Next Generation Firewalls, SIEMS, Anti APTs, Análisis de Vulnerabilidades, Gestión de dispositivos móviles, Endpoint Protection…) para generar flujos de trabajo automatizados que nos permitan controlar y responder en un menor tiempo a incidentes de seguridad, rellenando los huecos entre las diferentes soluciones de seguridad y optimizando recursos humanos y tiempos de respuesta.

> "NAC se implementa a menudo junto tecnologías de redes privadas virtuales (VPN) para detectar, clasificar y monitorear automáticamente los dispositivos administrados, IoT y otros dispositivos no administrados que se conectan a la red corporativa"
>
> Rafael Cuenca, Regional Channel Manager de Pulse Secure

En el caso de Aruba, los casos de uso vistos actualmente en el mercado coinciden totalmente con los cuatro pilares de la compañía:

- Identificar todos los dispositivos conectados a las redes de acceso corporativas, independiente del fabricante de infraestructura (multifabricante) así como del medio de acceso utilizado por el dispositivo/usuario (cable, aire, VPN).
- Proteger con políticas totalmente a medida en base al tipo de dispositivo/usuario del que se trate y en tiempo real, adaptándose a su comportamiento, no solo en el momento del acceso.
- Detectar todo comportamiento anómalo, dado que sabemos qué tipo de dispositivo es y con qué o quién puede interactuar habitualmente.

Compartir en RRSS

- Responder de manera coordinada, hablando con terceros de seguridad para automatizar la remediación en caso de un incidente.

Destacar por último que, según los expertos, los proveedores de NAC deben centrarse en facilitar la implementación y la administración. Y se habla de facilitar porque según Frost & Sullivan, las complejidades de la implementación y administración de una solución NAC pueden ser un factor de, por un lado, la tendencia del cliente a utilizar múltiples soluciones de seguridad que no están integradas y orquestadas y, por otro, la grave escasez de expertos en seguridad capacitados para administrarlas.

Dice la consultora que más del 25% de las organizaciones utilizan entre 11 y 20 proveedores de seguridad y que el 16% de las organizaciones usan entre 20 y 50. “Aprovechar una multitud de proveedores de seguridad que no están integrados y orquestados puede producir un volumen significativo de alertas de seguridad que pueden ser abrumadoras para cualquier personal de seguridad limitado para administrar”, dice Frost & Sullivan en un informe añadiendo que las organizaciones necesitan un sistema de seguridad que automatice, integre y organice otras soluciones de seguridad, como los Next Generation Firewalls (NGFW), la gestión de información y eventos de seguridad (SIEM) y las redes de inteligencia de amenazas para aumentar la eficacia de una solución NAC y justificar su inversión.

Enlaces de interés...

- openNAC Enterprise, ver y controlar para poder proteger
- ForeScout compra SecurityMatters para mejorar su visibilidad del OT
- La mitad de los principales exploits globales se dirigen a dispositivos IoT
- Casi la mitad de las empresas no pueden detectar brechas en sus dispositivos de IoT
- W Perímetro Definido por Software, guía para CIOs
- W Perímetro Definido por Software, por la Cloud Security Alliance

"La explosión en el número y tipología de dispositivos que se conectan a las redes empresariales, la 'cloudificación' y la convergencia de redes IT y OT hacen imprescindible una solución NAC"

Ricardo Hernández, Sales Manager Spain & Portugal de ForeScout

DESCUBRE LAS **TENDENCIAS** QUE DEFINEN EL **FUTURO DIGITAL**

it TRENDS

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.

“Zero Trust” la desconfianza que refuerza las estrategias de protección del dato

En plena implantación de las medidas que habilitan a las empresas para cumplir con la reciente aprobación de la última ley en materia de protección de datos (GDPR), vemos como las estrategias de ciberseguridad han ido evolucionando también durante los últimos años con escenarios IT que continúan su desarrollo imparable hacia entornos cada vez más dispersos y dirigidos hacia el mundo MultiCloud. De hecho, según IDC, en 2024 el 90% del Global 1000 habrá adoptado tecnologías y herramientas multicloud.

La adopción de los nuevos entornos MultiCloud nos confirma el desplazamiento del foco de protección, que en un principio se centraba en el perímetro que albergaban las empresas, para ir trasladándose poco a poco hacia los dispositivos móviles, según la necesidad de movilidad hacía viable la

Compartir en RRSS

apertura de esos perímetros controlados y de difícil acceso.

Pero es ahora en plena era digital, cuando es imprescindible proteger el DATO aportando nuevas tendencias y estrategias de ciberseguridad, reenfocando cualquier nueva estrategia hacia la protección del DATO con independencia de la red o el dispositivo utilizado.

Uno de los cambios más llamativos es el asociado a los patrones de protección asumidos a la hora de poner en práctica dichas estrategias de ciberseguridad en términos de confianza. Ya que ahora se modifica el concepto de confiabilidad de las redes corporativas y el cambio implica pasar a una posición de desconfianza continua, donde ya no importa la red o el dispositivo que acceda a la información, sino la información propiamente dicha. El concepto "Zero Trust" trata de generar un nuevo movimiento que permita definir una estrategia de ciberseguridad acorde al campo de acción MultiCloud donde la colaboración es fundamental y el ciclo de control debe reenfocarse hacia el DATO en lugar de al usuario.

Con la filosofía de trabajo "Zero Trust" trataremos de considerar que cualquier usuario y/o dispositivo es ajeno a la organización

EL LIBRO DE ESTRATEGIAS DE SECOPS

Este documento explica cómo SecOps puede ayudar a que las empresas continúen lanzando código regularmente sin sacrificar la seguridad. SecOps requiere un cambio de mentalidad y cultura, y en este libro de jugadas le mostramos cómo lograrlo usando un plan de acción del mundo real.

Este manual describe todos los aspectos prácticos de la implementación de SecOps, incluyendo: La historia de DevOps y SecOps; ¿quién debería implementar SecOps y por qué?; los seis pasos prácticos que debes seguir para comenzar con SecOps y los indicadores clave de rendimiento y las métricas de éxito que deberían interesarle

y acceso a la información de forma continua que no otorguen identidades de confianza consolidadas. De este modo, se establecen nuevos ciclos de autenticación y verificación continuos más allá de los tradicionales sistemas de acceso a redes corporativas.

Las nuevas estrategias de ciberseguridad deberán enfocarse en el ciclo de vida del DATO, y para ello las nuevas redes de información deben ser percibidas bajo la filosofía “Zero Trust” para aumentar la protección del dato, al mismo tiempo que se implementan nuevos nuevas modelos de acceso con sistemas de autenticación y gestión de identidades dinámicos capaces de orquestar las nuevas estrategias de ciberseguridad digital.

Con la filosofía de trabajo “Zero Trust” trataremos de considerar que cualquier usuario y/o dispositivo es ajeno a la organización, y entraremos a una nueva era donde cualquiera puede acceder al DATO y por lo tanto será necesario controlar el servicio del DATO. Es decir, quien accede o puede acceder a él, desde donde lo hace, para qué lo hace y en última instancia qué puede hacer ese usuario con él.

La evolución de las redes IT hacia entornos de concentración de los silos de información en el escenario MultiCloud refuerzan la viabilidad de construir el acceso al DATO con un servicio que puede ser monitorizado y controlado en cualquier momento desde la plataforma central de orquestación MultiCloud. La premisa de considerar a cualquier dispositivo y/o usuario como ajeno a la red corporativa supone introducir nuevos controles de identidad

Enlaces de interés...

- Seguridad en tu red: The Zero Trust Network Architecture
- Okta hace más accesible el modelo Zero Trust con la compra de ScaleFT
- Las ventajas de la identidad digital reconocida universalmente, cada vez más cerca

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos it User

Almacenamiento it

Con la colaboración de: HUAWEI

JORGE DÍAZ-CARDIEL

SOCIO DIRECTOR GENERAL DE ADVICE STRATEGIC CONSULTANTS

Autor de “Éxito con o sin crisis”, “Recuperación económica y Grandes Empresas”, “La victoria de América”, “Innovación y éxito empresarial”, “Las empresas y empresarios más exitosos de España”, “Digitalización y éxito empresarial” y “Digitalización, productividad y competitividad: empresas más exitosas gracias a la transformación digital”.

En diez años, la Inteligencia Artificial en empresa y sector público añadirá 14% al PIB mundial

Hacen falta concienciación de los líderes y formación a empleados en tecnologías digitales

La inteligencia artificial está aparentemente en todas partes. El lunes 11 de febrero de 2019, el presidente de Estados Unidos, Donald Trump, ha firmado una orden ejecutiva para desarrollar la Inteligencia Artificial (IA), uniendo sector público y empresas, para hacer frente a la competencia de China en este campo, como en otros (producción offshore, comercio…).

En los últimos dos años, los requerimientos necesarios para impulsar la IA más allá de los laboratorios y abarcar mercados más empresariales, ya se están dando: tecnologías informáticas potentes

Compartir en RRSS

y económicas; algoritmos avanzados; y enormes cantidades de datos sobre casi cualquier tema. Los periódicos y las revistas están llenos de artículos sobre los últimos avances en Machine Learning y tecnologías relacionadas con la inteligencia artificial.

Dos informes recientes de Advice Strategic Consultants concluyeron que, en las próximas dos décadas, IA será la mayor oportunidad comercial para las empresas y, todavía más, el desarrollo acelerado de las naciones en vanguardia: Estados Unidos, China, Japón y la Unión Europea. Los avances de IA tienen el potencial de aumentar el PIB mundial hasta en un 14% entre 2019 y el 2030, es decir, porcentaje equivalente a una contribución adicional de 14 a 15 trillones de dólares americanos a la economía mundial, y una contribución promedio anual al crecimiento de la productividad de alrededor del 1,2 por ciento, sin bajar o congelar salarios.

Con el tiempo, la IA podría convertirse en una tecnología aplicable a muchas utilidades, empresas, sectores, funciones… y, también, transformadora, como lo fueron la máquina de vapor, la electricidad e Internet y Computación (Las tres previas Revoluciones Industriales). La adopción por el mercado de la IA, probablemente seguirá un patrón típico de curva, con un inicio relativamente lento en los primeros años, seguido de una aceleración pro-

nunciada a medida que la tecnología madura y las empresas aprenden a aprovechar mejor la inteligencia artificial para aumentar el valor de la empresa.

Ya sucedió algo similar entre 1997 y 2000 con el “boom” de las “punto.com” y su posterior estallido. Entonces no se daban las condiciones para lo que sí hemos visto está sucediendo ahora: que una compañía que vende por Internet, como Amazon, sea líder mundial del retail/distribución y que su competencia sea una compañía global china, Alibaba; que Google (Alphabet) sea líder mundial de buscadores de Internet y su competidor principal sea la empresa china Tencent; y algo similar podría decirse de Apple (smartphones, computación…) versus Samsung y Huawei; Facebook, primera red social del mundo con 2,3 billones de usuarios y la reinventada por Satya Nadela, “la nueva Microsoft”, que ya no vive solo de su sistema operativo Windows, sino que se expande a cloud, inteligencia artificial, big data...

Todas las empresas mencionadas, líderes de sus mercados y las más valoradas en bolsa, con una capitalización bursátil del entorno del billón de dólares americanos, han desarrollado su propia inte-

Aunque todavía se encuentra en sus inicios, IA ya está brindando un valor significativo para aquellos que han adoptado la tecnología

ligencia artificial. La única empresa europea que lo hace, también, es española: Telefónica, "rara avis" que, cual supermercado de la tecnología, en palabras de su presidente, José María Álvarez-Pallete, ofrece inteligencia artificial, cloud computing, big data, convergencia, ciberseguridad, conectividad, paquete quíntuple… bien a través de sus propias empresas especializadas (Acens, Luca, Eleven Paths, Wayra…), agrupadas bajo el paraguas de Telefónica Empresas/Telefónica Business Solutions, que dirige José Cerdán Ibáñez, pionero en computación, internet y digitalización en España al fundar en 1990 la primera empresa fabricante de ordenadores de España-. Y, también, a través de 200 alianzas con empresas como AWS, Microsoft Azure, Sage, Cisco o Salesforce, entre otras muchas.

Para tener una idea más concreta del estado actual de la adopción de la IA, Advice Strategic Consultants, recientemente (diciembre 2018 a enero de 2019), realizó una encuesta global sobre el estado actual de la adopción de la IA. Respondieron 4,000 empresarios/as, directivos/as, CIO, en 10 sectores de la economía que aportan el 95% del PIB; ocho funciones de negocio y una amplia gama de regiones geográficas y tamaño de compañías: Estados Unidos, Unión Europea -con foco en España y en sus 17 Comunidades Autónomas-, China, Corea del Sur y Japón. La encuesta preguntó sobre el progreso en la implementación de nueve capacidades principales de inteligencia artificial, incluido el aprendizaje automático, la visión por ordenador, el texto en lenguaje natural y el procesamiento del habla y la automatización de procesos mediante robótica.

Algunas conclusiones

En general, el mundo de los negocios está comenzando a adoptar la inteligencia artificial. Estamos en sus primeros estadios y, decir lo contrario, no es creíble. Por un lado, hay adopción, implantación y uso en un porcentaje relativamente pequeño de empresas (grandes, pymes, microempresas, autónomos, organismos públicos) y, por otro, hay un

INFORME ANUAL SOBRE INCIDENTES DE SEGURIDAD DE LAS TELCOS

ENISA publica su séptimo informe anual sobre los principales incidentes de seguridad de las telecomunicaciones ocurridos en 2017 en la UE.

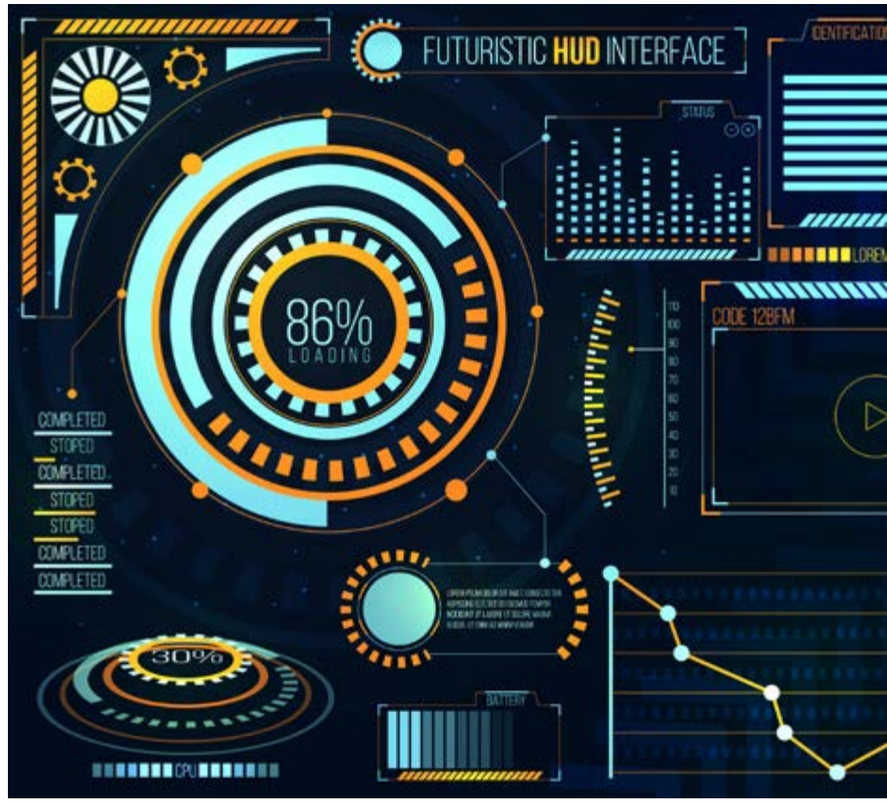
Entre los datos del informe:

- Durante 2017 se reportaron 169 incidentes a las autoridades reguladoras de telecomunicaciones nacionales (NRA)
- El 62% de los incidentes son fallos del sistema, principalmente de hardware y errores de software
- El 17% de los incidentes fueron causados por fenómenos naturales
- El 22% de los incidentes se deben a cortes de energía

Con el tiempo, la IA podría convertirse en una tecnología aplicable a muchas utilidades, empresas, sectores, funciones... y, también, transformadora, como lo fueron la máquina de vapor, la electricidad e Internet y Computación

potencial inmenso, como puso de relieve a finales de enero en el Foro de Davos el World Economic Forum, donde su fundador, Klaus Schwab, explicó el despliegue de las tecnologías digitales de la Cuarta Revolución Industrial: el treinta por ciento (30%) de las organizaciones están realizando pruebas piloto de IA. Casi la mitad, el 47%, ha incorporado, al menos, una capacidad de IA en sus procesos comerciales estándar, en comparación con el 20% en 2017.

Las oportunidades de IA se pueden encontrar en toda la empresa, pero solo el 21% responde que utiliza IA en múltiples funciones comerciales o captación de nuevos clientes. Esencialmente, la IA se está utilizando para remozar y mejorar procesos internos y aumentar productividad y competitividad: el Estudio Advice de Éxito Empresarial en Digitalización detectó, en los tres últimos meses que, en las pruebas piloto de pymes a las que se dota de las tecnologías de la digitalización vinculadas a la Inteligencia Artificial y se les da formación a empresario/a y trabajadores/as, los aumentos de productividad podrían alcanzar el 22% y la competitividad dispararse un 33%. Obviamente, habrán de pasar diez años para



que esta realidad se extienda a todo el mercado empresarial, español y del mundo desarrollado.

Las inversiones en IA son todavía bastante pequeñas. El cincuenta y ocho por ciento (58%) de los encuestados dijo que, menos de una décima parte de sus presupuestos digitales, se destina a IA, mientras

Si se quiere un impacto positivo de IA en toda la empresa, no basta solo con la difusión de las capacidades de Inteligencia Artificial en toda la organización, sino también es imprescindible un verdadero entendimiento y compromiso por parte de los líderes empresariales para impulsar cambios a gran escala

que el 71% espera que las inversiones en IA aumenten significativamente en los próximos años.

Hace falta formación en digitalización

Muchos de los encuestados dijeron que sus organizaciones carecen de las habilidades y prácticas necesarias para crear valor con IA a gran escala, incluida la identificación de oportunidades estratégicas de negocio y la obtención de los datos requeridos por las aplicaciones de IA. La mayoría de empresarios/as, directivos/as, CIO sintió que la IA tendrá un impacto relativamente menor en su futuro empleo en general, a pesar del hecho de que la IA probablemente automatizará un tercio del trabajo existente, incluida la toma de decisiones de los CEO en grandes multinacionales.

Aunque todavía se encuentra en sus inicios, IA ya está brindando un valor significativo para aquellos que han adoptado la tecnología. El setenta y ocho por ciento (78%) informa haber obtenido un valor significativo o moderado, mientras que solo el 1% dice que no ha visto ninguno o un valor negativo. En todas las funciones comerciales, el valor fue más alto en la fabricación y la identificación de la

gestión de riesgos, donde el 80% respondió haber recibido un valor significativo o moderado, seguido de la gestión de la cadena de suministro y el desarrollo de productos y servicios, con el 76%.

La encuesta del Estudio Advice de Éxito Empresarial de Digitalización preguntó sobre 11 prácticas básicas que permitirían a las organizaciones darse cuenta del valor potencial de la IA en calidad y cantidad. Los resultados confirmaron que la mayoría de las organizaciones tienen aún un largo camino por recorrer. Solo el 27% dijo tener acceso al talento interno y externo necesario para apoyar el trabajo de IA; el 26% dijo que sus líderes demuestran compromiso con las iniciativas de IA; El 18% afirmó que su compañía tiene una estrategia para acceder y adquirir los datos necesarios para que la IA funcione; el 17% remarcó que sus empresas han trazado las oportunidades potenciales de IA en toda la organización; y el 15% dijo que su empresa cuenta con la infraestructura tecnológica adecuada para respaldar los sistemas de inteligencia artificial. Casi una cuarta parte de los encuestados, el 24%, dijo que sus empresas no han desarrollado ninguna de las 11 prácticas sobre las que preguntó la encuesta. Y, la gran empresa es, en todos sitios, el único segmento empresarial más desarrollado en la adopción de la Inteligencia Artificial, aunque con funcionalidades todavía primarias.

Cuando se les preguntó sobre las barreras más importantes que enfrentan sus organizaciones para adoptar la IA, el 43% mencionó la falta de una estrategia clara, mientras que el 44% resaltó la falta de habilidades apropiadas. El 30% dijo que los silos funcionales (compartimento estanco) restringen el uso de soluciones de IA, y el 27% mencionó que sus líderes carecen del compromiso necesario con la IA.

La consecuencia es obvia: si se quiere un impacto positivo de IA en toda la empresa, no basta sólo con la difusión de las capacidades de Inteligencia Artificial en toda la organización, sino también es imprescindible un verdadero entendimiento y compromiso por parte de los líderes empresariales para impulsar cambios a gran escala, así como un enfoque estratégico en la gestión del cambio mediante las tecnologías digitales.

Enlaces de interés...

- Inteligencia Artificial: Adios mitos, hola realidades
- La realidad de la empresa española en datos

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

¡Descubra en nuestro

Centro de Recursos it User

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

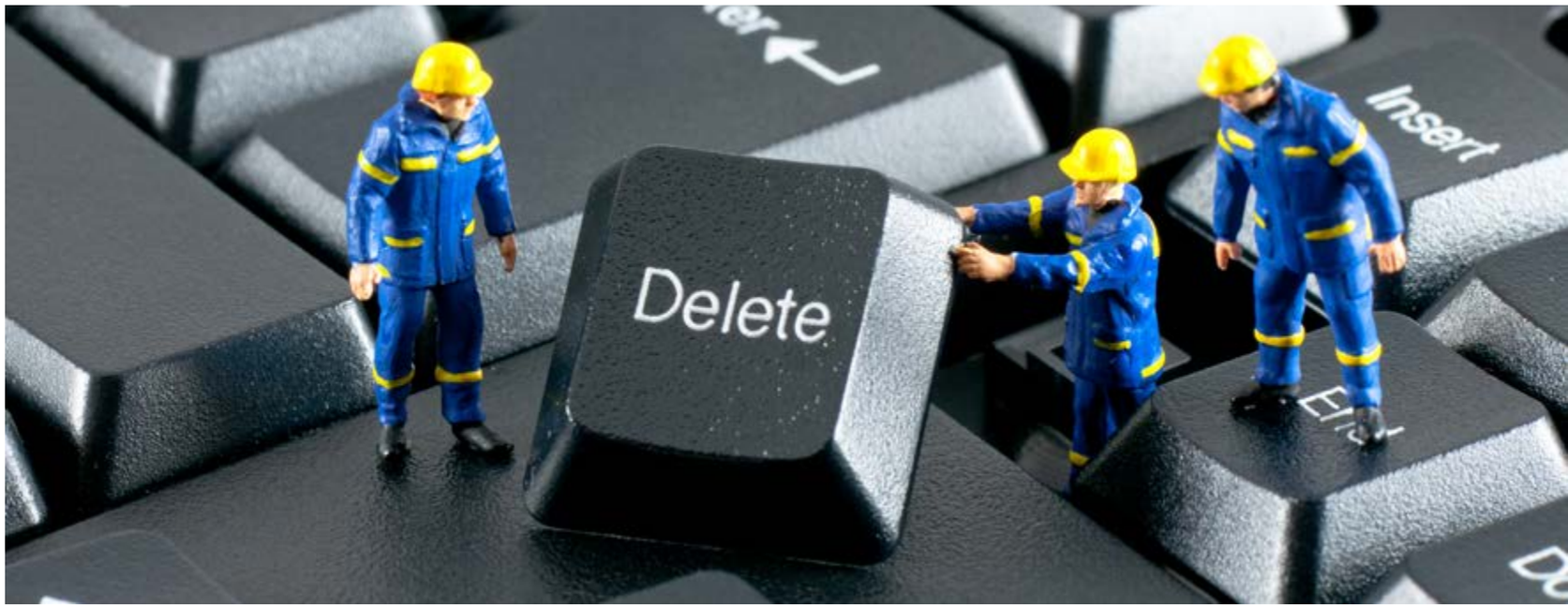
Con la colaboración de: brother Canon hp

La Inteligencia Artificial: ¿debemos ocuparnos de ella o preocuparnos por ella?

FERNANDO BALLESTERO

COUNSELOR DE CÍRCULO LEGAL

Licenciado en Ciencias Económicas, con Premio Extraordinario Fin de Carrera y Doctor cum Laude por la Universidad Complutense de Madrid. Técnico Comercial del Estado y Economista del Estado. PADE (Programa de Alta Dirección de Empresas) por el IESE, y Fellow de la Eisenhower Fellowship, Philadelphia USA. A lo largo de su trayectoria profesional ha sido Embajador de España en la OCDE y Miembro de su Consejo de dirección entre 2004 y 2008; Director General de Coordinación Técnica con la UE entre 1985 y 1990; Subd. Gral de RRII de la SE de I+D+I entre 2014 y 2017, y Consejero Comercial en la Oficina Comercial en Belgrado.



Los medios de comunicación han recogido estos días en los debates que han tenido lugar en el Foro anual de Davos, donde líderes de todo el mundo exponen su visión de los grandes temas que son objeto prioritario de preocupación de Gobiernos y ciudadanos.

Uno de ellos es sin duda el impacto sobre el empleo del desarrollo de la Inteligencia Artificial y la robotización, y en particular la sustitución de personas por máquinas.

Ya en 2016, el Foro elaboró un Informe sobre esta cuestión, sumándose a los primeros análisis que unos años antes habían aparecido. Los más destacados, el elaborado en 2013 por unos profesores de la Universidad de Oxford y el más completo

Compartir en RRSS

La Inteligencia Artificial, apoyándose en el Big Data, va a conseguir sin duda que las máquinas o robots puedan desarrollar a la perfección y sin errores muchas tareas que hacen los humanos

del McKinsey Global Institute en 2016. En ellos se destacaba que el desarrollo tecnológico y la capacidad de las máquinas de realizar tareas que vienen realizando las personas, va a llevar a una progresiva sustitución de personas por máquinas en muchos puestos de trabajo. El primero de los Informes estimaba que en EEUU el impacto puede afectar en unos años a un 47% de los empleos. Profundizando en ello, el Informe de McKinsey analizaba 800 ocupaciones en 54 países valorando cuales de ellas tenían más riesgo de ser reemplazadas. Este año en Davos se ha insistido de nuevo en la importancia de readaptar y adecuar la formación y capacitación profesional a la nueva realidad que estamos ya viviendo.

En las anteriores “Revoluciones Industriales” que han tenido lugar en la historia (aparición de la máquina de vapor, electricidad, y computación), esta sustitución se producía al pasar a realizar unas máquinas el trabajo físico que venían haciendo personas. Pero en la actual Revolución 4.0, con el desarrollo de la inteligencia artificial y la robótica, y la capacidad de las máquinas de aprender y adaptarse a nuevas tareas, el tema de la sustitución es más complejo. Cuando se habla de sustitución de personas por máquinas, no hay que pensar sólo en términos de saldo en número de puestos de trabajo, sino en las funciones o tareas que serán sustituidas, así como en las nuevas funciones o tareas que surgirán como necesarias. Por otra parte, si la “deslocalización” buscando costes más bajos era un hecho hasta ahora, hoy puede darse el fenómeno inverso.

Al mismo tiempo, no son lo mismo unos trabajos que otros. Como ya pusieran de manifiesto los Informes mencionados, no tiene el mismo riesgo de ser reemplazado por una máquina el trabajo de

recepción y cotejo de información de un administrativo, o el trabajo de un dependiente de comercio, que el de un médico, un abogado, un bombero, o un supervisor.

Todos los trabajos exigen para ser realizados, en distinta medida, una capacidad técnica y cognitiva, una capacidad física, y una capacidad de interacción social. El peso de cada una de ellas para el correcto ejercicio de la función, determinará, en última instancia, el grado de potencial de sustitución de personas por máquinas para realizar esa función. Las tareas pautables serán más fácilmente sustituidas, pero hay también tareas nuevas que surgen precisamente para facilitar que las máquinas puedan realizar sus cometidos, y que deben ser incorporadas. En el Informe sobre el futuro de los empleos que se ha presentado en Davos este año se afirma que si bien 75 mill. de puestos de trabajo pueden ser sustituidos entre 2018 y 2022, podrían serán creados 133 mill. Es una estimación, pero refleja algo.

Un ejemplo muy ilustrativo de la importancia de todo esto es la decisión de hace unas semanas del Hotel Henn Na de la ciudad de Sasebo, en Japón, de prescindir de la mitad de los 435 robots que tenía instalados (¿despedirlos?) para la gestión del hotel (recepción, servicios…) debido a su incapacidad de atender adecuadamente respondiendo a las necesidades y deseos de los clientes, o simplemente molestarles insistentemente con preguntas que no habían entendido.

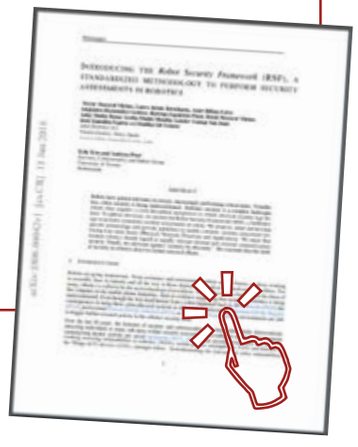
El hotel había incorporado robots sustituyendo a personas para aumentar la eficiencia y bajar costes, dejando las tareas físicas que requerían personas, como hacer camas, para empleados. Pero no pudo evitar que en portales tipo Trip advisor, aparecieran numerosas quejas porque el ordenador de la habitación despertara al cliente con preguntas que no había entendido o que en la recepción los robots no supieran dialogar adecuadamente con algunos clientes al interpretar que el que se quedara callado significa no decir más, en lugar de tiempo para recordar o reflexionar.

Pero no solo es una cuestión de interacción social. La Inteligencia Artificial, apoyándose en el Big Data, va a conseguir sin duda que las máquinas o robots puedan desarrollar a la perfección y sin errores muchas tareas que hacen los humanos. Pero hay tareas que requieren también aplicar unos criterios éticos o deontológicos a la hora de seleccionar e incluir los datos que deben ser considerados por la máquina para actuar a partir de ellos. Ejemplos de ello es el tratamiento de datos médicos de pacientes

THE ROBOT SECURITY FRAMEWORK (RSF)

Los robots realizan tareas cada vez más críticas. No obstante, se está subestimando la seguridad del robot. La seguridad robótica es un panorama complejo, que a menudo requiere una perspectiva interdisciplinaria a la que la seguridad clásica se queda atrás.

Presentado por un grupo de españoles, que aseguran que se han realizado pocos esfuerzos honestos para abordar la sistemática de la seguridad de los robots, el Robot Security Framework (RSF) es una metodología para realizar evaluaciones de seguridad sistemáticas en robots y que cuenta con ejemplos prácticos ilustrativos del mundo real. El documento apunta a arrojar luz sobre la escena de seguridad del robot, un área que ha permanecido oscura en la medida de lo posible.



Enlaces de interés...

- Foro anual de Davos
- Impacto sobre el empleo del desarrollo de la Inteligencia Artificial y la robotización
- Global Risk Report 2019
- Global Gender Gap Report 2018

En la Revolución 4.0, con el desarrollo de la IA y la robótica, y la capacidad de las máquinas de aprender y adaptarse a nuevas tareas, el tema de la sustitución de personas en determinadas funciones es más complejo

con diferentes condicionantes, o la interpretación de datos legales por los despachos de abogados. No basta con acumular datos y, procesándolos, generar unos algoritmos que marquen las pautas de actuación. Es necesario aplicar unos criterios éticos a la hora de considerar la información que puedan aportar los simples datos y el tipo de pautas actuación que puedan derivarse. En el caso del abogado, no bastará con conocer bien la normativa, jurisprudencia y sentencias relacionadas con el caso de un cliente, deberá también profundizar en las circunstancias que se dan en éste y en otros casos anteriores, lo que no hay garantía de que haya quedado bien recogido al desarrollar los algoritmos.

Por todo ello, no está claro cual va a ser, en un país concreto, el impacto final sobre el empleo de los avances y aplicaciones de la Inteligencia Artificial y la robótica. Sin duda, globalmente disminuirán los empleos, pero surgirán otros nuevos y otras modalidades de trabajo. El balance dependerá en gran medida de la política que ese país concreto adopte ya para hacer frente a esta nueva realidad. En este sentido, los ejes claves son tres: una educación y formación adecuada a las nuevas exigencias que serán demandadas, las políticas públicas en el ámbito digital, y la propia capacidad de adaptación y desarrollo del país, de sus empresas y de sus instituciones.

Es clave por tanto el que se genere ya un debate en la sociedad y los responsables políticos, los juristas, y los directivos empresariales, implementen estrategias y fijen criterios para hacer frente al nuevo entorno. Como bien ha señalado un catedrático experto en Inteligencia Artificial, Senén Barro, este es un tema en el que debemos ocuparnos ahora si no queremos tener que preocuparnos mañana.