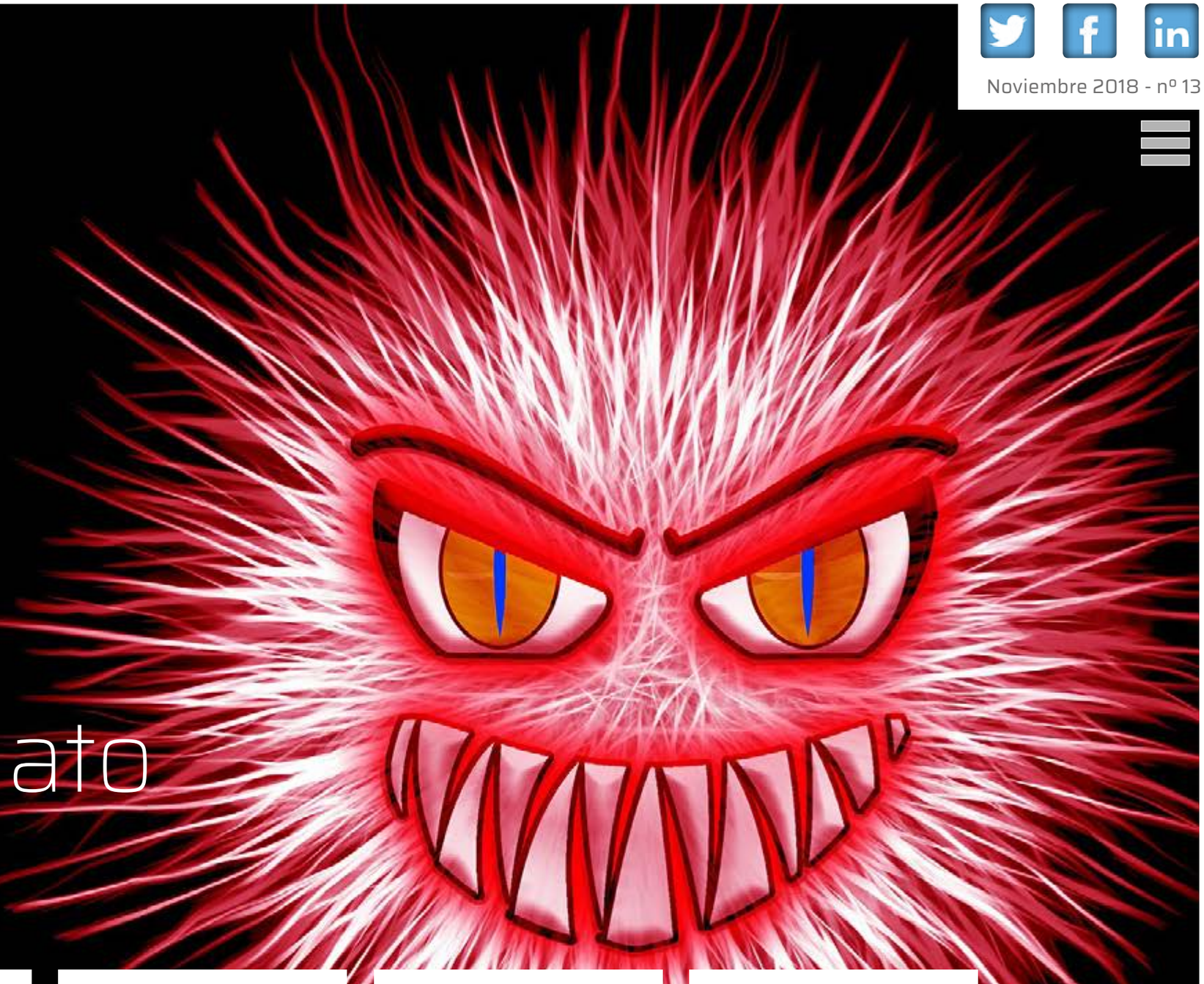
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Noviembre 2018 - nº 13

Malware Evasivo, jugando al gato y al ratón



12ENISE, un evento de referencia

Panda Security, a la conquista del mercado enterprise

Entrevista a Agustín Muñoz Grandes, S21sec | Nextel

Desayuno ITDS. Seguridad para Entornos Financieros

CPX España 2018. La seguridad es Infinity

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

it Digital Security

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

it Digital MEDIA GROUP

Juan Ramón Melara	juanramon.melara@itdmgroup.es
Miguel Ángel Gómez	miguelangel.gomez@itdmgroup.es
Arancha Asenjo	arancha.asenjo@itdmgroup.es
Bárbara Madariaga	barbara.madariaga@itdmgroup.es

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

Malware evasivo, jugando al gato y al ratón

El malware no ha dejado de evolucionar desde que los virus aparecieran como concepción teórica en 1949 y como una realidad pocos años después. Virus, troyanos, gusanos, ransomware, rootkits… la lista es larga y su número ha desbordado las previsiones. El volumen de malware se ha multiplicado por siete en los últimos cinco años, según datos de AV-test, que cada día detecta 350.000 muestras nuevas de malware.

El malware es más inteligente que nunca. Es evasivo. Se ha diseñado para escapar a las técnica de detección, para permanecer invisible hasta que el éxito está garantizado, para jugar al gato y al ratón con las soluciones de seguridad que han tenido que ir más allá de las firmas para poder detectarles.

Hablamos también en este número de 12ENISE, que se celebró en León los días 23 y 24 de octubre organizado por el Instituto Nacional de Ciberseguridad, (INCIBE), y donde se debatió sobre cómo avanzar en ciberseguridad y cómo ésta es un pilar fundamental de la transformación digital.

Fue en 12ENISE donde tuvimos la oportunidad de hablar con Agustín Muñoz Grandes, CEO de S21sec | Nextel, una compañía con ganas de crecer y convertirse en un referente del mercado de ciberseguridad en Europa y en Latinoamérica.

Hablar de Panda Security es hablar de empresas española, de antivirus y de pymes. Pero también es hablar de innovación, de una empresas con presencia en más de 55 países que generan el 82% de los ingresos de la compañía, y que ahora, coincidiendo con la incorporación de María Campos al cargo de VP Sales Worldwide Key Account, MSSP y Telcos, apuesta por estos segmento de mercado para seguir creciendo.

Nuestros #DesayunosITDS de octubre se centraron en la seguridad para entornos financieros, con la participación de SonicWall, Panda Security, F5 Networks, Sophos y Omega Peripherals, que plantearon cuáles son los retos a los que se enfrenta este segmento de mercado.

Por último, incorporamos en este número un especial del evento CPX España 2018 que se celebró los días 17 y 18 de octubre en El Escorial y en el que la compañía habló de Infinity, un paraguas bajo el que no sólo cae su arquitectura de seguridad, sino un acuerdo que permite a las empresas tener acceso a todas las herramientas de seguridad por un coste fijo por usuario.

No solo IT

Inteligencia artificial inteligente o inteligible

ROb1n HOOd de las Networks

La creación de un nuevo perfil profesional: el cyberlawyer

Índice de anunciantes

Actualidad

Desayunos ITDS

Seguridad para entornos financieros, ¿dónde está el reto?

Especial

KASPERSKY lab

938 ataques al minuto.
7 niveles de protección.
1 solución.

Proteja su empresa con cifrado de datos y sistemas de gestión más avanzados

Pruebe gratis Kaspersky Endpoint security for Business ADVANCED

Kaspersky® Endpoint Security for Business

Advanced

12ENISE, un evento de referencia

Más de 2.000 asistentes han participado en la décimo segunda edición del Encuentro Internacional de Seguridad de la Información, 12ENISE, que se celebró en León los días 23 y 24 de octubre organizado por el Instituto Nacional de Ciberseguridad (INCIBE), y donde se debatió sobre cómo avanzar en ciberseguridad y cómo ésta es un pilar fundamental de la transformación digital.

Convertido en encuentro de referencia dentro del sector, un evento en el que hay que estar, un evento dinamizador, con un alto grado de especialización, altavoz de la administración pública en materia de seguridad, ENISE sigue sumando aniversarios y este año se estrenaba en el Palacio de Exposiciones de León. Allí pudimos hablar con algunos directivos que asistieron al evento y que entre otras cosas dejaron claro que sí, que España está en una buena posición para hacer frente a las amenazas. Obviamente se necesitan mejoras, pero "estamos en el camino correcto, las inversiones se han incrementado y se destaca una colaboración público-privada "muy interesante".

En las acreditaciones de ENISE se habla de seguridad como pilar de la transformación digital. Parece claro que sí, pero ¿están las empresas conciencia-

das? Se avanza en ello, en transformar digitalmente la manera de hacer negocio y en ir tomando las medidas de seguridad adecuadas, decía Samuel Bonete, director general de Ketskope para España y Portugal. Para Ignacio Gilart, Director general de White Bear Solutions, “cuanto más grandes son las empresas más concienciación y más inversión.

Dice Pablo López López, Gerente de Ventas y Desarrollo de Negocio de Ciberseguridad en Administración Pública, Telco e Industria de S21Sec, que se está haciendo una buena labor de concienciación para hacer entender a las empresas que la seguridad es una herramienta básica e imprescindible para poder transformarte digitalmente; “La ciberseguridad debe ser pieza fundamente para poder garantizar que los nuevos canales de comunicación con los clientes protegen la información que se está manejando”, y añade que “Wannacry nos hizo un favor en el sentido de la concienciación”

Se opinión similar es Miguel Ángel Martos, director de Symantec para España y Portugal, al asegurar que las empresas lo entienden y lo están aplicando y que la seguridad “ha pasado a ser un facilitador de esa transformación del negocio. Es algo fundamental que se inicia de base en cualquier proyecto”.

Para Raúl Pérez, Regional VP Enterprise Sales de CounterCraft, quién no tenga claro que la seguridad es un pilar fundamental de la transformación

12ENISE RESUMEN

CLICAR PARA VER EL VÍDEO

La ciber-resiliencia, esa capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes, debe mejorarse

digital “ha desaparecido o está a punto de hacerlo”. Raúl Pérez - Regional VP Enterprise Sales.

La concienciación de seguridad va calando entre las empresas dice Vicente Martín, Director Preventa Iberia Panda Security, añadiendo que “tenemos mucho camino andado” y que “estamos mucho mejor que hace unos años”. De manera similar, Juan Luis Gosalvez Palmeiro, director de canal de Varonis, dice que sí, que las empresas lo entienden, pero que el problema es el grado de madurez en términos de seguridad en el que se encuentra cada empresa; “todos somos conscientes, pero no todos podemos abordarlo de la misma manera”.

Resiliencia y Ciberseguridad

Las organizaciones están expuestas a sufrir ataques cada vez más sofisticados y en constante evolución, dirigidos hacia los servicios y sistemas de información que tienen expuestos en las redes. Y porque están expuestas deben estar preparadas para dar respuestas rápidas a este tipo de ataques, permitiendo que los servicios que prestan no se vean interrumpidos, fortaleciendo sus capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua contra las ciberamenazas.

La ciber-resiliencia, esa capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes, debe mejorarse. Durante su ponencia,

Alberto Hernandez Moreno, director general en Incibe

En 12ENISE también se habló de la importancia de asegurar la ciberseguridad y de las implicaciones legales y reputacionales de la fuga de datos

la embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad, Julia Alicia Olmo, repitió en varias ocasiones que las empresas deben mejorar su ciber-resiliencia, y eso es lo que preguntamos. Pablo López López, de S21Sec está de acuerdo "porque estamos hablando de la continuidad de negocio". Apunta Samuel Bonete, de Netskope que la ciber-resiliencia pasa por tomar medidas de precaución y medidas de recovery.

Para Miguel Ángel Martos, de Symantec, la capacidad de resiliencia está asociada directamente con tener una política preventiva, y la manera de tener una política de seguridad efectiva es "prevención, detección rápida y, en caso de ataque, resiliencia y remediación".

"Por la cuenta que le trae a la empresa afectada, más vale que se recupere de cualquier caída que pueda tener cuanto antes y de la mejor forma posible". Dice Ángel Heredia, gestor comercial de Eulen Seguridad, añadiendo que el término resiliencia "es muy bonito, pero yo creo que es mucho más simple, se llama plan de continuidad y los ha habido siempre".

Dice Raúl Pérez de CounterCraft, que la ciber resiliencia es uno de los caminos, y que la prevención es otro, así como la capacidad de detección temprana; "la ciber resiliencia es interesante porque todo el mundo terminará siendo atacado, y sin resiliencia el día que tengas un impacto vas a sufrir mucho".

También para Vicente Díaz, de Panda, la ciber resiliencia es el camino; "la capacidad de rehacerse ante el daño es la mejor opción porque la seguridad al 100% es imposible". Ignacio Gilart, de White Bear Solutions, asegura que cuanto más versátil, cuanto más se adapte una empresa a todo lo que está sucediendo.

Cómo avanzar en Ciberseguridad

Durante la primera jornada del evento los ponentes hablaron de la estrategia de ciberseguridad a nivel nacional, la colaboración internacional y de la necesidad de una legislación internacional. Además, se abordaron las claves para conseguir hogares, coches y sistemas de control industrial ciberseguros y la importancia de contemplar la transformación digital como una oportunidad para el sector.

El director operativo del Departamento de Seguridad Nacional, Joaquín Castellón señalaba que España está en muy buena situación para acoger la Red de Centros de Competencia en Ciberseguridad y mencionó que entre los retos del Plan

¿Por qué hay que ir a ENISE?

ENISE es un evento de referencia dentro del sector. Lo han dejado claro las respuestas de algunos asistentes a este 12ENISE.

"ENISE sigue siendo un evento de referencia, en el que hay que estar. Un foro fantástico para poner en contacto lo que piensa la organización, lo que piensan los organismos de la administración dedicados a la protección y lo que piensa la industria"

Miguel Angel Martos, responsable de Symantec para España y Portugal

"Hay que venir porque es un buen punto de encuentro. El congreso, además, ha evolucionado mucho en cinco años y tiene ahora un ambiente más moderno y dinámico"

Samuel Bonete, director general de Netskope para España y Portugal

"Hay que venir a ENISE porque brinda la oportunidad de reunir a todo el sector para intercambiar experiencias, conocer las novedades y, en general, dinamizar este sector tan importante"

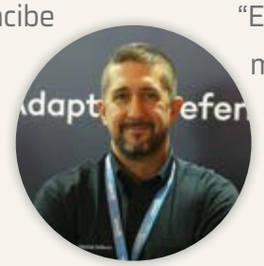
Ignacio Gilart, responsable de White Bear Solutions

"Hay que venir a ENISE porque se es parte del ecosistema y es un punto de reunión del sector; el evento más generalista de toda la parte de ciber seguridad"

Ángel Heredia, gestor comercial de Eulen Seguridad

"ENISE es un evento clave dentro del sector, con un nivel de presencia y de especialización muy alto, y al que hay que asistir para ver el punto de vista de Incibe y de las compañías que participan con en este evento"

Vicente Martín, Director Preventa Iberia Panda Security



"ENISE es el evento, con mayúsculas, el evento en el que todas las empresas que somos alguien en el mundo de la seguridad debemos estar presentes. Colaborar con el Incibe en un evento como este era obligatorio"

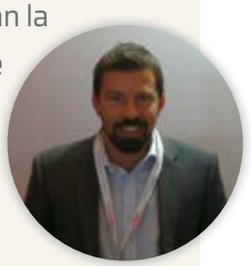
Pablo López López, Gerente de Ventas y Desarrollo de Negocio de Ciberseguridad en Administración Pública, Telco e Industria de S21Sec

"Hay que venir a ENISE porque es un punto de encuentro del mundo de la ciberseguridad y da mucha salud al sector"

Raúl Pérez, Regional VP Enterprise Sales de CounterCraft

"ENISE es un evento puntero en el que se dan la mano los principales actores en el sector de la seguridad de la información"

Juan Luis Gosalvez Palmeiro, director de canal de Varonis



de Ciberseguridad se encuentran la creación del Centro de Operaciones de Seguridad, el impulso de I+D+I en ciberseguridad nacional, la construcción de plataformas de intercambio y análisis de información sectorial, la captación de talento, el apoyo a las pymes para adaptarse a los retos de la ciberseguridad y avanzar hacia una cultura de Ciberseguridad Nacional.

Por su parte, Eduardo Mastranza, Ejecutivo de Gartner, habló de la situación de la ciberseguridad a nivel global señalando que "el miedo en ciberseguridad ha dejado de funcionar" porque en 2021 los incidentes de seguridad dejarán de tener impacto en la sociedad o en los clientes. Por este motivo, ha abogado por contemplar la transformación digital como una oportunidad para quien trabaja en ciberseguridad, aumentar la creatividad, enfocar el discurso hacia la confianza y buscar más la versatilidad de los profesionales.

En cuanto a la colaboración internacional en defensa de la ciberseguridad, la embajadora en Misión Especial para las Amenazas Híbridas y la Ciberseguridad, Julia Alicia Olmo, resaltaba que "no existe una regulación internacional del ciberespacio y la regula-

INCIBE, en colaboración con la Junta de Castilla y León y el Ayuntamiento de León, lanzará una nueva convocatoria de Ciberemprende

ción nacional no es suficiente, por lo que debe desarrollarse una regulación internacional desde Naciones Unidas". Sobre este tema también ha hablado la secretaria ejecutiva del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos (OEA), Alison August Treppel.

Hogares, coches y sistemas de control industrial ciberseguros

El Internet de las cosas y la ciberseguridad han sido otros de los temas que se abordaron en la primera jornada de 12ENISE. Azucena Hernández, de Cybentia, presentaba el primer programa ideado específicamente para medir el nivel de ciberseguridad de los vehículos nuevos, explicado que es importante despertar en la sociedad que la misma preocupación que existe por viajar en un coche tradicionalmente seguro (dotado de airbags, ABS, ESP…) se traslade a viajar en coches ciberseguros. En este punto ha señalado que organismos, instituciones, directivos y usuarios deben implicarse.

El responsable de Sistemas de Control Industrial (SCI) de INCIBE, Enrique Redondo, indicaba que "con la irrupción de las Nuevas Tecnologías, los sistemas de control industrial se han ido conectando a redes más inseguras y han heredado los problemas de ciberseguridad de la parte de la Tecnología de Información. Redondo ha señalado que "el número de incidentes en infraestructuras soportadas por sistemas de control industrial ha aumentado y la mejor solución para combatirlos es trabajar de forma colaborativa con todos los agentes clave". En este sentido, abogaba por instaurar buenas prácti-

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

cas en ciberseguridad e ir tendiendo progresivamente a modelos de certificación de sistema.

La jornada se completaba con una mesa redonda centrada en el reto de la seguridad integral y la convergencia IT/OT para la transformación digital, una convergencia que va a suponer un gran avance a la hora de la implantación de la industria 4.0 y de la tecnología digital dentro de nuestra sociedad.

Internacionalización en ciberseguridad

La necesidad de la internacionalización de la industria española, la búsqueda de financiación y la colaboración entre empresas de tamaños diferentes fueron algunos de los temas tratados en la parte de emprendimiento del Encuentro Internacional de Seguridad de la Información (12ENISE) organizado por el Instituto Nacional de Ciberseguridad (INCIBE).

El director de Infraestructuras, Sanidad y TIC del Instituto Español de Comercio Exterior (ICEX), Jorge Alvar, señaló que "la internacionalización no es una opción, sino una necesidad" y ha añadió que las empresas y startups están obligadas a internacionalizarse para crecer. Esta ha sido una de las conclusiones extraídas del primer panel de Emprendimiento de la segunda jornada de 12ENISE, en el que también se puso de manifiesto que "en España hay capacidad técnica para emprender y para saltar fuera, pero muchas veces el problema es de mentalidad, de ambición o de falta de financiación".

> La transformación digital es una oportunidad para quien trabaja en ciberseguridad, aumentar la creatividad, enfocar el discurso hacia la confianza y buscar más la versatilidad de los profesionales

Los expertos defendieron que en España se están haciendo grandes cosas para apoyar a las startups, como el programa de Ciberemprende de INCIBE y recomendaron a las empresas dirigirse al mercado latinoamericano sin olvidar el mercado asiático. Otro de los temas abordados fue la necesaria colaboración entre las startups y las grandes empresas de ciberseguridad.

12ENISE también fue el marco elegido para presentar el nuevo ciclo del programa de apoyo al emprendimiento del Instituto Nacional de Ciberseguridad. El responsable de Industria de Ciberseguridad de INCIBE, Ignacio Caño, anunció que próximamente, INCIBE en colaboración con la Junta de Castilla y León y el Ayuntamiento de León lanzará una nueva convocatoria de Ciberemprende en la que elegirán los mejores 30 proyectos en fase de semilla y los llevarán por un proceso de mentoring y de formación. Asimismo, el próximo año se desarrollará una nueva edición de Cybersecurity Ventures, que pretende superar el número de proyectos presentados en la anterior edición a la que concurrieron 75 proyectos de los cuales se aceleraron los 15 mejores.

El reto de asegurar la ciberseguridad

En 12ENISE también se habló de la importancia de asegurar la ciberseguridad y de las implicaciones legales y reputacionales de la fuga de datos. Respecto a la primera, los expertos en la materia señalaron que "asegurar los ciberriesgos es un reto por muchas razones, pero especialmente porque hay una falta de concienciación. Nadie se plantearía que su empresa no tenga un seguro contra incendio pero no tienen un seguro de este tipo". Del mismo modo, han apuntado que "hay

Enlaces de interés...

- Todo listo en León para la duodécima edición de ENISE
- Tercera edición del Premio ENISE a la mejor iniciativa escolar de ciberseguridad
- El CISO, figura fundamental en los organigramas de las empresas en el siglo XXI
- Empleo en ciberseguridad: INCIBE publica una convocatoria para cubrir 27 puestos
- El Centro de Respuesta a Incidentes de Seguridad pasa a llamarse INCIBE-CERT

neral de la Protección de Datos y la Directiva NIS de seguridad sobre sistemas y redes. En los seis meses desde que entró en vigor esta nueva normativa, se han registrado 300 brechas. Andrés Calvo, coordinador de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos, apuntó que "la intención es que la adaptación llegue por capilaridad a todo nuestro tejido empresarial" mientras que Francisco Pérez Bes, secretario General de INCIBE, apostó por "establecer cultura interna de ciberseguridad dentro de las organizaciones" y resaltó que la nueva directiva NIS proteja al notificante de las brechas de seguridad ente el operador.

Como novedad este año, 12ENISE ha contó con un 'Trade Show' o espacio expositivo en el que han participado medio centenar de empresas del sector que han dado a conocer soluciones innovadoras además de presentar sus productos y hacer demostraciones. Asimismo, dentro del International Business Forum un total de 10 inversores internacionales procedentes de Alemania, Colombia, Chile y México, mantuvieron reuniones bilaterales con proveedores españoles de productos y servicios de ciberseguridad.

Las empresas deben estar preparadas para dar respuestas rápidas a los ciberataques para que los servicios que prestan no se vean interrumpidos

que perder el miedo a notificar y existen pólizas para mitigar el impacto en la cuenta de resultados.

Respecto a la fuga de datos y las implicaciones legales y reputacionales, Pablo García, vicepresidente de Internet Society-Capítulo español, señaló que 2018 "es el año de las fugas de datos, el año de las brechas de ciberseguridad" y hablaron de los cambios que supone el nuevo Reglamento Ge-

Compartir en RRSS

iGoNet Fraud Prevention & Intelligence

cambia de nombre pero no de pasión!

BOTECH

Fraud Prevention & Intelligence

Más de una década especializados en **Detección de fraude, Ciberinteligencia y Ciberseguridad**

Principal compañía de ciberseguridad en el sector bancario

Empresa española líder en prevención de fraude

Proveedor referente en ciberinteligencia y ciberseguridad

WWW.BOTECHFPI.COM

BOTECH FPI BOTECH FPI BOTECH FPI

España
Ronda de Valdecarrizo Nº 41-A, 1ª planta.
Tres Cantos, C.P. 28760, Madrid.
+34 (91) 174 35 66

México
Av. Ejercito Nacional 207, Piso 1,
Colonia Verónica Anzurez. Mexico City, DF.
11300.
+52 (55) 5025 4009 x1160

S21sec | Nextel: “El mérito está en la capacidad de detección y de respuesta”

El pasado mes de junio se anunciaba la fusión entre 2S1sec y Nextel para crear “la mayor compañía de ciberseguridad de Europa”, pero el camino se había iniciado unos años antes, en 2014, cuando la portuguesa Sonae compró una participación mayoritaria en S21sec, una empresa que su actual CEO, Agustín Muñoz-Grandes, define como “muy innovadora, tipo startup”. Dice también el directivo que con la entrada del Grupo Sonae en la compañía se cambió de etapa y se cambió también “el nivel de ambición”.

Durante los 18 años de vida de S21sec se lanzaron productos tan novedosos como Lookwise Device Manager en 2005 para hacer frente a la regulación del cumplimiento o la seguridad del big data; se crearon los S21sec Labs en 2006, el primer centro de innovación europeo dedicado a la industria de la ciberseguridad; dos años después la compañía lanzaba su unidad eCrime de servicios antifraude y en 2009 S21sec University, ofreciendo cursos a profesionales técnicos y no técnicos interesados en mejorar sus habilidades.

S21sec fue una de las empresas pioneras en España en el mercado de seguridad. Creada en el

"Con la entrada del Grupo Sonae en S21sec en la compañía se cambió de etapa y se cambió también el nivel de ambición"

año 2000, prácticamente cuando se estaba creando el sector. En su etapa actual, tras la adquisición por parte de su propietario, el grupo inversor SONAE IM, de la firma Guipuzcoana Nextel, la compañía está dispuesta a crecer, a convertirse en un referente en Europa y en Latinoamérica, "y estamos poyándonos para ello en la adquisición de empresas", nos cuenta Agustín Muñoz-Grandes en una entrevista.

Compras, inversiones y fusiones, porque si la compañía adquiría a la portuguesa Sysvalue en 2015, invertía en Secucloud en 2017 y se fusionaba con Nextel en 2018. La apuesta por Sysvalue "nos ha dado un tamaño importante en Portugal", dice Agustín Muñoz-Grandes, añadiendo que la fusión con Nextel les coloca "claramente" como la empresa de seguridad número uno en España y Portugal, "con más de 400 profesionales dedicados a la seguridad". El proceso no ha terminado, porque se siguen estudiando otras operaciones en Europa.

Sobre si lo que buscan está en la línea de comprar servicios, integración, cuota de mercado o productos, dice Muñoz-Grandes que S21sec | Nextel se presenta al mercado "como una empresa de servicios gestionados, porque estamos viendo que la seguridad hoy en día tiene que ser gestionada". Asegura que la integración de sistemas no es suficiente, sino que tiene que ser parte de un servicio gestionado en el que además se refuerce la monitorización y la gestión con servicios de Threat Intelligence, en el que puedas integrar multitud de fuente para prevenir los ataques, detectar quiénes son los actores que hay detrás, predecir su comportamiento... "Es decir que ya no es sólo monitorización y ya no es sólo integración", concluye el directivo.

La fusión con Nextel ha reforzado la oferta de servicios de S21sec, y en el resto de los países "iremos viendo cuál es la opción más complementaria". Sobre Sysvalue dice Muñoz-Grandes que ha permitido a S21sec | Nextel poner un pie en el país vecino, tener un punto partida para poder ofrecer los servicios gestionados y conseguir clientes como Galp o Euronex. En Portugal "estamos ganado clientes de referencia muy rápido y la idea es esa, en lugar de empezar de cero en Austria, o en Alemania, adquirir una empresa sobre la que construir, sobre la que llevar el portfolio de servicios".

Modelo Multi-SOC y Servicios

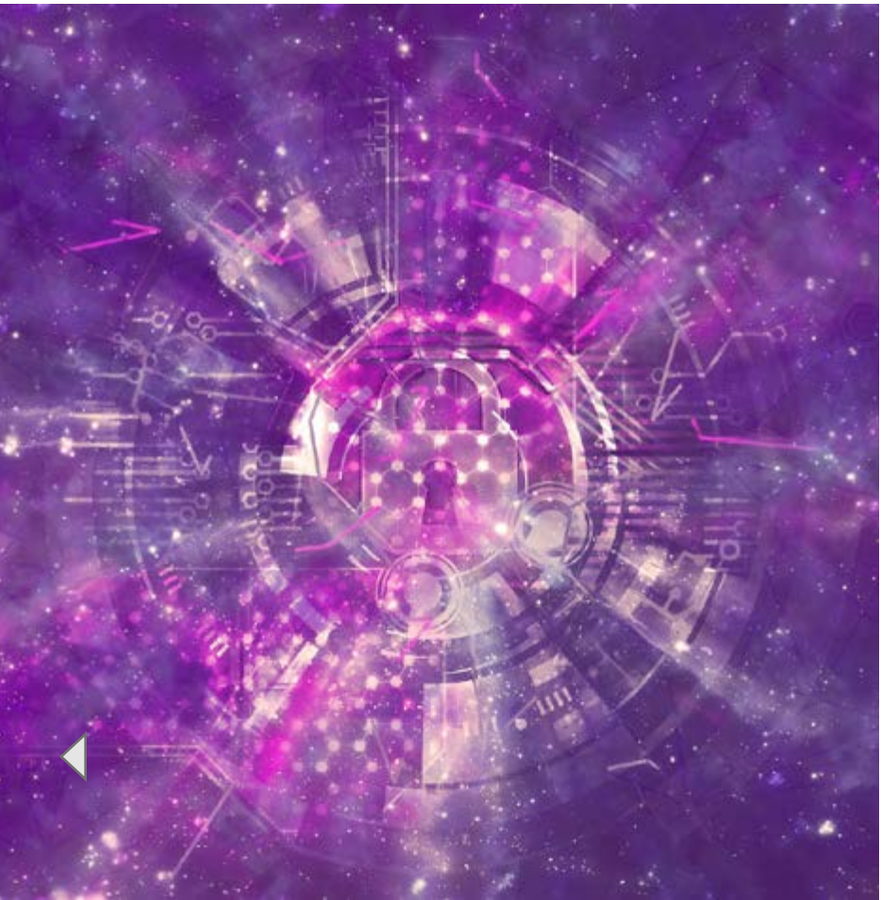
Preguntamos al CEO de S21sec | Nextel si la expansión de la compañía supondrá la apertura de otros centros de operaciones de seguridad y de alerta temprana. Explica que el modelo con el que se trabaja es un modelo multi-SOC en el que el grueso de los servicios, de los analistas de ciber-

"La fusión con Nextel ha reforzado la oferta de servicios de S21sec, y en el resto de los países iremos viendo cuál es la opción más complementaria"

seguridad, de la parte de Threat Intelligence y de servicios avanzados está centralizada, y en cada países se coloca una capa local, de atención al cliente. Es decir que "los recursos de más valor añadido, las capacidades más avanzadas están centralizadas, y luego hay una capa de cercanía al cliente que sí que está en el país en el que operamos. Eso ya lo tenemos activo en España, en Portugal y en México y es un modelo de servicio que queremos extender a otros países según vayamos extendiendo nuestras operaciones".

Los servicios se han convertido en parte importante del mercado de la seguridad. Según datos de Transparency Market Research, este mercado de MSSP generará ingresos de 87.590 millones de dólares para el año 2025, frente a los 30.910 millones ingresados en 2016. Se estima que el mercado registrará una tasa media de crecimiento anual del 12,5% de 2017 a 2025.

Los servicios son el core de S21sec | Nextel. A primeros de año se incorporaba a Jorge Hurtado como VP de servicios gestionados de la compañía para reforzar el equipo. Sobre el tipo de servicios que más se están demandando, dice el máximo responsable de S21sec | Nextel que se ha visto mucho incremento de la demanda de respuesta ante incidentes, el Digital Forensics and Indicent Response de la compañía. Es un dicho en sector que la seguridad 100% no existe y que es un hecho que tarde o temprano vas a tener un incidente de seguridad. Partiendo de esta afirmación, dice Muñoz-Grandes que "el mérito está en tu capacidad de



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

La sede de Madrid

La evolución de toda gran compañía puede seguirse estudiando sus sedes y oficina. Su crecimiento, o decrecimiento, va a par de los metros cuadrados y plazas de parking. Como parte de su trayectoria, S21sec| Nextel cuenta con oficinas en San Sebastián, que es donde arrancó S21sec, a las que se suman las del Bilbao, territorio de Nextel, y la de Madrid "que es donde mayor número de personas tenemos", explica Agustín Muñoz-Grandes, CEO de S21sec | Nextel.

La fusión con Nextel también tiene un antes y un después en lo que a sede se refiere, porque será a primeros de año cuando la compañía se trasladará a una nueva sede en Madrid, en lo que será el edificio corporativo del Grupo. S21sec | Nextel ocupará dos plantas completas del edificio donde se alojará un nuevo Security Operations Center (SOC-CERT) con una plantilla de más de 50 personas, en modo 7x24x365.

El SOC cuenta para ello con herramientas de inteligencia, análisis y detección de amenazas (threat intelligence) de desarrollo propio, reforzadas con soluciones avanzadas de partners estratégicos, así como sistemas de inteligencia artificial y machine learning.

Sobre el nuevo SOC dice Muñoz-Grandes que es diferente a aquellos primeros SOC que "tenían que ser blindados". Parece que ahora en los SOC modernos "todo tiene que ser de cristal y muy luminoso", dice, asegurando también que el edificio es "espectacular" y que van a tener una "oficinas muy cómodas".

detección y en tu capacidad de respuesta, y es ahí donde nos estamos focalizando más".

Se han dado casos en los que empresas que no son clientes de S21sec | Nextel han llamado a la compañía para la contención de un incidente de seguridad. Y a partir de esa contención se realiza un análisis del gap que hay entre el nivel de seguridad que tiene esa empresas y el que debería tener, a partir del cual se lanzan unas recomendaciones; es entonces cuando "entran en juego los servicios de consultoría para abordar ese plan, los servicios de integración (gracias a la compra de Nextel), para poder desplegar la infraestructura, y después todo engancha con los servicios de seguridad gestionada". De forma que se consigue el círculo completo: respuesta al incidente, consultoría, integración y monitorización 24x7.

El mercado MSSP, o de servicios gestionados de seguridad, generará ingresos por valor de 87.590 millones de dólares para el año 2025

Concienciación, ¿necesitamos otro Wannacry?

Dice Muñoz -Grandes que no se necesita otro Wannacry para seguir despertando conciencias, que con uno ha habido suficiente, que la persona con la que las empresas de seguridad se reúnen ahora es "con el consejero delejado de un gran banco, o el director de una gran empresa. Y eso antes no pasaba". Antes se hablaba con el CISO, o el responsable de IT y se hablaba de virus, ahora se habla con el CEO y se habla de negocio, de poder abrir la empresa el lunes porque tiene un problema de seguridad. Sí, definitivamente, la concienciación ha mejorado, se tiene en cuenta que "como parte de los procesos de la transformación digital la seguridad es parte del contorno, no puedes ignorarla y afecta de forma directa al negocio de las empresas".

S21sec | Nextel trabaja en un modelo multi-SOC en el que el grueso de los servicios, de los analistas de ciberseguridad, de la parte de Threats Intelligence y de servicios avanzados está centralizada

La seguridad, por tanto, ha entrado en los consejos de dirección, una queja recurrente que parece que se está superando. De hecho, nos cuenta Agustín Muñoz-Grandes que S21sec | Nextel ofrece asesoría a los consejos de dirección con una persona en el comité de dirección cuando tienen que tratar temas de su plan de seguridad; “hay esa sensibilidad, demanda de ese tipo de asesoría y cercanía a los clientes”.

Previsiones de S21sec | Nextel

También hablamos con Muñoz-Grandes sobre previsiones: seguir creciendo por encima del mercado. “A nivel de negocio orgánico el año pasado crecimos un 25%”, dice el CEO de S21sec | Nextel, añadiendo que ese crecimiento es la suma de la imagen de marca y del posicionamiento que tenemos, junto con el portfolio renovado de servicios; “de esa capacidad que te comentaba de seguridad gestionada y de capacidad de despliegue de soluciones que están teniendo muy buena acogida. Y por lo tanto a corto plazo esperamos seguir contando con estos ratios de crecimiento”.

Agustín Muñoz-Grandes habla también de crecimiento a nivel regional. Un crecimiento “en el que hace falta contar con unos servicios que escalen bien geográficamente y unas metodologías de trabajo que te permitan tener unas competencias y un personal centralizado en este caso en España pero que nos permita también apoyar al resto de países donde vamos abriendo operaciones”. Estos modelos escalable, dice Muñoz-Grandes, requieren su tiempo para ir escalando.

Enlaces de interés...

- S21sec | Nextel presente en 12ENISE
- S21sec | Nextel demuestra el potencial de Lookwise Device Manager en el ATM & Payments Innovation Summit
- Lookwise Device Manager de S21sec premiado con el ATM CyberSecurity Excellence Award 2018
- ‘La fusión con Nextel forma parte de un proceso continuo que va a seguir’ (S21Sec)
- La fusión de S21sec y Nextel crea la mayor empresa española de servicios de ciberseguridad
- Nueva solución de S21sec para mejorar la seguridad de los pagos comerciales

Compartir en RRSS

SOPHOS

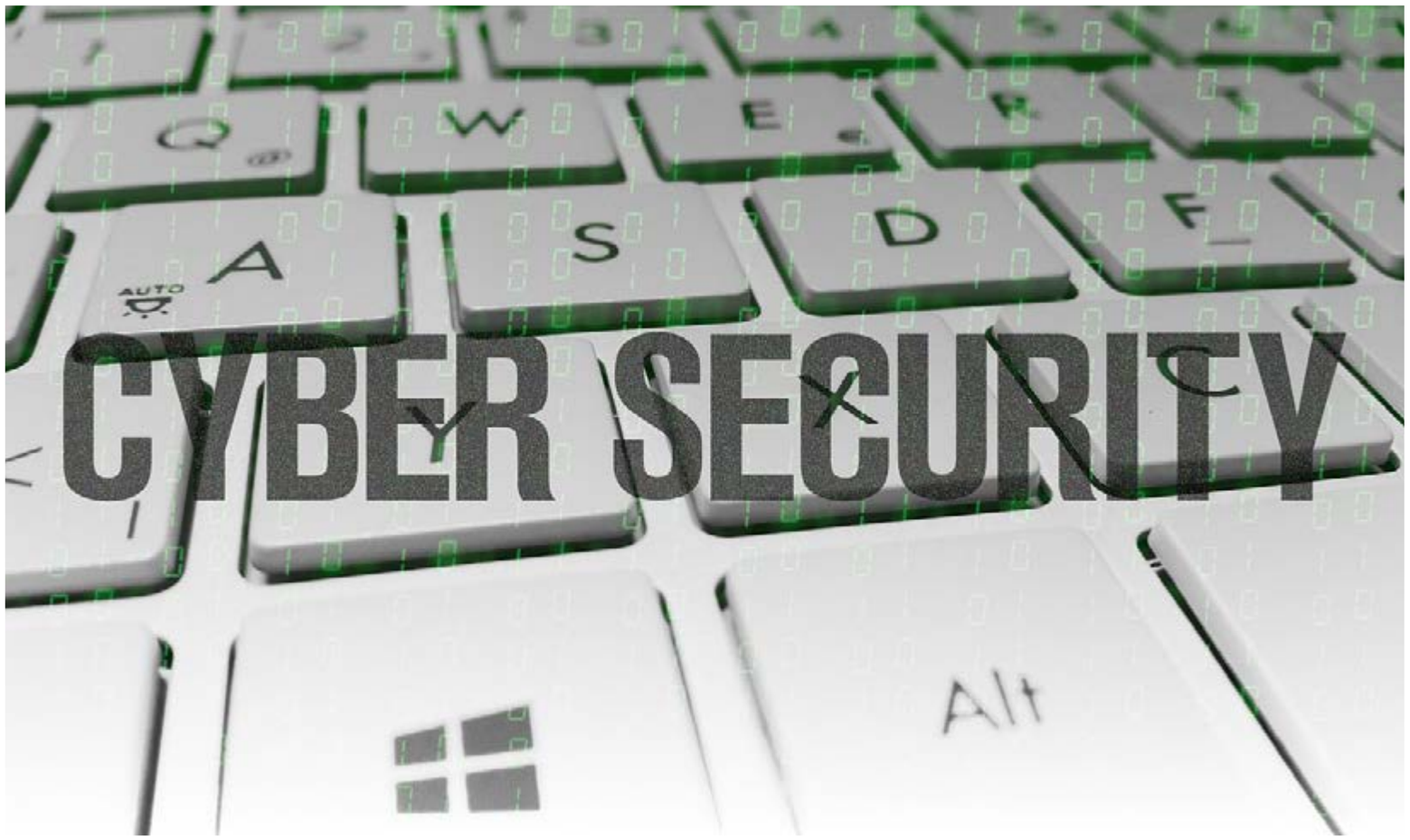
INTERCEPT X

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



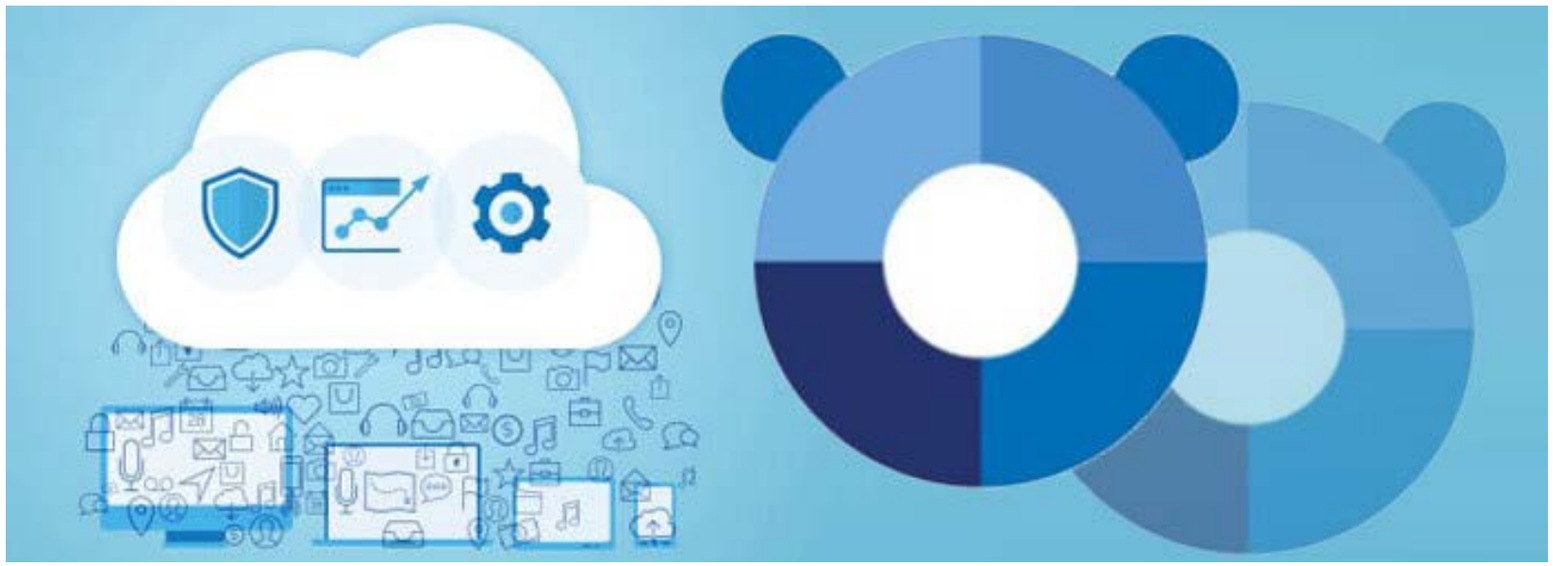
Panda Security, a la conquista del mercado Enterprise

Hablar de Panda Security es hablar de empresas española, de antivirus y de pymes. Pero también es hablar de innovación, de una empresas con presencia en más de 55 países que generan el 82% de los ingresos de la compañía, y un foco en un mundo empresarial que genera el 80% de los ingresos, frente al 20% de ventas del mercado de consumo.

Hablar de Panda Security es hablar de una empresas que protege a más de 30 millones de usuarios, capaz de procesar diariamente más de 500 millones de archivos o neutralizar más de 200 millones de nuevos malware. Esta es la empresa que se encontró María Campos cuando hace unos meses decidió aceptar el puesto de VP Sales Worldwide Key Account, MSSP y Telcos de Panda Security tras pasar más de tres años en McAfee. Un puesto que busca colocar a la compañía en el segmento alto del mercado, en el mundo Enterprise, de las Telcos y de los proveedores de servicios de seguridad gestionada.

Lo contaba María Campos durante una rueda de prensa en la que se presentaba también un nuevo

Panda Security busca su hueco en el segmento alto del mercado, en el mundo Enterprise, de las Telcos y de los proveedores de servicios de seguridad gestionada



programa de canal de la mano de Karina Rojas, nombrada Enterprise Channel Account Manager con el objetivo de reforzar la estrategia de canal de Panda.

Haber nacido y crecido en el mercado de antivirus tiene sus ventajas ahora que el perímetro ha saltado por los aires, ha puesto en evidencia el valor del firewall y la vuelto a colocar al endpoint en el centro de la estrategia de seguridad. “El objetivo es el endpoint”, decía María Campos, asegurando que ese punto final “es el nuevo perímetro”, es desde donde se puede acceder a otros objetivos, exfiltrar información, robar credenciales, recabar inteligencia o desplegar nuevos ataques.

El tiempo entre que se produce un ataque y se detecta sigue siendo demasiado, entre otras cosas porque los atacantes son cada vez más eficientes comprometiendo sistemas que las víctimas detectándolos. El reto está ahí, en reducir ese gap. Hace años que algunas empresas se dieron cuenta de que había que innovar, modificar los modelos de seguridad, y Panda fue una de ellas. Se dieron cuenta que, de mantenerse el crecimiento de nuevos malware, la cantidad de analistas necesarios para separar el grano de la paja sería insostenible en pocos años y lanzaron su Inteligencia Colectiva aprovechando todo el potencial que podía dar el cloud. De forma que frente a un modelo tradicional basado

THE STATE OF SOAR REPORT, 2018

El panorama empresarial actual es un acto de equilibrio delicado entre el avance tecnológico y la seguridad. Los cambios en el lugar de trabajo y las innovaciones técnicas han hecho que sea más fácil hacer negocios y vivir nuestras vidas, pero asegurar estos múltiples desarrollos es una tarea gigantesca que recae sobre los equipos de seguridad ya sobrecargados de trabajo.

Ya hay una gran cantidad de investigaciones que destacan el crecimiento sin fin de las alertas de seguridad, una brecha de habilidades de seguridad cada vez mayor y la consiguiente fatiga que se acumula en los equipos de seguridad con personal insuficiente. Demisto realizó un gran estudio para profundizar en estos temas, sus manifestaciones y posibles soluciones.

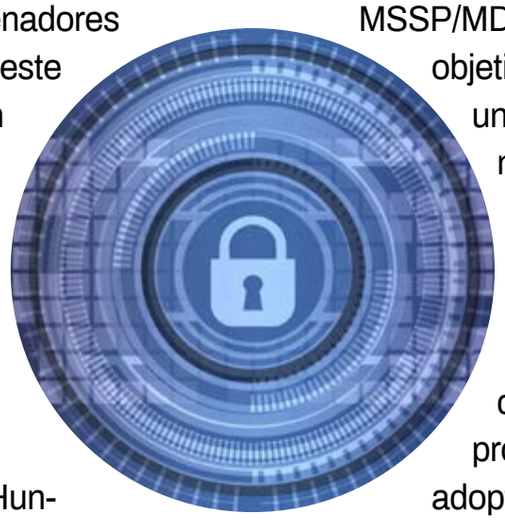
El endpoint recupera protagonismo

Dice María Campos, VP Sales Worldwide Key Account, MSSP y Telcos de Panda Security, que "tiene mucho sentido interesarse por el endpoint". Nuevamente protagonista de la infraestructura de seguridad, a su alrededor han aparecido tecnologías que están pegando fuerte en el mercado. La última EDR, Endpoint Detection and Response, que frente a las EPP (Endpoint Protection Platforms) tradicionales, está sacudiendo el mercado.

Interesarse por el endpoint tiene todo el sentido si tenemos en cuenta que empresas como SonciWall, Check Point o Cisco están ampliando su oferta para añadir protección al endpoint. Es decir, que expertos en seguridad de red, apuntan hacia el punto final. Camino contrario fue el tomado por Sophos hace años. En 2011 la empresa de antivirus británica anunciaba la compra de Astaro, adentrándose en el mercado de UTM, en el mercado de seguridad de red. ¿Quiere hacer lo mismo Panda? No, dice María Campos. Y es que ahora "hay otros mecanismos para recolectar toda la información que llega de la red sin entrar en el mundo appliance".

en el PC del usuarios decidieron moverse al cloud, evitando la ralentización de los ordenadores y ganando capacidad de escala. "Y este ha sido el gran avance de Panda en el mundo de la seguridad", apunta María Campos.

Un avance que no se detuvo ahí, sino que ha dado pie a la compañía para avanzar en machine learning, en inteligencia artificial, en EDR (Endpoint Detection and Response), en capacidades de Threat Hunting y en un nuevo objetivo: el mercado Enterprise, MSSP/MDR y Telco. La consecución de ese objetivo está a cargo de María Campos, un equipo que ya suma ocho personas, y un canal especializado de 15 o 20 partners.



Mercado Cautivo

Se habla del mercado Enterprise como un mercado cautivo de sus propias soluciones, las que decidió adoptar hace años y que han arraigado tanto en los procesos y las arquitecturas, que pocos se deciden a cambiar.

Explica María Campos que Panda Security no quiere abordar ese mercado con el fin de sustituir a esos fabricantes tradicionales, sino "para ponernos por encima, para cubrir la última milla", para aportar el valor de las tecnologías EDR, las tecnologías de Threat Hunting as a Service, las de control del dato y del parcheado de vulnerabilidades con las que no contaban en otros intentos, anteriores e infructuosos, por llegar a la cima de la pirámide. Y a estas últimas se añadirán más en un futuro cercano, como la analítica de conductas (UEBA) o ampliar el espectro del endpoint incorporar al IoT como un punto final que también debe tenerse en cuenta.

El objetivo es multiplicar por tres o por cuatro la facturación en ese mercado Enterprise que por ahora sólo representa el 10% del total de la compañía.

> En endpoint es el nuevo perímetro, es desde donde se puede acceder a otros objetivos, exfiltrar información, robar credenciales, recabar inteligencia o desplegar nuevos ataques

Programa de canal

En 2016 el mercado de servicios de seguridad gestionada, o MSSP, generó 9.400 millones de dólares, según Gartner. El 90% de esos ingresos son generados por servicios tradicionales que según María Campos "no tardarán en ser comoditizados" y que van desde la gestión de un firewall, un SIEM o un proxi, a la monitorización de eventos. El 10% de los ingresos, o 940 millones de dólares, se generaron a partir de servicios diferenciados. La clave está en que este tipo de servicios, los de detección y respuesta, los MDR, crecerán un 45%, "y es por eso por lo que invertimos en este segmento", explica María Campos, añadiendo que es donde tiene sentido un programa de canal.

Los MDR son, en opinión de María Campos, una evolución de los MSSPs. Son los que están especializados en la detección y respuesta de amenazas, en Threat Hunting, los que cuentan con analistas capaces de estudiar los indicadores de compromiso. Deloitte, Telefónica, Innotec o Grupo ICA son algunos de los nombres que identifican a esos 15 o 20 partners que entran en ese grupo de MDR.

Karina Rojas, Enterprise Channel Account Manager

De forma que la nueva estrategia de canal de la compañía, que busca hacerse un hueco en el mercado alto de la pirámide, en el mundo Telco, Enterprise y de servicios gestionados, lleva a la compañía a poner en manos del canal todas las ventas, a ser 100% canal. Para ello, una de las prioridades está en proporcionar herramientas para que el integrador y los partners que quieran introducirse en el mundo de los servicios, puedan hacerlo con las soluciones de la compañía. Así lo aseguraba Karina Rojas, nombrada Enterprise Channel Account Manager, con el objetivo de reforzar la estrategia de canal de Panda.

De esta manera, el foco de la compañía se centra en el canal y, dependiendo de la tipología del cliente, operan de manera diferente. Por un lado, con partners más pequeños se encargan de abastecer a todas aquellas denominadas pyme, con un programa muy específico que les permite dar servicio a través de su solución. Por otro lado, Panda dispone de una red de integradores que tienen SoC con una herramienta para permitirles llegar al puesto de trabajo.

Para Karina Rojas dotar a los partners de herramientas avanzadas adaptadas a las necesidades de cada cliente, unido a su profundo conocimiento del mercado "les aporta más valor, impulsándolos y les sitúa en una posición privilegiada". it

Enlaces de interés...

- María Campos deja McAfee por Panda Security
- El endpoint necesita algo más que un antivirus y el EDR es la clave
- El reto del ransomware y otras grandes amenazas
- La Seguridad Endpoint a debate con los líderes del sector
- Qué hacer para que más mujeres trabajen en ciberseguridad... y por qué no lo hacen
- Panda Security prepara su primera cumbre sobre ciberseguridad

Panda Adaptive Defense

Control y visibilidad de tus datos personales

Data Control

Simplifica el cumplimiento del GDPR

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

Descubre y audita

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

Monitoriza y detecta

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

Simplifica la gestión

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

Control de datos

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

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

panda

pandasecurity.com/business/

Tráfico ilegal de personas,

ciberterrorismo o Fake News, el lado oscuro de las redes sociales

Aunque las redes sociales han aportado numerosos beneficios a millones de usuarios y de empresas, también tienen su lado oscuro. El potencial de éstas está siendo aprovechado por las mafias de inmigración clandestina, grupos terroristas como el Estado Islámico o países para propagar Fake News.

Una cosa está clara. La llegada de las redes sociales ha traído numerosos beneficios a la vida de millones de personas y negocios. En el ámbito personal, éstas permiten una comunicación instantánea, una mayor relación con familiares y amigos, nuevas oportunidades laborales o el hecho de que permiten compartir información y conocimiento, fomentando, además, la denuncia social.

A las empresas les ha permitido aumentar la visibilidad de la marca, gracias a que es un canal de difusión de contenidos de la empresa. Además, gracias a las redes sociales se puede tener una mejor comunicación con clientes y proveedores, permitiendo la fidelización y un contacto con potenciales clientes, entre otros muchos beneficios.

Pero no todo son ventajas. Las redes sociales permiten llegar a millones de personas, con lo que

La lucha de Twitter contra las Fake News impulsa sus resultados económicos

Si los resultados económicos de Amazon y Google no han cumplido con las expectativas de los analistas, la política que está llevando a cabo Twitter sí que ha convencido a Wall Street. Ésta es una de las principales conclusiones de los resultados presentados por la red social, que han superado las previsiones y cuya estrategia de luchar contra las cuentas que propagan noticias falsas ha hecho que se haya convertido en una herramienta de calidad para anunciantes.

Los ingresos por publicidad de Twitter han crecido un 29% en el tercer trimestre del año, alcanzando los 650 millones de dólares. En esta subida, los acuerdos alcanzados con grandes medios de comunicación, como Live Nation Entertainment, o con las grandes ligas de baseball o de fútbol, han sido claves a la hora de que Twitter haya presentado unos ingresos de 758 millones de dólares, casi 56 millones de dólares más de lo que habían pronosticado los analistas.

Esta situación contrasta con la vivida por Twitter hace tres meses, cuando la firma anunció que tanto sus ingresos como su número de usuarios habían caído. En esta ocasión, la reducción del número de usuarios se ha debido a la eliminación de miles de cuentas falsas.

El pasado mes de julio, Twitter informó de que había suspendido en los últimos meses más de un millón de cuentas al día. Sólo en los meses de mayo y junio, Twitter había suspendido más de 70 millones de cuentas, un ritmo que, según confirmó la red social, quiere mantener.

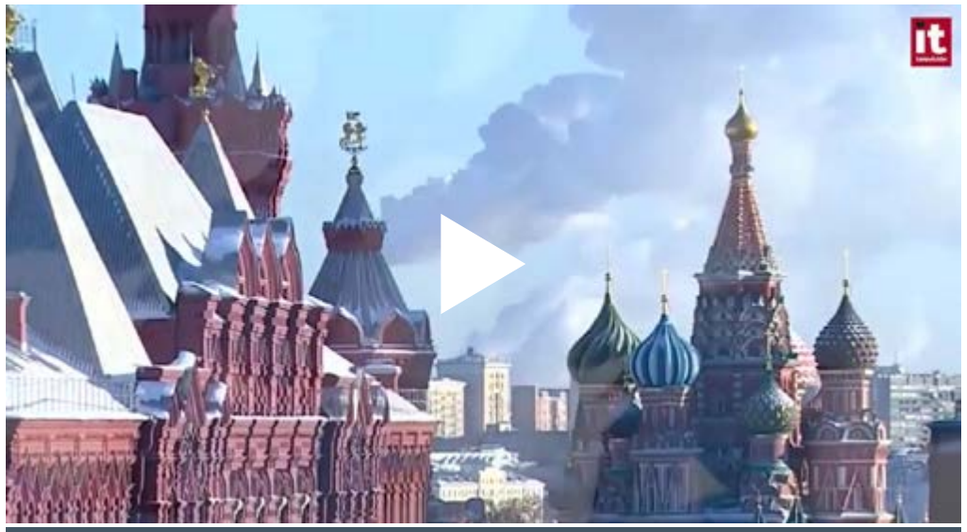
Las mafias de inmigración clandestina utilizan las redes sociales para captar a personas que quieren llegar a Europa

mafias, delincuentes y terroristas las utilizan con fines delictivos.

Tráfico ilegal de personas

Según datos de la Oficina Europea de Apoyo al Asilo (EASO), que recoge El Mundo, las mafias de inmigración clandestina utilizan las redes sociales para captar a personas que quieren llegar a Europa. La estrategia de estas mafias pasa por estar presente en, por ejemplo, Facebook, Instagram, Twitter o Google+ como “simples” agencias de viaje, prometiendo llegadas garantizadas a buenos precios.

Aunque el primer contacto se realiza a través de estas páginas, los “acuerdos” se cierran utilizando



Daesh ha sabido utilizar las redes sociales e Internet como herramienta de propaganda, de captación, de formación, y de financiación

otras plataformas, en este caso de mensajería instantánea, como pueden ser WhatsApp o Telegram.

El informe destaca que estas mafias gestionan todos los trámites para llegar a Europa, desde pasaportes hasta visados, todos ellos falsos, y "enseñan" argumentos si se decide pedir asilo político en un país. Sólo en 2016 se detectaron más de 1.100 perfiles falsos en redes sociales de mafias que llevan personas a Europa.

Ciberterrorismo

El potencial de las redes sociales como herramienta de captación es otra de las grandes preocupaciones de gobiernos de todo el mundo. No en vano, según diferentes informes, Daesh ha sabido utilizar las redes sociales e Internet como herramienta de propaganda, de captación, de formación, y de financiación.

Y para muestra un botón. Los últimos atentados que ha sufrido Europa se realizaron por personas que "fueron captadas, adiestradas y encaminadas" en Internet. Según datos del año pasado, Daesh fue capaz de captar a 35.000 personas en Internet. La organización terrorista disponía de 46.000 cuentas en Twitter, de las que 6.000 cuentas utilizan bots.

Pero los terroristas no sólo utilizan las redes sociales para captar nuevos adeptos. La encriptación que proporcionan los chats de los videojuegos son utilizados tanto para la captación como para la comunicación entre los yihadistas.

Fake News

Otros de los grandes problemas a los que se están enfrentando las redes sociales son las Fake News o noticias falsas. Éstas se están convirtiendo en un quebradero de cabeza para las instituciones europeas, que han visto cómo algunos Gobiernos, como Rusia, han estado detrás de la publicación de este tipo de contenidos en acontecimientos como el Bre-

El 57% de los españoles admite haber creído alguna vez como verdadera la información de una noticia falsa

xit, las elecciones de Estados Unidos o, más recientemente, el desafío independentista de Cataluña.

Europa cree que la intención es influir en la opinión pública y desestabilizar algunos países europeos se están publicando noticias falsas y, por ello, ha puesto en marcha una consulta pública sobre las fake news y la desinformación online, además de que ha creado “un grupo de expertos de alto nivel” integrado por representantes de universidades, plataformas online, medios de comunicación y organizaciones de la sociedad civil.

Y las cifras avalan esta opinión. El 57% de los españoles admite haber creído alguna vez como verdadera la información de una noticia falsa. Ésta es una de las principales conclusiones de un estudio de Ipsos Global Advisor en el que además se asegura que el 62% de la población española afirma que los españoles sólo buscan información en aquellas fuentes que piensan de forma similar a ellos.

Según Vicente Castellanos, director de Public Affairs de IPSOS, “tendemos a tener una percepción errónea de la realidad en la que vivimos, y esto hace más fácil que se difundan noticias falsas sin apenas darnos cuenta. De hecho, a pesar de que creemos tener un alto conocimiento sobre los temas sociales del país, el estudio de Ipsos “Peligros de la Percepción” demuestra que en la mayoría de las ocasiones no es así. Por ejemplo, en general consideramos que el índice de asesinatos en nuestro país sigue igual que en el año 2000, cuando en realidad ha descendido a la mitad”.

Enlaces de interés...

- Cuándo es delito difundir Fake News
- Las amenazas del crimen organizado en Internet
- Amenazas invisibles. La seguridad en el primer semestre de 2018
- La cambiante cara de los ciberataques

Compartir en RRSS

DETECTE MÁS AMENAZAS CON
ANTIVIRUS DE PRÓXIMA GENERACIÓN

Comparando Q1 2018 y Q1 2017, el cliente promedio de SonicWall enfrentó un aumento de...

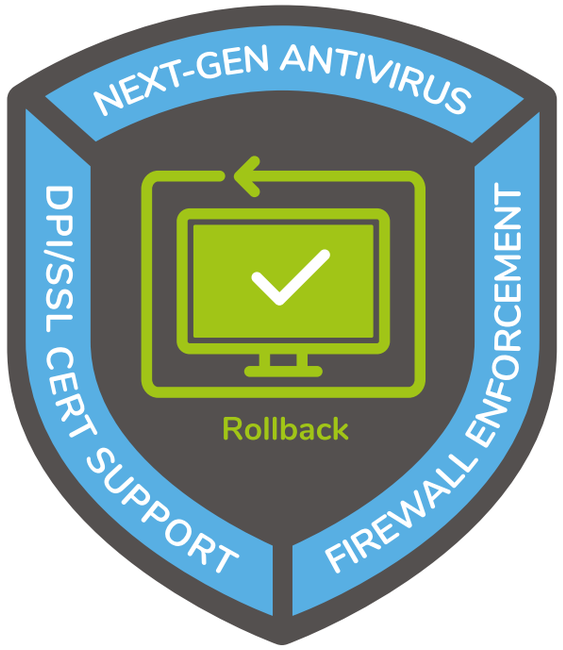
15% en ataques de phishing

400% en ataques encriptados

151% en ataques de malware

226% en ataques de ransomware

CON CAPTURE CLIENT PUEDE



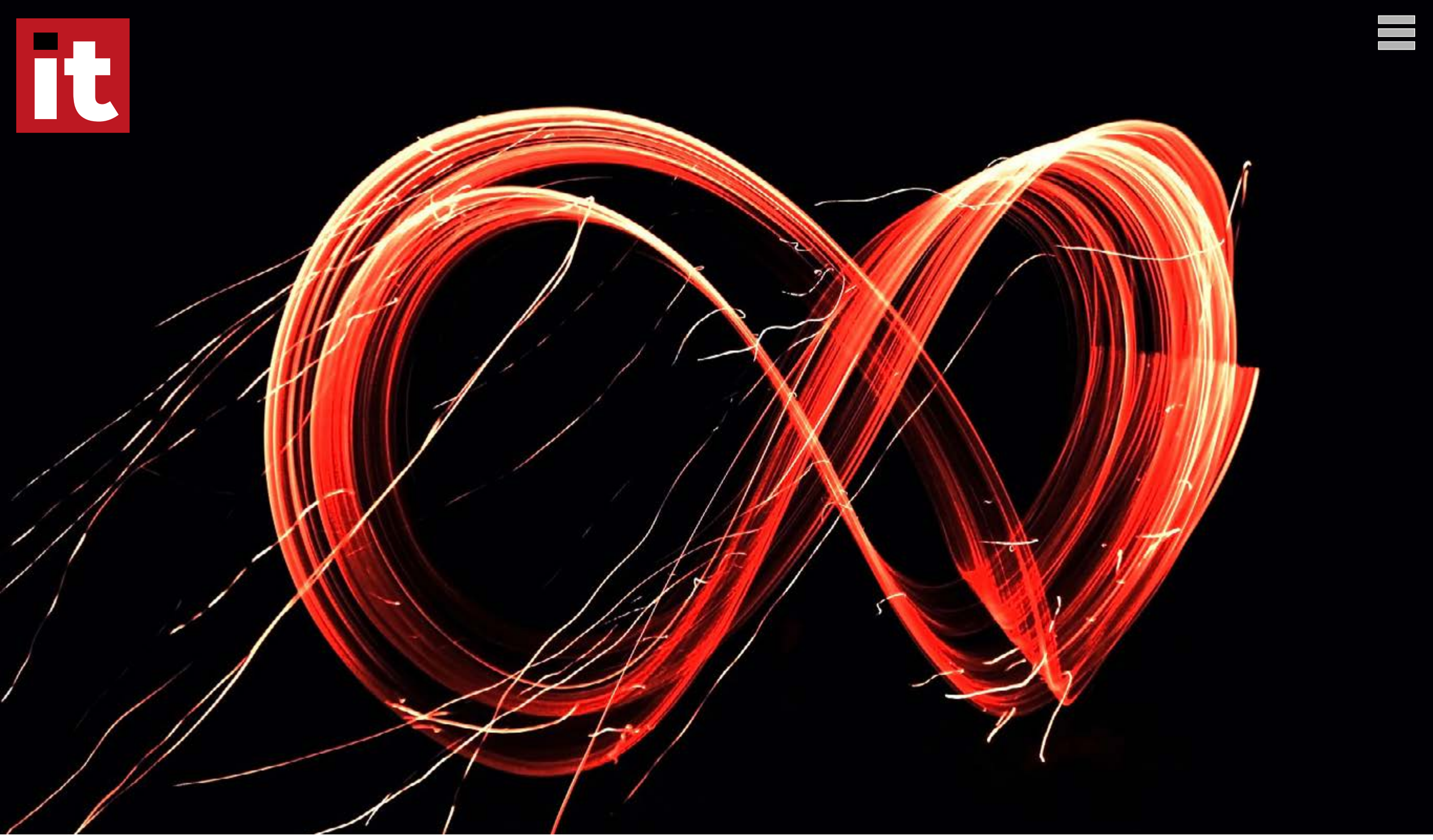
- Controlar continuamente su sistema en busca de comportamiento malicioso
- Hacer rollback de un ataque de ransomware
- Usar el aprendizaje automático para detener los ataques antes de que sucedan
- Sinergizar con los firewalls de SonicWall para protección en capas
- Permitir la inspección del tráfico cifrado por el firewall sin advertencia del navegador

ADEMÁS, CAPTURE CLIENT ESTÁ CERTIFICADO PARA USO CORPORATIVO

Más información en: **SonicWall.com/Capture-Client**

SONICWALL®

spain@SonicWall.com
935 480 400



La Seguridad es Infinity

Check Point
SOFTWARE TECHNOLOGIES LTD.

Noviembre 2018

La Seguridad es Infinity

Coincidiendo con el 25 aniversario de la compañía, Check Point Software Tehcnologies 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.

Check Point cumple 25 años en el mercado. 25 años de evolución de la seguridad, de pasar de una generación a otra, de la primera a la quinta, que es en la que estamos. Una sucesión de ataques y contraataques, de la llegada de los antivirus para hacer frente a los virus que sólo afectaban a los ordenadores; de la de los firewalls para hacer frente a las amenazas que llegaban a través de Internet; de los sistemas de prevención de intrusiones para intentar controlar la seguridad de las aplicaciones; de las tecnologías de sandboxing y antibots para hacer frente a las cargas útiles y los ataques polimórficos… hasta llegar a la actual, a la quinta, en la que los ataques son a gran escala, multiverctoriales y utilizan tecnologías patrocinadas por estados, técnicas en las que el nivel de sofisticación es realmente avanzado.

Hablaba sobre ello Mario García, director general de Check Point para España y Portugal durante el CPX España 2018, un evento celebrado los días 17 y 18 de octubre en El Escorial, coincidiendo con el 25º aniversario de la empresa; un evento que incluyó ponencias, formaciones, laboratorios y sesiones prácticas y que estuvo patrocinado por Aruba, BackBox, Arrow, Tufin, V-Valley y Westcon, y al que acudieron 400 profesionales del sector de la seguridad informática.

La Seguridad es Infinity

CPX ESPAÑA 2018

CLICAR PARA VER EL VÍDEO

Con el apoyo de la arquitectura Infinity, Check Point CloudGuard SaaS proporciona protección contra amenazas de quinta generación para aplicaciones SaaS

Decía Mario García que hay que ser consciente de que hay que proteger la empresa y el entorno y que “tenemos una importante tarea que realizar para hacer frente al futuro de la seguridad”, un futuro marcado por la prevención, que es “la mejor forma de combatir el malware para que no entre”.

Considera Mario García que WannaCry fue una llamada de atención y que estamos llegando a un momento de inflexión, a esa quinta generación de amenazas, de ataques, que llegan por todos lados y están esponsorizados por los estados. ¿Cómo podemos protegernos de ellas? “Con las mejores tecnologías de seguridad, con tecnologías de prevención de amenazas en tiempo real”, decía el directivo. La protección llega a través de Check Point Infinity, una arquitectura de ciberseguridad consolidada en redes, nube y móviles que apuesta por la prevención de amenazas, “una consola centralizada que te avisa si está pasando algo”.

Check Point Infinity busca dar solución a la pérdida del perímetro, esa muralla que rodeaba a la empresas y que ha ido desapareciendo con la llegada de los dispositivos móviles, de las instancias virtuales, de la nube, del IoT… Estos avancen han difuminado ese perímetro, han multiplicado el número de endpoints que hay que proteger, y ha incrementado y potenciado los retos de los responsables de seguridad de las empresas.

Todo el mundo tiene cosas en el cloud, recordaba Mario García durante su ponencia. “No van a dejar de existir las tiendas físicas, ni las infraestructuras físicas, pero el cloud tampoco”, aseguraba el directivo, añadiendo que el cloud va a pasar y está pasando, “y si no tenéis una estrategia de seguridad

Infinity Total Protection, la seguridad a tu alcance por un coste fijo

Para poder sacar partido a la protección Infinity de Check Point, la compañía ha desarrollado Infinity Total Protection, una propuesta que permite a los clientes poder consumir y acceder a todas sus soluciones de seguridad 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.

Este modelo utiliza componentes de la arquitectura Infinity de Check Point, que proporciona elevados niveles de seguridad y, al mismo tiempo, reduce los costes al consolidar los componentes de seguridad.

Todos los sectores empresariales están experimentando ciberataques Gen V, que se caracterizan por ser a gran escala y de rápido movimiento en múltiples industrias. Estos sofisticados ataques dirigidos a dispositivos móviles, la nube y redes empresariales, evitan fácilmente las defensas convencionales y estáticas basadas en la detección que utilizan la mayoría de las organizaciones en la actualidad. Para proteger las redes y los datos contra estos ataques, las organizaciones deben optar por Check Point Infinity, que combina prevención de amenazas en tiempo real, inteligencia compartida y seguridad avanzada en redes, nubes y dispositivos móviles.

cloud debéis planteárosla". Los datos están ahí, la seguridad está creciendo y si en entornos móviles ha crecido un 300%, en entornos cloud el incremento es del 350%.

Check Point Infinity unifica la mejor protección, la mejor inteligencia y la mejor gestión a través de las redes, la nube y los dispositivos móviles, y está diseñada para asegurar que las organizaciones estén preparadas para manejar la dinámica tan cambiante de la TI del futuro. Y es que con Infinity, con la arquitectura de seguridad de la compañía, no sólo se hace frente a las actuales amenazas de seguridad, de la Gen I a la Gen V, sino a las que vengan.

"Los ataques de quinta generación se acaban y llega la VI de la mano del IoT", decía Mario García al tiempo que aclaraba que la estrategia de defensa en IoT y en cloud no es la misma que la del datacenter; "nacen y mueren más rápido, y la seguridad tiene que cambiar de la misma manera. La Gen VI es la generación de la nano seguridad".

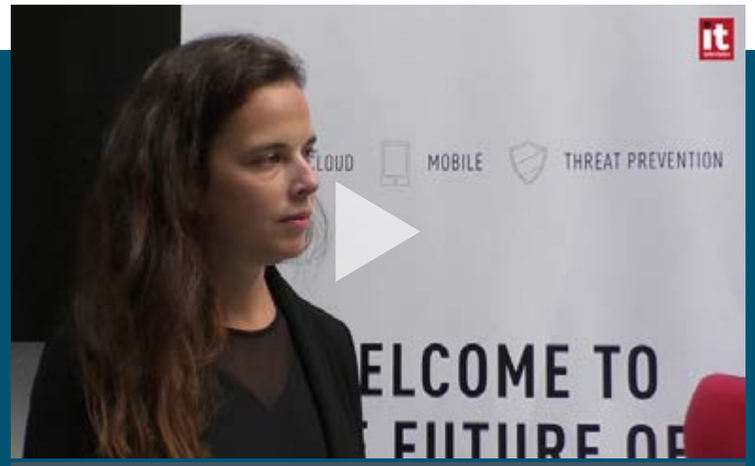
Queda mucho trabajo por hacer para que las empresas estén al día en seguridad, y Check Point propone más Infinity para hacer frente al reto. En este caso se trata de Infinity Total Protection y es "un plan de cómo trabajar con vosotros", un acuerdo que permite a las empresas tener acceso a todas las herramientas de seguridad por un coste fijo por usuario, un acuerdo "tan largo, o tan corto como queráis", que ofrece a los clientes la flexibilidad que necesitan.

Y concluía Mario García su ponencia asegurando: "En Check Point tenemos gente con talento, gente realmente buena. Bienvenidos al futuro de la seguridad".

IA aplicada a la seguridad

Tal Eisner, Product Marketing Manager, participaba en el evento explicando la importancia de la Inteligencia Artificial y su prometedor futuro en la industria de la ciberseguridad.

La Seguridad es Infinity



ENTREVISTA CON MAYA HOROWITZ, THREAT INTELLIGENCE GROUP MANAGER DE CHECK POINT

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON ALBERTO MAESTRE, SOLUTION ARCHITECT DE TUFIN

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON DAVID GARCÍA CANO, CYBER SECURITY SALES MANAGER SOUTHER EUROPE DE ARUBA

CLICAR PARA VER EL VÍDEO

ENTREVISTA CON ALON ROTHCHILD, PRE SALES INGENIEER DE BACKBOX

CLICAR PARA VER EL VÍDEO

Infinity Total Protection es un modelo de consumo que permite a las empresas tener acceso a todas las herramientas de seguridad de Check Point por un coste fijo por usuario

Todo el mundo habla de Inteligencia Artificial, en todas las industrias. Para Stephen Hawking “el desarrollo de una inteligencia artificial completa podría significar el fin de la raza humana”, una opinión muy similar a la de Steve Wozniak, quien asegura que no hay duda de que “los ordenadores van a tomar el relevo a los humanos”, o a la de Vladimir Putin, cuando dice que “los países que lideren la IA serán los que gobiernen el mundo”. Para Elon Musk, la Inteligencia Artificial “será la causa más probable de la tercera guerra mundo”. Tal Eisner prefirió referirse a la Inteligencia Artificial como “la próxima

Check Point Infinity es una arquitectura de seguridad que unifica la mejor protección, la mejor inteligencia y la mejor gestión a través de redes, nube y dispositivos móviles

DA EL SALTO A LA GEN V DE LA CIBERSEGURIDAD

CLICAR PARA VER EL VÍDEO

MARIO GARCÍA, DIRECTOR DE CHECK POINT PARA ESPAÑA Y PORTUGAL

revolución industrial, una revolución en la que los músculos serán sustituidos por el cerero".

La capacidad de almacenar petabytes de información con lo que alimentar el machine learning; la capacidad de cómputo con la que digerir y analizar la información almacenada y la capacidad de enfocarse en los algoritmos matemáticos que extraigan valor es lo que está impulsando la adopción de la Inteligencia Artificial, algo cada vez más presente en nuestras vidas, tanto en previsiones como en soluciones de búsqueda de imágenes o en el reconocimiento del habla a través de asistentes como Siri, Alexa y otras grandes amigas.

Lo decía el directivo de Check Point antes de preguntar si hay magia en la Inteligencia Artificial y enumerar algunos ejemplos de cómo se está aplicando y dejar claro que lo que necesita una buena solución de IA son datos. "Cuando no hay datos y no hay suficiente experiencia se generan veredictos oscuros que afectan a la tasa de detección", decía el Product Marketing Manager de Check Point antes de asegurar que la Inteligencia Artificial está revolucionando la ciberseguridad "porque permite crear procesos mecanizados para detectar malware y amenazas".

Check Point ya ha desarrollado y evolucionado motores basados en IA en su plataforma de prevención de amenazas, consiguiendo mejorar la detección de malware hasta un 600% gracias a ellos. Las herramientas que ha desarrollado son, entre otras, Campaign Hunting, Huntress y Context-Aware Detection (CADET).

Seguridad cloud, Check Point Cloudguard SaaS

El 70% de las empresas están utilizando algún tipo de aplicación en la nube, según datos de Gartner. El gran reto del cloud es cómo proteger los datos que ahora se encuentran en aplicaciones que salen de nuestros control, como puede ser un Office 365, un Salesforce, un Dropbox…

Check Point afronta el reto de securizar este entorno aplicando tecnologías que la compañía ha estado aplicando en el firewall, o en el endpoint, pero ahora aplicado al mundo cloud. Se presta mucha atención al robo de credenciales, identificado como

Grandes amenazas de seguridad móvil

Probablemente WannaCry es el malware más conocido de los últimos tiempos e infectó a menos de un millón de ordenadores y generó un negocio de dos millones de dólares. El mundo móvil es más rentable, aseguraba Francisco Arcia, Threat Prevention Sales Manager Iberia en Check Point, durante la celebración del CPX España 2018.

Durante su ponencia sobre las últimas amenazas se seguridad móvil el experto de Check Point hacía referencia a algunos ejemplos de malware para plataformas móviles. Nombraba a HummingBad, con el que sus creadores llegaron a ganar más de 300.000 dólares al mes tras infectar unos diez millones de dispositivos.

También descubierto por Check Point, CopyCat infectó más de 14 millones de dispositivos Android alrededor del mundo, y generar negocio por valor de más de 16 millones de dólares por anuncios fraudulentos.

Otro ejemplo de malware móvil con pretensiones es Gooligan que generó el mayor robo de credenciales de la historia. El malware comprometió un total de un millón de cuentas de Google que se encuentran en nuestros dispositivos móviles. Según Check Point, Gooligan se encontró en 86 aplicaciones infectadas en varios mercados de aplicaciones de terceros.

Las aplicaciones son un coladero de malware, y si el ejemplo de Gooligan no es suficiente añadía Francisco Arcia el de Dreesscode, un malware que se coló en 40 aplicaciones alojadas en Google Play, un malware que además interactuaba sólo cuando el dispositivo se conectaba a la wifi de la empresa para establecer una comunicación y hacer una copia de todos los datos y ficheros.

SandBlast Mobile es la propuesta de Check Point, una solución que protege los dispositivos de las amenazas en el dispositivo, en las aplicaciones y en la red, para iOS y que se integra con casi todos los MDMs del mercado.

el mayor problema a nivel de aplicación, junto con el malware, pero además se incorpora un motor de DLP porque según Francisco Arcia, Threat Prevention Sales Manager Iberia en Check Point, “otro de los grandes problemas que estamos viendo son las fugas de información. El resultado es Check Point Cloudguard SaaS para aplicar la seguridad sobre múltiples aplicaciones en la nube y con una manera de comercialización por la que el cliente que quiera este tipo de soluciones sólo tiene que saber cuántos clientes quiere proteger y le vamos a dar todas esta tecnología para todas las aplicaciones que quiere proteger.

CloudGuard SaaS utiliza la tecnología ID-Guard para identificar el acceso de usuarios ilegítimos y evitar que los usuarios no autorizados accedan a las aplicaciones SaaS. Además, CloudGuard SaaS permite crear políticas coherentes entre dispositivos móviles, PC e incluso gateways, y una monitorización de seguridad unificada que se aplica en forma generalizada.

Check Point Cloudguard SaaS incorpora diferentes tecnologías, como de la sandboxing, Threat Extraction, motores antiphishing y DLP, protección de identidad, etc., y todo ello basado en una consola cloud sin coste adicional para los clientes y fácil de utilizar, con integración vía API con todas las aplicaciones.

“Para evitar el robo de credenciales hemos hecho algo único”, decía Francisco Arcia: poder validar que un usuario se está conectando desde un dispositivo verificado y seguro. “Podemos combinar dispositivos, nivel de riesgo, usuarios y en muchos casos geolocalización”, decía Arcia.

Check Point está en el móvil, está en las redes, en el cloud, en el puesto de trabajo, y eso significa que, si un usuario accede a una página que se califica como maliciosa, esa información pasa a formar

La Seguridad es Infinity

Ponencias CPX España 2018

TAL EISNER, PRODUCT MARKETING MANAGER DE CKECK POINT

IS AI THE SILVER BULLET IN CYBER SECURITY?

CLICAR PARA VER EL VÍDEO

MAYA HORROWITZ, THREAT INTELLIGENCE GROUP DE CHECK POINT

CYBER ACADEMY AWARDS 2017 – LEADING TRENDS IN THE THEATS LANSDCAPE

CLICAR PARA VER EL VÍDEO

DAVID GARCÍA CANO CYBER SECURITY SALES MANAGER SOUTHENR EUROPE DE ARUBA

CYBERTALK: PROTÉGETE DE LAS AMENAZAS INTERNAS CON ARUBA SECURITY Y CHECK POINT

CLICAR PARA VER EL VÍDEO

EUSEBIO NIEVA, DIRECTOR TÉCNICO DE CHECK POINT ESPAÑA Y PORTUGAL

LA NUEVA ARQUITECTURA DE SEGURIDAD CONSOLIDADA: INFINITY

CLICAR PARA VER EL VÍDEO

ALON ROTHCHILD, PRE SALES INGENIEER DE BACKBOX

CYBERTALK: INTELLIGENCE AUTOMATION FOR SECURITY OPERATIONS

CLICAR PARA VER EL VÍDEO

JAVIER HIJAS, CHECK POINT; MARIOLA DE LOPE, MICROSOFT Y VICENTE PÉREZ, VMWARE

TECNOLOGÍA CLOUD EN ESPAÑA, RETOS Y OPORTUNIDADES DE SEGURIDAD

CLICAR PARA VER EL VÍDEO

parte de una base de datos que comparten todos los productos de la compañía. “Por lo tanto para ser buenos en seguridad no sólo basta con tener buenos productos, sino también tener información, y gracias a ese enfoque que nosotros llamamos Infinity hoy en día tenemos los mejores datos”, decía Francisco Arcia.

De forma que con el apoyo de la arquitectura Infinity de Check Point, CloudGuard SaaS proporciona protección contra amenazas de quinta generación para aplicaciones SaaS, desde dondequiera que se acceda, a través de un solo panel.

Seguridad móvil, Check Point SandBlast

Más de la mitad del tráfico de internet está generado por dispositivos móviles. Ya en 2014 había más suscripciones a líneas móviles que a personas a nivel mundial. Cada día se envían por 65.000 millones de mensajes por WhatsApp. Está claro que el mundo es móvil y que las empresas empiezan a tomar medidas: en Estados Unidos el 50% de las compañías ya adoptaron el BYOD, han permitido a los empleados que utilicen sus móviles en los entornos laborales, y esta cifra se duplicará el próximo años. Para Francisco Arcia, Threat Prevention Sales Manager Iberia en Check Point, es ahí donde está el reto, no sólo en proteger el móvil

La Seguridad es Infinity

Ponencias CPX España 2018

ALBERTO MAESTRE, SOLUTION ARCHITECT DE TUFIN

CYBERTALK: INCREMENTAR LA AGILIDAD DE NEGOCIO, REDUCIR COSTES Y RIESGOS CON LA AUTOMATIZACIÓN — CLICAR PARA VER EL VÍDEO

ESTIBALIZ EGUIDAZU UGALDEA, BETSAIDE E IÑIGO VALLEJO, NEXTEL

BETSAIDE: UN CASO REAL DE TRANSFORMACIÓN EN ENTORNO INDUSTRIAL — CLICAR PARA VER EL VÍDEO

FRANCISCO ARCIA, THREAT PREVENTION SALES MANAGER IBERIA EN CHECK POINT

ÚLTIMAS AMENAZAS DE SEGURIDAD MÓVIL — CLICAR PARA VER EL VÍDEO

ANTONIO DELGADO, SENIOR SOLUTIONS ARCHITECT EN AWS

CYBERTALK AWS: AUTOMATION IS THE NEW BLACK, X BY ORANGE — CLICAR PARA VER EL VÍDEO

JAVIER CASTILLO, IP/SDN ARCHITECT EN X BY ORANGE

CYBERTALK ORANGE: AUTOMATION IS THE NEW BLACK, X BY ORANGE — CLICAR PARA VER EL VÍDEO

FRANCISCO ARCIA, THREAT PREVENTION SALES MANAGER IBERIA EN CHECK POINT

SECURIZANDO LAS APLICACIONES SAAS: UNA APROXIMACIÓN PRAGMÁTICA — CLICAR PARA VER EL VÍDEO

que te da la empresa sino de cómo hacer que el móvil personal, con el que muchas veces se accede a los recursos de la empresa, tenga la seguridad adecuada.

Decía el directivo durante el CPX España 2018 que seguimos pensando que es más importante proteger un portátil que un móvil, pero que este último es un vector que cada vez está siendo más atacado. “WannaCry no llegó a infectar más de un millón de portátiles y sin embargo todo el mundo lo conoce, mientras en el mundo móvil estamos viendo muestras de malware para móvil que han llegado a infectar 14 millones de terminales, como CopyCat”.

Estamos tan enfocados en proteger las redes, el endpoint, el cloud… que nos dejamos cosas tan importantes como es la seguridad en el móvil. Una solución antivirus no es suficiente porque ha de tenerse en cuenta la conexión a redes inalámbricas abiertas y la complicación que supone el poder comprobar que esa red pueda estar haciendo un ataque man in the middle. “Con SandBlast Mobile nuestro objetivo es entender qué está ocurriendo a nivel de conectividad en ese móvil, a nivel de wifi, a nivel de bluetooth, a nivel de aplicaciones”, aseguraba Francisco Acacia.

Check Point lleva trabajando más de tres años en un producto que se llama Sandblast Mobi-

le, donde tenemos módulos que protegen estos vectores. Vamos a ver conexiones, aplicaciones, qué hay en ese mensaje de WhatsApp. Bluetooth, WiFi, SMS… es una aplicación que tiene muy poco impacto en el dispositivo, tanto en el consumo de batería como de ancho de banda y que se integra con casi todos los MDMs del mercado

Los principales beneficios de esta solución son la posibilidad de detectar, evaluar y mitigar amenazas avanzadas de ciberseguridad para móviles; proteger los datos empresariales confidenciales en reposo, en uso y en tránsito en dispositivos móviles iOS y Android de ataques cibernéticos; mejorar la visibilidad y la protección mediante la integración con los sistemas existentes de movilidad y ciberseguridad (MDM, MAM, NAC, SIEM...); habilitar la respuesta rápida a ataques de amenazas persistentes avanzadas (APT) entre plataformas; preservar la experiencia del usuario y la privacidad, a la vez que añade la protección requerida por los mandatos organizacionales o regulatorios.

Enlaces de interés...

- Check Point Infinitve
- Check Point SandBlast
- Check Mates
- Check Point CloudGuard SaaS
- Check Point Seguridad Cloud

BE SURE TO BE FREE

BLINDA TUS "SUPERCONFIDENCIAL"

#BlindaTuLibertad

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

www.eset.es

ESET

ENJOY SAFER TECHNOLOGY™

Seguridad para entornos financieros, ¿dónde está el reto?

Los cibercriminales ponen sus miras en el sector financiero porque ahí es donde está el dinero. El interés no ha cambiado con los años, pero sí la velocidad y las consecuencias, que han aumentado. Las empresas deben mantener un equilibrio entre el estar abiertas a los clientes y ofrecer una experiencia satisfactoria con el mantenerse seguras. A medida que aumentan los ataques y las regulaciones se refuerzan la presión aumenta. Saber reconocer que los ciberdelincuentes actuarán, que encontrarán vulnerabilidades e intentarán explotarlas permite a los responsables mejorar la forma en que diseñan y prestan servicios, administran los riesgos y capacitar a sus equipos.

Los incidentes de fraude se incrementaron más de un 130% el pasado año, lo que no sólo generó pérdidas económicas, sino de reputación a las instituciones financieras. No hay que olvidarse de las ciber extorsiones, del ransomware, de Petya y Wannacry, que hacen que la defensa se complique.

Para hablar de los retos de la seguridad en entornos financieros IT Digital Security ha reunido un grupo de expertos en uno de sus #DesayunosITDS. Participaron Luis Frisas, Director para el Sur de Europa de SonicWall; Javier Múgica, Mayor Account Manager Bank, Insurance and Retail de F5 Networks; Vicente Martín, Director Preventa de Panda

Compartir en RRSS

Regulaciones como PSD2, obligan a los bancos a permitir que se acceda a sus datos a través de APIs, lo que les obliga a cierto nivel de exposición

Security; Alberto Ruiz, Presales Engineers Sophos España y Portugal y Miquel Morell, Consultor de Omega Peripherals.

Aunque la banca está más avanzada que otros sectores en lo que a adopción de medidas de seguridad se refiere, “sufren todos los problemas que sufren los demás”, dice Luis Frisas, de SonicWall. Y es que, como el resto de la industria, la banca y los servicios financieros afronta la transformación digital y un aumento de los riesgos de seguridad. El directivo repite una vieja premisa del mercado: hay dos grupos de empresas, las que han sido atacados y las que lo serán, “y los bancos están todos en el primer grupo”.

Añade Javier Múgica, de F5 Networks, que los bancos están abordando una gran transformación en la manera en que ellos interactúan con los clientes, incluido el uso de nuevas aplicaciones y cómo hacen el delivery de las misma; “aunque son bastante avanzados en algunas cosas, tienen los mismos problemas que tiene otros, los mismos ataques, y son muy golosos. Y por eso tiene un reto muy importante”.

Quizá el reto de la banca y los servicios financieros es que son, en opinión de Vicente Martín, de Panda Security, “el centro de la diana de cualquier atacante”, y que probablemente “reciben ataque más dirigidos y más sofisticados que el resto de sectores”. Para Alberto Ruiz, de Sophos, dentro de este segmento de mercado hay dos vertientes, bancos en los que la seguridad se toma muy en serio, y otros en los que incluso no se ven consideran posibles objetivos de un ataque.

Añade Miquel Morell que lo que tiene la banca con muchas regulaciones. La PSD2, por ejemplo, les obliga a exponerse al tener que permitir que se acceda a sus datos a través de APIs para que puedan existir aplicaciones capaces de conectar a varios bancos, “y eso es un enorme agujero. Son regulaciones que les obligan a estar en un cierto nivel de exposición”.

SEGURIDAD PARA ENTORNOS FINANCIEROS, ¿DÓNDE ESTÁ EL RETO? **CLICAR PARA VER EL VÍDEO**

Explica además Javier Múgica que hace un año su compañía estudió lo que dice la legislación española sobre que un cliente tenga un virus en su PC, le roben información y puedan sacar dinero de su cuenta. ¿Qué puede ocurrir en este caso? Pues que según la jurisprudencia en España el responsable es el banco, “que no ha puesto todos los medios para impedir ese ataque”, explica Mújica. Y es que las entidades financieras no sólo deben tener cuidado de las actividades de los empleados, sino de los clientes, que operan desde casa, desde el móvil, desde un cajero, en

lo que Luis Fisas define como “un entorno complejo, difícil, regulado y con multitud de ataques”.

Amenazas online y continuidad

Para el responsable del negocio de banca de F5 Networks, para la banca es cada vez más crítico que no se caigan los aplicativos, que los clientes tengan acceso a los datos a través de aplicaciones que se están desarrollando de manera constante en un proceso de DevOps y que están situadas en un entorno híbrido. Se añade el reto, o amenaza de tener que exponer sus datos a empresas externas (PSD2), lo que les obliga a abrir al mundo exterior sus datos, “y eso requiere de medidas de seguridad adicionales”.

Vicente Martín, de Panda, está de acuerdo en que colocar a las aplicaciones como un vector de ataque, y añade al empleado, capaz de desencadenar un ataque interno, y que el tipo de ataques que recibe la banca son ataques más dirigidos, más avanzados. “El usuario no ha recibido actualización y está totalmente a merced del click”, añade Alberto Ruiz, que habla de explosión de vulnerabilidades y de phishing como algunas de las amenazas online a los que la banca, y en general la industria, está expuesta.

La tecnología de doble autenticación añade una capa de seguridad en los procesos de banca, pero se acaban de detectar una aplicaciones para móvil que acaban con ellas, explica Miquel Morell, de Omega Peripherals. “Te entran en el móvil, se quedan con tus credenciales y además interceptan el SMS que te envía el banco”, dice preguntándose cuál es el siguiente paso; ¿triple autenticación?, no, responde, quizá el siguiente paso sea la autenticación con dos dispositivos.

Siendo la banca un sector de servicios, la continuidad de los mismos es fundamental, y por tanto los planes de disaster recovery también. No son planteamientos nuevos, ni se establecen únicamente porque el desastre lo haya generado un ciberataque, ya que se pueden producir de manera natural, como un incendio, o una inundación. Preguntamos a nuestros expertos si la banca y los servicios financieros están más avanzados en la adopción de estos programas de continuidad.

“Decir que son perfectos sería mentir”, dice el director preventa de Panda Security, añadiendo que ese campo [disaster recovery] dentro de la seguridad es el que más tienen que evolucionar. “Tienes que ser capaz de sobreponerte a un ataque, la capacidad de rehacerte ante un ataque, porque el ataque va a llegar”, añade Vicente Martín.

Alberto Ruiz dice que hay bancos muy bien preparados y otros menos, e introduce el concepto EDR (Endpoint Disaster Recovery), que las empresas de

"Hay dos aspectos de GDPR que han tenido un gran impacto en la banca: uno es la gestión de las autorizaciones, que antes era única, y otra es el derecho al olvido"

Vicente Martín, Director Preventa de Panda

Frente a grandes retos, grandes soluciones

Como es habitual, al finalizar el debate pedimos a nuestros experto que expongan sus propuestas, en esta ocasión para securizar los entornos financieros

Luis Fisas, SonicWall. Desde SonicWall proponemos la defensa en profundidad y multicapa defendiendo en este caso el perímetro de la banca, que es una nube híbrida, con aplicaciones web, y por tanto hay que ofrecer un WAF, aplicaciones virtuales, firewalls físicos, hay que hacer inspección de paquetes físicos y en profundidad... Nosotros tenemos un gran surtido de productos y se servicios para poder ofrecerle al banco desde la seguridad endpoint hasta la del centro de datos. La banca tiene un entorno complejo y grandes retos, y les ofrecemos un tipo de servicio o producto que, evidentemente, hay que aplicar correctamente.

Javier Mújica, F5 Networks. Nuestra propuesta para la banca es ofrecer soluciones que permiten proteger las aplicaciones, proteger incluso al usuario que accede a esas aplicaciones, realizando chequeos en el equipo del cliente de forma transparente con la ventaja de no tener que tocar las aplicaciones que tenemos detrás porque somos un elemento intermedio que tenemos la capacidad y agilidad para poder hacer muchos cambios. Y nos dedicamos a la seguridad en las aplicaciones con servicios de seguridad en la nube, sea pública o privada. Y de gran relevancia en el mercado, sobre todo en el de banca, es la capacidad de descifrar el tráfico para poder enviarlo a otros elemento de seguridad.

Vicente Martín, Panda Security. A nosotros siempre se nos ha conocido como una empresa de antivirus tradicional, pero hemos evolucionado mucho. Basamos nuestra protección del puesto en la inspección del 100% de los procesos que corren en él. Estamos explotando toda esa información que extraemos de los procesos en los equipos para hacer labores de threat hunting, de perfilado de máquinas... y otra serie de labores que nos permite ver qué está pasando dentro de los equipos, si su funcionamiento es correcto o si ya tenemos un ataque dentro de la red. La banca está interesada en esas labores de threat hunting que están funcionando realmente bien dentro de los clientes que la están probando porque está detectando cosas que de otra manera no podrían detectar.

Alberto Ruiz, Sophos. Seguimos apostando por la seguridad sincronizada que iniciamos hace tres años, donde ese mundo del perímetro, del endpoint, de las pasarelas de correo está sincronizado de forma que si el perímetro detecta un ataque IPS que no ha sido detectado en el puesto de trabajo, automáticamente habla con todos los usuarios para aislar el problema, de forma que un móvil que no cumple la normativa ya no se puede conectar, un usuario que recibe un ataque vía correo electrónico es rápidamente aislado, a pesar de lo cual se le pueden seguir dando la misma protección.

Miquel Morell, Omega Peripherals. No somos un fabricante y nuestro enfoque es la capacidad que tenemos de proveer soluciones en diferentes aspectos. Omega Peripherals viene del mundo de la infraestructura, nos metimos en el mundo de los servicios y ahora estamos reforzando la parte de la seguridad. Lo que sí que tenemos es gente conocedora de todos los aspecto, de forma que podemos atacar la seguridad desde diferentes aspectos, como es proponer la virtualización del escritorio para mejorar la seguridad del endpoint. Creo que tenemos una capacidad de atacar problemas multidisciplinar. Probablemente esa sea nuestra baza, el aprovechar estas tecnologías tan estupendas que nos han estado contando e integrarlas con los conocimientos que tenemos de infraestructuras y toda la capa de servicios que podemos dar.

seguridad endpoint están adoptando desde los últimos años y que permite, una vez se ha sido atacado, poder hacer la investigación del ataque. En todo caso lo mejor es que el ataque no haya tenido éxito, “hay que poner el foco en medidas para evitar que esto no ocurra”.

Miquel Morell utiliza su experiencia en el mundo de las infraestructuras para poner sobre la mesa un problema que se está generando con la consolidación de empresas en el mundo financiero. “La banca se está fusionando a nivel de diferentes países, y en ocasiones parece que es políticamente correcto poner el disaster recovery lejos. Y el problema de ponerlo lejos, es que la tecnología no te permite replicar las cosas tan rápido; se aumenta hueco que tienes entre el último dato bueno y el último dato que puedes recuperar. Y cuanto más lejos, más grande es el hueco”. Las alianzas o fusiones están modificando las políticas de disaster recovery, insiste Morrel y “generan problemas tecnológicos que hay que resolver y no son difíciles de atacar”.

"El problema de que el disaster recovery esté lejos es que la tecnología no te permite replicar las cosas tan rápido y se aumenta el hueco entre el último dato bueno y el último dato que puedes recuperar"

Miquel Morell,
Consultor de Omega Peripherals

“SonicWall es una empresa de prevención y cuando se habla del Disaster Recovery Plan es que ya significa que ya ha habido un desastre, que hemos llegado tarde”, dice Luis Fisas, añadiendo que siendo evidente que hay que tener un plan de contingencia, hay que tomar medidas de prevención que deben ser multicapa. “Ser CISO de un banco hoy en día es estresante”, asegura el director de SonicWall para el sur de Europa.

Dedicándose a la disponibilidad de las aplicaciones, en F5 Netwoks tienen claro que es complicado que el plan de continuidad avance al mismo ritmo que el ecosistema de aplicaciones y servicios que tiene un banco. “El hecho de tener dos CPDs no es garantía de que vayas a estar seguro ante un desastre. No creo que ninguna empresa pueda sentirse tranquila cuando tenga que disparar un mecanismo de disaster recovery”, dice Javier Mújica.

La banca española tuvo que empezar a funcionar con las tarjetas de crédito mucho antes que en

Es de vital importancia desarrollar soluciones de seguridad que puedan trabajar con ATMs que la solución de seguridad no merme su productividad"

Alberto Ruiz,
Presales Engineers Sophos Iberia

otros países, y ese avance, dice Morell, y eso hace que esté más evolucionado en otros aspectos.

Seguridad endpoint, del PC al TPV

Perdido el perímetro, el endpoint recobra importancia en la estrategia de seguridad. En el caso del sector bancario, ¿cómo ha afrontado este cambio? ¿ordenadores obsoletos? ¿políticas de BYOD? ¿y qué pasa con las ATMs? Sore las ATMS, o los cajeros automáticos, dice Alberto Rodas que muchas veces utilizan sistemas operativos antiguos, muchas veces sin soporte y con pocos recursos, por lo que es de vital importancia "desarrollar soluciones de seguridad que puedan trabajar en esos sistemas. Que la solución de seguridad no implique que no pueda hacer el negocio para el que está pensado". Se trata de soluciones capaces de hacer frente a amenazas conocidas o exploits nuevos pero sin merma en su productividad.

Introduce Miquel Morell en la ecuación de seguridad del endpoint la virtualización, "porque en el momento en que los virtualices los vuelves a colocar detrás del perímetro". Y explica el consultor de Omega Peripherals que inicialmente la banca, y todo el mundo, "se planteó el tema de la virtualización como un ahorro de costes, pero ahora se está viendo como una manera de meter de nuevo el puesto de trabajo dentro del perímetro de seguridad".

Dice Luis Fisas que el perímetro es muy complejo y que tiene que haber políticas que lo gestionen. Habla de un banco que sustituyó todos los iPhones por terminales Android con una capa de seguridad. "Proteger el endpoint es importantísimo", dice el directivo, añadiendo que SonicWall cuenta con soluciones de protección del endpoint que utilizan técnicas de Deep learning e IA "porque los malos seguirán evolucionando".

Javier Mújica añade otro término a la ecuación: la protección del usuario que accede al servicio; "la capacidad de inspeccionar el dispositivo con el que se conecta el cliente es muy interesante desde el punto de vista del dueño del dato, que es el banco. Es críti-

"La capacidad de inspeccionar el dispositivo con el que se conecta el cliente es muy interesante desde el punto de vista del dueño del dato, que es el banco"

Javier Mújica, Mayor Account Bank, Insurance and Retail de F5 Networks

co porque es un punto de entrada". Es la dualidad de tener que protegerte a ti y también a los clientes.

Vicente. Somos especialista en la parte de endpoint y nos basamos en deep learning, machine learning, EDR… es el discurso ahora mismo.

"La banca no sólo necesita la protección del puesto sino algo más", dice Vicente Martín, explicando a continuación que la estrategia de Panda Security se basa en la monitorización de todo lo que ocurre en todos los equipos, y ser capaces de proveer otras funcionalidades, incluso de threat hunting.

GDPR y el mundo financiero

De obligado cumplimiento desde el pasado mes de mayo, el reglamento europeo de protección de datos, o GDPR, debe ponerse sobre la mesa. ¿Ha sido un dolor de cabeza para los responsables de servicios financieros? Miquel Morell tiene claro que GDPR "no la ha digerido nadie" y que es una normativa "pensada para el norte de Europa". Añade que estamos acostumbrados a la LOPD, que te decía lo que tenías que hacer, "frente a un reglamento que te dice que tu obligación es hacer las cosas bien, que has de considerar la seguridad desde el diseño de tus aplicaciones empresariales". GDPR concluye Morell, "es una manera muy diferente de afrontar las cosas".

Para Luis Fisas "la UE ha hecho muy bien en trasladar la responsabilidad a las empresas". Recuerda

AUTENTICACIÓN BIOMÉTRICA EN LA BANCA MÓVIL

Para realizar pagos seguros a través de teléfonos móviles se deben utilizar nuevos métodos de autenticación segura. La Biometría se considera como una de las autenticaciones más eficaces para todos. El documento recoge una encuesta sobre sobre varios parámetros biométricos y en especial el uso de la huella digital.

El uso de un método de autenticación biométrica en la banca móvil reduce diversas actividades fraudulentas, lo que a su vez aumenta la seguridad y proporciona al usuario transacciones seguras y confiables.


International Journal of Innovative Research in Computer and Communication Engineering

Survey on Biometric Authentication in Mobile Banking

"Como el resto de la industria, la banca y los servicios financieros afrontan la transformación digital con un aumento de los riesgos de seguridad"

Luis Fisas, Director para el Sur de Europa de SonicWall

el directivo que en España teníamos la LOPD cuando el resto no tenía nada, y que el 80% de nuestra LOPD es GDPR, "de forma que quien estaba al día con la ley española ha hecho ya mucho".

Para Javier Mújica GDPR "realmente no ha cambiado tanto en el entorno bancario porque ya eran muy celosos de los datos. Lo que realmente ha cambiado son las sanciones", y como el impacto está en las aplicaciones que permiten el acceso a esos datos, son las aplicaciones lo que hay que proteger, por lo que la demanda de WAF (Web Application Firewalls) está creciendo.

"De puertas afuera todos están preparados, de puertas adentro empiezan a provisionar las multas," dice Vicente Martin, director Preventa de Panda Security, quien añade que hay dos aspectos de GDPR que han tenido un gran impacto: uno es la gestión de las autorizaciones, que antes era única, y otra es el derecho al olvido.

Alberto Ruiz, ingeniero preventa de Sophos Iberia menciona otro cambio que introduce GDPR: hace que las empresas tengan sistemas para educar a los usuarios, que siguen siendo ese eslabón débil capaz de desencadenar el desastre.

Enlaces de interés...

- La banca ante el reto de la ciberseguridad. ¿Es posible mantener la seguridad?
- Banca, industria y sector público, los que más invertirán en seguridad en los próximos años
- Los troyanos de banca móvil, en su máximo histórico
- Chief Regulatory Officer, la nueva figura que será crítica para la banca, ¿por qué?
- Consejos de ciberdefensa para la banca
- Principales amenazas de seguridad para el sector bancario

#ITWebinars

it Digital Security

Seguridad efectiva y escalable para blindar tu empresa

➔ Proteger el datacenter, y también las aplicaciones, los datos, las redes, el email… y hacerlo desde diferentes enfoques, con distintas soluciones.

➔ Proteger a la empresa capa a capa, empezando por el servidor, analizando el tráfico en busca de ese bit cifrado y maligno, enviar a la sandbox lo sospechoso, reducido al mínimo gracias a una correcta cuota de machine learning, hasta llegar al endpoint, esté donde esté, fuera, o dentro del perímetro, conectándose a redes de naturaleza muy diversa.

➔ Se hace frente a la amenaza con seguridad proactiva, con simulación de ataques, con cebos y trampas que lleven al ciberdelincuente a desvelar sus intenciones mientras preparamos la respuesta.

➔ Protección de extremo a extremo y por capas, pero efectiva, práctica y escalable.

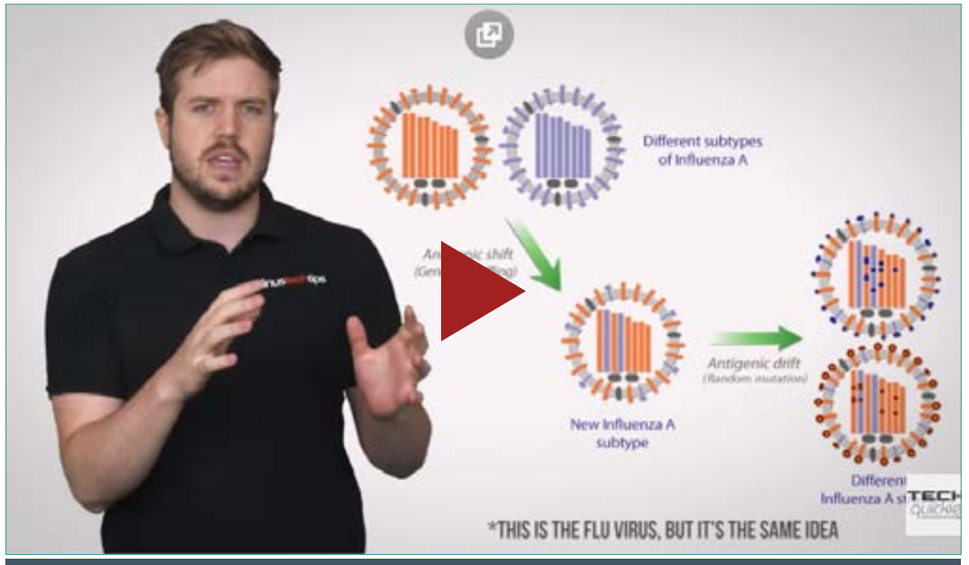
13 NOVIEMBRE 10.00 h.

Registro

Malware evasivo o cómo camuflarse

Para evitar ser detectado, el malware evasivo se camufla, se anexa a aplicaciones legítimas o hace un uso ilegítimo de ellas. La capacidad de los atacantes para evitar ser detectados no es tan simple como parece cuando los expertos en seguridad, los sistemas de inteligencia artificial y los proveedores de software de protección endpoint de todo un mundo se enfocan en hacer precisamente eso, pero la evolución es constante y este tipo de malware reconoce cuando está siendo analizado en un entorno aislado y retrasa su ejecución, pudiendo esperar días, semanas o incluso meses hasta encontrar la oportunidad adecuada para atacar.

Noviembre 2018



¿CUÁL ES LA DIFERENCIA ENTRE VIRUS Y MALWARE

CLICAR PARA VER EL VÍDEO

Malware es un término muy amplio para hacer referencia a la variedad de programas maliciosos que nos hacen la vida un poco más complicada. Adware, spyware, troyanos, virus o gusanos quizá sean los tipos de malware más comunes, pero no son los únicos. La concepción teórica del malware data de 1949, concretamente de la mente de John von Neumann, un matemático húngaro nacionalizado estadounidense que realizó contribuciones fundamentales en física cuántica, análisis funcional, teoría de conjuntos, teoría de juegos, ciencias de la computación, economía, análisis numérico, cibernética…, además de la "Theory and Organization of Complicated Automata", que postula cómo un programa informático podría reproducirse a sí mismo. Parece ser, sin embargo, que los detalles de la implementación técnica no eran concebibles en este momento.

Fue la semilla para que en la década de los 50 empleados de Bell Labs crearan un juego llamado Core Wars, en el que los programadores soltaban "organismos" de software que competían por sobrevivir en el área de la memoria. Algunas versiones podían copiarse a sí mismos y es aquí donde parece que se encuentran las raíces de los virus informáticos.

> El volumen de malware se ha multiplicado por siete en los últimos cinco años, según datos de AV-test, que cada día detecta 350.000 muestras nuevas de malware

Seguimos buceando en Internet para descubrir que el término "virus informático" fue empleado por primer vez por el Profesor Leonard M. Adleman en una conversación con Fred Cohen, considerado como el padre de los virus que definió como: "un programa que puede infectar otros programas modificándose para incluir una versión de sí mismo, posiblemente evolucionada.

No fue hasta primeros de los años '70 cuando aparecen los primeros virus documentados. El primero atacó una máquina IBM Serie 360, se llamaba Creeper, y fue creado en 1972 por Robert Thomas Morris; este programa accedió a ARPANET, se copiaba a sí mismo en sistemas remotos, donde mostraba un mensaje en pantalla: "I'm the Creeper catch me if you can!".

A partir de ese momento fue un no parar: Wabbit, Elk Cloner, Brain Boot Sector Virus, Morris, Melissa son algunos ejemplos de virus conocidos nacidos antes de 2000. Entre este año, el de I Love You, y el año 2010, el malware creció de manera significativa, tanto en número como en sofisticación. Aparecieron los primeros toolkits al alcance de casi cualquiera que quisiera experimentar y

"Para que un malware pueda considerase evasivo debe llevar incorporadas una serie de rutinas orientadas a modificar u ocultar su comportamiento"

Dani Creus, analista de seguridad de Kaspersky Lab

conforme avanzaban los años, el malware también lo hacía.

Las limitadas máquinas de hace un par de décadas, las que se arrancaban con ayuda de un floppy disk, se han convertido en potentes sistemas capaces de enviar enormes volúmenes de datos de manera casi instantánea, enviar correos electrónicos a cientos o miles direcciones de internet, a entretener con películas, música o juegos. Y la evolución de los virus, del malware, ha ido a la par de la evolución de esos sistemas.

De hecho, el mercado del malware, del software malicioso, se ha convertido en un gran negocio. Hace años que superó al negocio de la droga y también hace años que se ha convertido en un arma de espionaje de los estados.

El volumen de malware se ha multiplicado por siete en los últimos cinco años, según datos de AV-test, que cada día detecta 350.000 muestras nuevas de malware.

Malware Evasivo

Hay numerosos tipo de malware. Hemos mencionado al comienzo al adware, spyware, troyanos, virus y los gusanos, pero la lista es más larga y en ella hay que incluir al temido ransomware, a los rootkits, backdoors o keyloggers. Un estudio de Verizon asegura que en el 50% de las brechas de seguridad sufridas hay involucrado algún tipo de malware. Y menciona empresas de la talla de Target o Home Depot, empresas de gran tamaño, con equipos de seguridad y presupuesto de seguridad dedicado. Es seguro que cuenten con soluciones antimalware y que se hayan tenido que enfrentar con el denominado malware evasivo, un tipo de malware desarrollado para evadir las defensas antimalware tradicionales. Muy atrás quedaron los tiempos de los binarios ejecutables estáticos que se comunicaban con un servidor de comando y control (C&C) fijo a través de comunicaciones de texto sin formato. Los malwares de hoy son sofisticadas herramientas de ataque que incluyen una variedad de técnicas de evasión diseñadas para engañar, eludir y evitar las defensas antimalware existentes.

Más del 98% del malware que llega a la matriz de una sandbox utiliza al menos una táctica evasiva, y un 32% acumular seis o más, según un estudio de Cyren.

Descubrimos que más del 98 por ciento del malware que llega a la matriz de sandbox usa al menos una táctica evasiva, y que el 32 por ciento de las muestras de malware que llegan a esta etapa fue lo que podríamos clasificar como “hiper evasivo”, acumulando seis o más. Técnicas de detección de evasión.

Los malware sencillos tienen sus días contados porque los motores antivirus (AV) han pasado de ser basados en firmas a usar motores de detección basados en heurística y comportamiento, y ahora incluso incluyen aprendizaje automático e Inteligencia Artificial. En la práctica esto significa que la

"El malware evasivo se combate con soluciones de seguridad multicapa que sean capaces de identificar una amenaza en alguna de las diferentes fases por las que pasa cuando intenta infectar a su víctima"

Josep Albors, Responsable de investigación y concienciación de ESET España

mayoría de los programas maliciosos que siguen el patrón "convencional" serán capturados. A diferencia del malware normal que simplemente se ejecuta y espera lo mejor, el malware evasivo se oculta y observa para asegurarse de no ser visto hasta el momento del ataque, algo que realiza con sigilo.

Antes de iniciar ninguna actividad el Malware Evasivo comprueba si se está ejecutando en una máquina virtual, lo que podría indicar que se encuentra en una sandbox, o entorno aislado; el siguiente paso es ver si se están ejecutando las herramientas de AV o de seguridad y la presencia de herramientas de análisis. En caso de que el Malware Evasivo detecte alguno de estos antes de ejecutarse, simplemente no se ejecuta. Es decir, que cuando el entorno es hostil no se ejecuta, esperando mejor oportunidad.

Características del malware Evasivo

En su nivel más básico, el malware intenta evadir a los defensores siendo único, de forma que pequeños cambios generan variante de esos malware. "Pero la protección anti-malware moderna todavía puede determinar que las nuevas variantes pertenecen a varias familias. Y único o no, el malware sigue llevando a cabo acciones reconocibles", explica Sullivan Sean, Security Advisor de F-Secure Coporation, diciendo que la tecnología antimalware puede centrarse en la detección genérica de las "herramientas" (código) utilizadas o en el propio comportamiento.

¿Qué debe tener un malware para ser evasivo? Esta es la primera pregunta que hemos lanzado a un grupo de expertos de seguridad. Dani Creus, analista de seguridad de Kaspersky Lab, explica que para que un malware pueda considerase evasivo debe llevar incorporadas una serie de rutinas

CÓMO VENCER AL MALWARE EVASIVO, O AVANZADO

El éxito de la detección de malware basado en el comportamiento depende del propio comportamiento que presenta el archivo durante el análisis. Por lo tanto, el objetivo de cualquier técnica de evasión de sandbox es ocultar el comportamiento real del archivo malicioso, evitando así la detección.

Los creadores de malware siempre están buscando formas nuevas e innovadoras para eludir las sandbox. En este documento técnico se analizan tres categorías de enfoques adoptados por el malware para evadir las sandboxes y explorar técnicas asociadas con cada enfoque.

orientadas a modificar u ocultar su comportamiento (flujo, entorno de ejecución o comunicaciones) dependiendo si se dan o no ciertas condiciones. El malware evasivo, asegura, “puede tener en cuenta desde factores temporales (fecha en la que se ejecuta), geográficos (desde que localización se ejecuta) o detectar aspectos de su entorno para decidir si ejecutarse de una manera o de otra (o no ejecutarse) u optar por alguna otra contramedida”.

Para Josep Albors, Responsable de investigación y concienciación de ESET España, debido a la evolución de las soluciones de seguridad, “ya no basta solamente con camuflar el código para no ser identificado cuando descargamos un archivo malicioso o intentamos ejecutarlo”. De forma que el malware que quiera considerarse realmente evasivo ha de ser capaz de sortear esa primera capa de detección, conseguir ubicarse en memoria sin levantar sospechas, comunicarse con los centros de mando y control establecidos por los delincuentes y realizar modificaciones en el sistema sin ser clasificado como actividad maliciosa.

TIPOS DE MALWARE Y CÓMO PROTEGER TU PC

CLICAR PARA VER EL VÍDEO

Al diseñar herramientas de ataque, los adversarios reconocen que las víctimas probablemente tendrán defensas antimalware modernas, dice Lenny Zeltser, VP Products de Minerva Labs, añadiendo que los atacantes incorporan tácticas de evasión en el software malicioso para aumentar la probabilidad de que su malware sobreviva, lo que implica el evitar la detección y el análisis al evitar herramientas de seguridad, eludir los métodos antimalware al operar principalmente en la memoria y comprometer los puntos finales al abusar de las características del sistema operativo y las aplicaciones. Y añade el directivo que muchas de estas tácticas de evasión se encuentran bajo el paraguas de los llamados Fileless Attacks, o ataques sin archivos, “durante los cuales los atacantes evitan colocar códigos claramente maliciosos en el sistema de archivos para evitar escaneos y enfoques de detección similares”.

"Si consideramos el polimorfismo como una técnica de evasión, la mayoría del malware es evasivo"

Bogdan Botezatu, Senior Cybersecurity Analyst de Bitdefender

Rubén Franco, Sales Security Engineer Panda Security, dice que cualquier malware que incorpore funcionalidades que permitan evaluar su entorno y de esta manera poder cambiar su comportamiento para eludir cualquier medida o tecnología puesta en marcha dentro de un modelo de protección de seguridad establecido podrá considerarse como malware evasivo.

Tipos de malware

Según Kaspersky Labs, se puede dividir el malware en los siguientes clases:

Virus clásicos. Programas que infectan a otros programas por añadir su código para tomar el control después de ejecución de los archivos infectados. El objetivo principal de un virus es infectar. La velocidad de propagación de los virus es algo menor que la de los gusanos.

Gusanos de red. Este tipo de malware usa los recursos de red para distribuirse. Su nombre implica que pueden penetrar de un equipo a otro como un gusano. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (P2P), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.

Caballos de Troya, troyanos. Esta clase de programas maliciosos incluye una gran variedad de programas que efectúan acciones sin que el usuario se dé cuenta y sin su consentimiento: recolectan datos y los envían a los criminales; destruyen o alteran datos o usan los recursos del ordenador para fines criminales, como hacer envíos masivos de correo no solicitado.

Los troyanos no pueden penetrar a los equipos por sí mismos, sino se propagan por los criminales bajo la vela de algún software “deseable”, a pesar de lo cual son capaces de causar mucho más daño que los virus clásicos.

Spyware. Software que permite colectar la información sobre un usuario/organización de forma no autorizada, pero no es su única función, ya que son conocidos por lo menos dos programas (Gator y eZula) que permiten también controlar el equipo.

Otro ejemplo de programas espías son los programas que instalan su código el navegador de Internet para redireccionar el tráfico. Posiblemente haya visto cómo funcionan, cuando en cambio de la página web solicitada se abre una otra.

Phishing. Es una variedad de programas espías que se propaga a través de correo. Buscan los datos confidenciales del usuario, de carácter bancario preferente. Los emails phishing están diseñadas para parecer igual a la correspondencia legal enviada por organizaciones bancarias, o algunos brands conocidos y contienen un enlace que redirecciona al usuario a una página falsa que va a solicitar entrar algunos datos confidenciales, como el numero de la tarjeta de crédito.

Adware. Muestran publicidad al usuario y a veces pueden recolectar y enviar los datos personales del usuario.

Riskware. No son programas maliciosos, pero contienen una amenaza potencial. En ciertas situaciones ponen sus datos a peligro. Incluyen programas de administración remota, marcadores, etc.

Rootkits. Un rootkit es una colección de programas usados por un hacker para evitar ser detectado mientras busca obtener acceso no autorizado a un ordenador.

"Si bien puede estar diseñado para evitar la detección de cualquier motor, el malware evasivo suele estar orientado a entornos donde existe un sandbox"

José de la Cruz, CTO de Trend Micro Iberia

"Para que un malware se considere evasivo, puede emplear diversas técnicas, que van desde el cifrado, la codificación o el polimorfismo hasta bloquear el appliance de seguridad o el dispositivo de análisis", señala Bogdan Botezatu, Senior Cybersecurity Analyst de Bitdefender.

De manera similar José de la Cruz, CTO de Trend Micro Iberia, asegura que se puede denominar como evasivo a un malware que intenta pasar desapercibido ante los motores de detección automatizados. "Esto lo consigue empleando técnicas de detección del entorno, retardo de ejecución, o ejecución programada por aportar algunos ejemplos. Si bien puede estar diseñado para evitar la detección de cualquier motor, suele estar orientado a entornos donde existe un sandbox", añade.

El juego del gato y el ratón

Así se refiere uno de nuestros expertos a la manera de combatir el malware evasivo, añadiendo después que "al margen de medidas técnicas de bajo nivel para mejorar la detección, algunas de las contramedidas utilizadas en el campo de análisis son: ejecución en entornos altamente modificados para tal propósito, modificación del sistema virtual para ocultar sus características reales al malware, emulación de un entorno "real" y simulación de comportamiento humano (creando actividad como apertura de documentos, movimientos de ratón, etc.)", explica Dani Creus, de Kaspersky Labs.

MaaS, o Malware-as-a-Service

El malware-as-a-service ofrece una serie de servicios que sin duda facilita las operaciones en este ámbito, de manera que los criminales pueden simplemente alquilar una infraestructura o servicio determinado para optimizar sus campañas. "Aunque la propia definición del servicio puede llevarnos a pensar que MaaS es utilizado por delincuentes con poca sofisticación y recursos, lo cierto es que durante los últimos años no se ha dejado de innovar en este ámbito, ofreciendo servicios cada vez más profesionales y difíciles de perseguir", asegura Dani Creus, analista de Seguridad de Kaspersky Lab.

Sobre el papel que juega el Malware-as-a-Service en el incremento del malware avanzado, dice Josep Albors, responsable de investigación y concienciacón de ESET España que es "bastante menos de lo que podríamos imaginar. La mayoría del malware que se genera como servicio son amenazas ya conocidas a las que se les aplica alguna variación e incluso muchas veces la calidad del código deja bastante que desear".

Para Bogdan Botezatu, Senior Cybersecurity Analyst de Bitdefender, "las familias de malware con capacidades avanzadas no se venden a terceros; solo las utiliza el grupo de delincuentes informáticos responsable de su desarrollo".

Dice José de la Cruz, Director Técnico de Trend Micro, que el Malware-as-a-Service juega un papel fundamental puesto que este tipo de malware, con el ánimo de evitar ser detectado por motores tradicionales basados en firmas, se genera de manera dinámica minutos antes de comenzar el ataque.

Los servicios de Malware-as-a-Service "facilitan las herramientas necesarias para que de una manera sencilla y rápida se puedan crear muestras de malware con diferentes características y funcionalidades permitiendo enfocarse en un número determinado de objetivos o en un espectro más amplio dependiendo de la finalidad del ataque", dice Rubén Franco, Sales Security Engineer Panda Security.

Dice Sullivan Sean, Security Advisor de F-Secure, que el "Malware-as-a-Service puede estar en declive en estos momentos y que "s tendencias se están orientando más hacia pequeños grupos de atacantes que atacan a organizaciones, en busca de buenos objetivos de extorsión".

Para Lenny Zeltser, VP Products at Minerva Labs, la disponibilidad de malware comercial diseñado para ser utilizado por adversarios que no pueden o no desean crear su propio código malicioso "ha contribuido a la mayor prevalencia de tácticas de evasión".

Dice José de la Cruz, Director Técnico de Trend Micro, que el malware evasivo se combate como cualquier otro tipo de malware, "combinando diversas tecnologías (seguridad multicapa) basadas en una combinación de tecnologías tradicionales (firmas, reputación, etc.) con otras de última generación (machine learning, sandboxing, análisis de comportamiento, etc.".

Josep Albors, de ESET, apunta a las soluciones de seguridad multicapa "que sean capaces de identificar una amenaza en alguna de las diferentes fases por las que pasa cuando intenta infectar a su víctima. Empezando por las detecciones estáticas de código y pasando por la detección del malware cuando intenta ubicarse en la memoria del sistema, comunicarse con un centro de mando y control o usar de forma maliciosa una aplicación legítima del sistema, entre otras".

En Minerva Labs utilizan el engaño, "mentirle al malware con respecto a lo que es real, por lo que sus intentos de implementar la funcionalidad file-less no funcionan, lo que hace que el malware se bloquee, se ponga en suspensión o finalice", dice Lenny Zeltser.

Para Bogdan Botezatu, de BitDefender, el único método eficaz para detectar el malware evasivo “es crear modelos de aprendizaje automático adiestrados con conjuntos de muestras existentes”. Estos modelos de aprendizaje automático pueden identificar las características principales del malware y buscarlas independientemente de lo alterada que esté la muestra.

Dice Rubén Franco, de Panda Security, que una de las posibles vías para poder combatir este tipo de amenazas es disponer de tecnologías avanzadas aplicadas a la Ciberseguridad con capacidad de análisis y computación muy potente además de escalable debido a la variedad y el volumen de muestras de malware generado día a día. También se recomienda disponer de capacidades de análisis inteligente, análisis de comportamiento y, muy importante, el análisis de contexto. “Una de las tecnologías que mejor está encajando ahora mismo con este modelo es el de Machine Learning que está ofreciendo unos ratios de detección y remediación realmente interesantes”, dice Rubén Franco.

Técnicas de evasión

Los creadores de malware siempre han buscado nuevas técnicas para permanecer invisibles. Y no sólo en la máquina comprometida, sino poder ocultar indicadores y comportamientos maliciosos durante el análisis. Los ciberdelincuentes intentan utilizar técnicas para ocultar archivos maliciosos a los sistemas automatizados de análisis de amenazas y sistemas antivirus, utilizando técnicas de ocultación y evasión.

¿Cuáles son esas técnicas? Para Sullivan Sean, Security Advosor de F-Secure, si en años pasados la técnica más utilizada eran los rootkits, actualmente es el fileless malware, o malware sin archivos.

Explica Lenny Zeltser, de Minerva Labs, que una táctica de evasión consiste en implementar técnicas de inyección de memoria sencillas desde un programa Java, en lugar de usar un archivo ejecutable compilado. Estas tácticas son bien conocidas por las compañías de antivirus y, a menudo, son evitadas por las herramientas antimalware típicas si son ejecutadas por ejecutables compilados. “Sorprendentemente, cuando el malware implementa las mismas técnicas que usan Java, son increíblemente efectivos para evitar el antivirus, lo que resalta la naturaleza frágil de las modernas herramientas antivirus contra las técnicas de evasión”.

"Las soluciones de sandboxing han tomado más protagonismo porque sirven como apoyo para la detección de malware avanzado, que en los últimos años ha adquirido un alto grado de polimorfismo"

Rubén Franco, Sales Security Engineer Panda Security

Asegurando que existen muchas técnicas y muy variadas, Rubén Franco, de Panda Security, menciona las dedicadas a reconocer el entorno en el cual se encuentra la muestra de malware y en base a esto accionarse o no, lo que suele servir para la detección de entornos sandboxing. También existen técnicas que en función de la fecha y la hora toman determinadas acciones cambiando su comportamiento. Por último, menciona las técnicas de ejecución de código malicioso en memoria a través de macros o scripts pertenecientes a herramientas

legitimas del sistema; “en este caso, por ejemplo, una macro con contenido malicioso que se inyecta al ejecutar un archivo EXCEL, por lo que no habría ningún ejecutable en disco involucrado”.

Dani Creus, analista de seguridad de Kaspersky Labs, destaca, por su volumen, las técnicas que detectan si el malware está intentando ser depurado o ejecutándose en un entorno virtual. Y destacables por su complejidad, “el malware que utiliza comunicaciones no-standard para exfiltrar información (Airgap, encapsulación de tráfico, etc.) o aquel que es altamente dirigido y solo se ejecutará en máquinas que cumplan unas condiciones muy específicas”.

"El malware evasivo se combate con años de experiencia. El malware desarrolla nuevas técnicas para esconderse y el anti-malware desarrolla nuevas tecnologías para descubrir. Así, la innovación combate el malware, evasivo o no"

Sullivan Sean, Security Advisor at F-Secure Coporation

Para Josep Albors, responsable de investigación y concienciación de ESET España, las técnicas de evasión más destacadas son las que consiguen que el malware pase como una aplicación legítima y realice sus acciones de forma que no levante sospechas, muchas veces usando para ello procesos reales del sistema.

Sandboxing Revival

Una sandbox, o caja de arena, es un mecanismo de seguridad en el que se crea un entorno separado y restringido y en el que se prohíben ciertas funciones. Una sandbox se utiliza a menudo cuando se utilizan códigos no probados o programas no confiables de fuentes de terceros.

El sandboxing de aplicaciones comenzó a desarrollarse durante la década de 1990 como una

respuesta clave al malware polimórfico. Veinte años más tarde, ha evolucionado. Las soluciones de sandboxing han sido de utilidad desde hace bastantes años sirviendo como complemento a otras muchas soluciones, formando parte del denominado modelo de protección en profundidad basado en capas, explica Rubén Franco, de Panda Security. Dicha tecnología ha asistido y asiste a Firewalls, soluciones de protección de email y web además de otras como antivirus o las nombradas anteriormente EDR. Ofreciendo así un modelo de protección cohesionado y compacto, siendo cierto que las soluciones de sandboxing cada vez han tomado más protagonismo “debido a que sirve como apoyo para la detección de malware avanzado que en los últimos años ha adquirido un alto grado de polimorfismo”.

Da la sensación de que, existiendo desde hace décadas, ha sido hace unos años cuando las sandboxes han recobrado protagonismo. Esto se ha producido por dos motivos, explica Josep Albors, de ESET. Primero, el aumento de los recursos de los que disponen los sistemas ha permitido que se puedan usar de forma más intensiva las sandboxes para revisar archivos sospechosos sin impactar negativamente en el rendimiento. De igual forma, la optimización de las sandboxes ha conseguido que se reduzcan notablemente incidentes como los falsos positivos.

> "Los continuos avances en las tecnologías antimalware motivan a los adversarios a incorporar tácticas de evasión en su malware"
>
> Lenny Zeltser, VP Products en Minerva Labs

Dice Dani Creus, de Kaspersky que dejando a un lado el grado de sofisticación de las mismas, las sandboxes han sido una herramienta necesaria desde siempre. “Probablemente su protagonismo actual se debe a que cumplen un rol importante para mitigar algunos de los problemas a los que se nos enfrentamos hoy en día en este ámbito: el volumen del malware (número de muestras), sus características de evasión y la necesidad de automatización”, añade el analista de seguridad.

Para Bogdan Botezatu las sandboxes han tenido una mayor acogida durante los últimos años, "coincidiendo con la aparición del ransomware camuflado como documentos de Word o archivos PDF que se utilizaba para causar estragos en las empresas", y añade que las tecnologías de análisis del comportamiento y en espacio aislado son modernas tecnologías de detección no basadas en firmas más eficaces para combatir el malware en constante evolución.

Apunta Sullivan Sean el impacto de la nube al decir que, aunque hace ya diez años se utilizan sistemas de emulación básicos, hace años que se utilizan sistemas basados en la nube que no impactan en el ordenador del cliente, "pero ahora podemos extender fácilmente nuestro software a la nube. Por lo tanto, sí, el análisis dinámico mediante el uso de sandbox se está convirtiendo en una herramienta importante en la búsqueda de malware".

Finalmente apunta Lenny Zeltser, VP Products en Minerva Labs, que la capacidad de analizar automáticamente un archivo sospechoso para determinar su naturaleza es un componente importante de la arquitectura defensiva actual. Dichas herramientas, que están disponibles como utilidades gratuitas y productos comerciales, son utilizadas por muchas empresas y también por compañías anti-malware. Los atacantes son ciertamente conscientes de que los defensores utilizan dichos enfoques para examinar archivos potencialmente maliciosos y, a menudo, idean formas para evitarlos. Explica la compañía que una sandbox debe parecerse a un punto final del mundo real para "persuadir" al malware que se está ejecutando en un sistema real. "Desafortunadamente, hay muchas formas en que el código malicioso puede determinar cuándo su entorno de ejecución es inusual, en cuyo caso dicho malware evasivo terminará por sí solo o se pondrá en suspensión para evitar revelar su verdadera naturaleza a la sandbox". El paso siguiente es pasar de ratón a gato utilizando el engaño, y hacer uso del mismo para hacer creer al malware evasivo que no está donde cree estar para que se active y pueda ser detectado.

Enlaces de interés...

- Clasificación del malware evasivo
- Cómo derrotar a todo lo malicioso como servicio
- El malware de minado de criptomonedas y los troyanos bancarios, entre las amenazas más prevalentes
- Guía práctica para combatir el malware avanzado
- Crisis: The Advanced malware
- Un enfoque eficaz para la clasificación de malware avanzado con alta precisión
- Protección frente al malware evasivo

Compartir en RRSS

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.

Inteligencia artificial inteligente o inteligible

A pocos días del comienzo de la campaña de Navidad, los principales fabricantes de tecnología preparan el lanzamiento de sus últimos dispositivos inteligentes. La inteligencia artificial irá incorporándose paulatinamente a cualquier dispositivo tecnológico para aportar el valor extra demandado por el usuario digital.

El gran reto en la era digital consiste en optimizar los interfaces de usuario para que puedan proporcionar experiencias digitales únicas. El interfaz debe simplificarse y trasladar al usuario la máxima naturalidad posible. Qué mejor manera de optimizar estos nuevos interfaces que hacerlo en modo conversacional con el dispositivo. Precisamente en esta área es donde los asistentes conversacionales inteligentes llegan al mundo digital tanto en entornos corporativos como en el segmento de consumo para facilitar esta operati-

va diaria del usuario y añadir valor adicional con sugerencias que puedan enriquecer la tan ansiada experiencia digital. Según IDC, En 2019, el 75% de los trabajadores tendrán acceso a asistentes personales inteligentes para aumentar sus habilidades y conocimientos.

¿Estamos preparados para incorporar un dispositivo inteligente en nuestros entornos corporativos o domésticos? Ante esta pregunta surge la incertidumbre acerca del nivel de seguridad que pueden aportar estos dispositivos y como podrían impactar en nuestro entorno si ésta fuera vulnerada de alguna forma.

Cómo pensamos resolver el conflicto respecto a la seguridad de un dispositivo que puede actuar como un micrófono de nuestras conversaciones privadas e incluso transmitir imágenes en tiempo real de la estancia en la que están colocados. Es difícil dar respuesta a esta esta cuestión cuando se extienden recomendaciones de seguridad que proponen soluciones tan sencillas pero eficientes como tapar la cámara del portátil con un simple esparadrapo o para los usuarios más avanzados, con una de esas ventanitas fabricadas a propósito para facilitar la ocultación de la cámara a deseo del usuario.

Solo debemos acudir a una reunión de trabajo dentro o fuera de nuestras oficinas para comprobar el efecto contagio de estas sencillas recomendaciones de “seguridad casera”. En uno u otro momento habremos sido nosotros los que preguntamos sobre el motivo de dicha ocultación de cámara y seguro que más de uno habrá recurrido a ese olvidado rollo de esparadrapo para hacer lo propio en su cámara al llegar a casa. Los más afortunados incluso habrán salido de la reunión con una de esas ventanitas que sirven a la vez de escaparate promocional de la marca de aquellas empresas que las regalan habida cuenta de la creciente demanda.

¿Entonces qué ocurre con la seguridad de los dispositivos de asistencia inteligente para el hogar? ¿Lograrán vencer la creencia del usuario respecto a su nivel de seguridad? Y aquí tenemos que hacer memoria de los mensajes a los que a diario nos vemos expuestos en cuestiones de ci-

it whitepapers

EL PAISAJE DE AMENAZAS DE IOT Y LAS VULNERABILIDADES MÁS COMUNES EN 2018

Mucho se ha hablado de los beneficios que Internet of Things ofrece no solo a la vida cotidiana de los consumidores, sino también a las infraestructuras de la ciudad, los gobiernos y las empresas. Pero, ¿cuán conscientes son los consumidores de la seguridad? Según una encuesta de Bitdefender, aunque los usuarios están entusiasmados con la incorporación de dispositivos conectados en sus vidas, los más populares siguen siendo los teléfonos inteligentes (91%), los televisores inteligentes (73%) y las tabletas (72%).

berseguridad, ya que todos hemos aprendido que las nuevas amenazas se diseñan para permanecer ocultas, en funcionamiento y sin ser detectadas el mayor tiempo posible. En la actualidad el tiempo de detección de un malware de este tipo supera los meses e incluso puede superar el año sin que sea detectado. Cada vez son más avanzadas las técnicas de evasión incorporadas en este tipo de malware que dificulta su detección e incluso pueden generar falsos positivos aportando maniobras de distracción mientras que siguen su ejecución y recopilación de datos.

También hemos aprendido que la propagación de este tipo de amenazas se realiza en su mayor

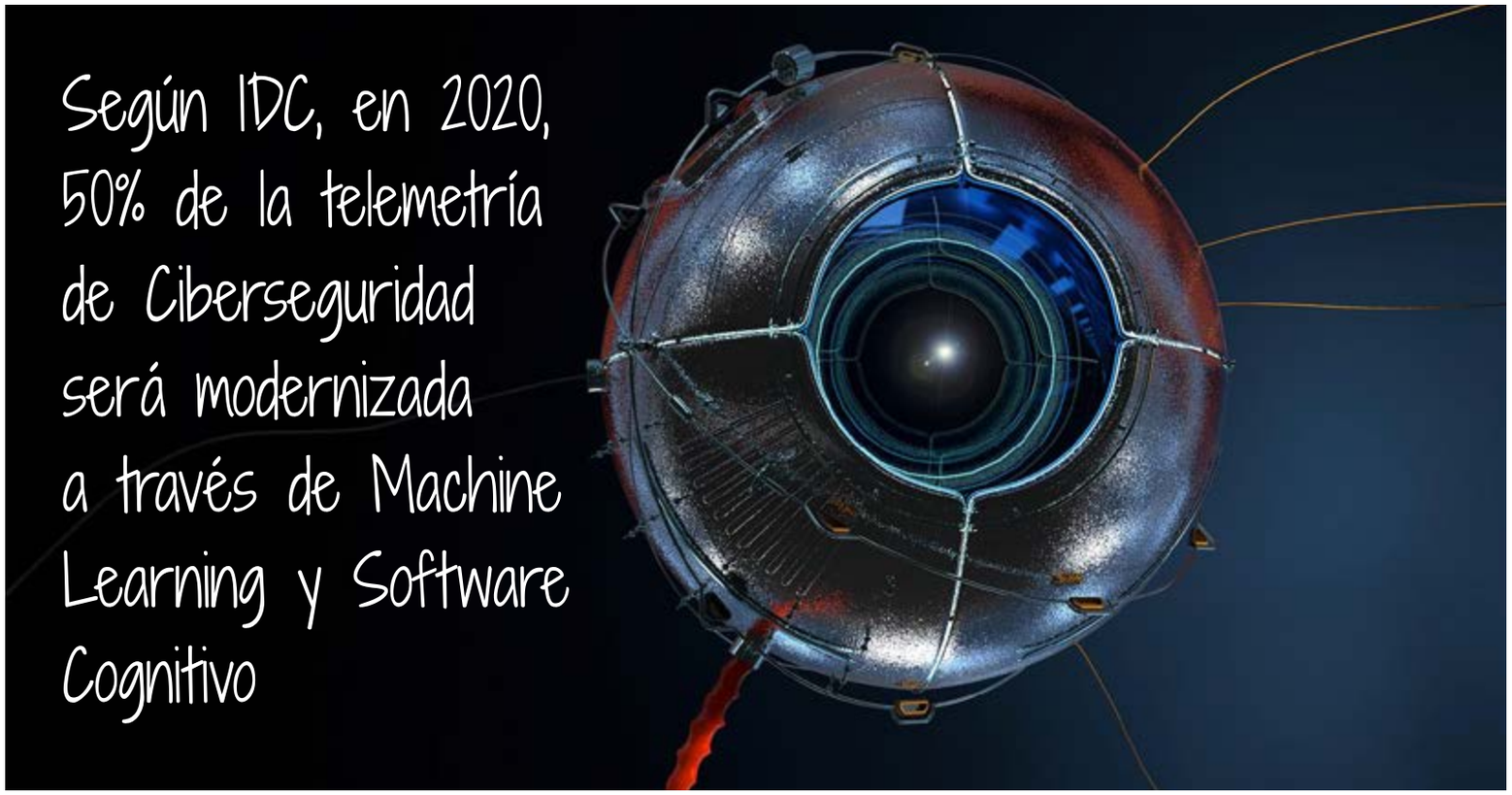
Debemos contribuir a seguir generando una cultura de seguridad en el usuario final, haciéndole participe de lo importante que es que tome conciencia de ciertas actividades diarias

Enlaces de interés...

- TimpDoor, un malware que convierte dispositivos Android en proxies de red
- Nueva herramienta de descifrado para el ransomware GandCrab
- Detectadas 25 apps de Google Play con criptomalware
- Se reaviva el interés por crear nuevo código malicioso

parte por ingeniería social con objetivos muy bien definidos y difícil de evitar si no hay una concienciación y formación en el usuario que debe evitar abrir ciertos correos electrónicos, pinchar en links adjuntos, utilizar memorias USB regaladas, instalar software no corporativo,..etc

Según IDC, en 2020, 50% de la telemetría de Ciberseguridad será modernizada a través de Machine Learning y Software Cognitivo. Pero la ciberseguridad además de tener a la tecnología y a la propia inteligencia artificial utilizada para detectar este tipo de nuevas amenazas también necesita de una componente humana que debe contribuir a aplicar el sentido común a muchas de las estrategias de ciberseguridad articuladas. El símil es muy sencillo: es como el que instala en su casa una puerta acorazada y después deja las ventanas abiertas y sin rejas cuando sale de casa. Del mismo modo debemos contribuir a seguir generando una cultura de seguridad en el usuario final, haciéndole participe de lo importante que es que tome conciencia de ciertas actividades diarias y el riesgo que éstas pueden implicar para la información que maneja. Solo así podremos continuar difundiendo mensajes de “seguridad doméstica” que al igual que el esparadrapo en la cámara del portátil pueden parecer muy rudimentarios, pero también altamente efectivos.



Conoce cómo la Logística y los marketplace transforman el eCommerce

Centro de Recursos **User**

Patrocinado por:

Packlink® PRO
Simply Shipping

ROb1n HOOd de las Networks

LORENZO MARTÍNEZ RODRÍGUEZ

EXPERTO EN CIBERSEGURIDAD

Ingeniero Informático de profesión, con gran experiencia en el mundo de la seguridad informática, Lorenzo Martínez Rodríguez es un reconocido ponente en Congresos de Seguridad Informática, tanto nacionales como internacionales, con vocación académica y co-fundador del blog de seguridad informática de habla hispana Security By Default, y con numerosas certificaciones en soluciones punteras de seguridad.

Lorenzo Martínez pertenece a ANCITE (Asociación Nacional de Ciberseguridad y Pericia Tecnológica), además de disponer de reconocidas certificaciones CISA y CISSP (hasta el 13 de Marzo de 2015).

Desde siempre, Internet ha estado plagado de riesgos en mayor o menor medida. La constante evolución de la tecnología, que la misma sea desarrollada e implementada sin considerar el modelo de "Security By Design", la curiosidad insana de algunos actores, la necesidad de los gobiernos para tener un acceso secreto y permanente a cualquier ordenador o dispositivo conectado a Internet; son apenas unos cuantos ingredientes del caldo de cultivo actual, que ha generado que Internet se haya convertido en una versión moderna del Salvaje Oeste.

Por su grado de exposición, aquellos sistemas que tengan servicios accesibles desde Internet de forma directa serán las víctimas más probables de recibir más ataques de forma activa y frecuente.

Las organizaciones y empresas con recursos y procedimientos para corregir y parchear sus sistemas de forma proactiva e inmediata tendrán una ventana de exposición más controlada. Sin embargo, los más vulnerables siempre serán los mismos: los usuarios de a pie, ya sea porque carecen de tales recursos y procedimientos, porque no tienen posibilidad de acceder a ellos o simplemente, por desconocimiento o falta de información.

Aquellos para los que la tecnología es un medio de uso y no algo a mantener, cuidar, proteger y afi-

LA CRISIS DEL EMAIL FALSO

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

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

lar, son quienes sin duda acusan más esa falta de preocupación y actualización, y cuyo nivel de exposición es aún mayor si cabe.

Recuerdo los antiguos tiempos, en los que mientras instalábamos Windows XP con una conexión por modem, y al tener en el sistema operativo la IP pública de forma directa, miles de máquinas contaminadas con el gusano Sasser nos infectaban la máquina reiniciándola. No fue hasta la implementación del Service Pack 2 de Windows XP que se introdujo el firewall integrado en la máquina, con bloqueo de tráfico entrante por defecto. Si te tocaba empezar la instalación desde un Windows XP anterior a SP2, corrías con suerte si lograbas terminar la descarga y actualización hasta Service Pack 2, sin que tu proceso "lsass" resultase afectado y tu sistema infectado.

En 2016, los ataques a dispositivos denominados como IoT ("The Internet of Things" o el "Internet de las Cosas") que derivaron en un control total para formar parte de la botnet Mirai, dieron fe de lo peligroso que resulta dejar conectados a Internet dispositivos que, a la hora de ser actualizados, no se lo ponen fácil al usuario.

En 2017, Wannacry fue sin duda el malware más popular afectando a sistemas Windows que tenían activo SMBv1, una versión obsoleta del protocolo

que permitía ejecución de código de forma remota en la máquina afectada, con los más altos privilegios del sistema operativo. En este caso, el malware era una combinación de ransomware que cifraba ficheros del disco, y además se reproducía a través de la red, infectando todo aquel sistema que tuviese el mismo protocolo activo. Miles de máquinas de grandes compañías resultaron afectadas.

En Mayo de 2018, una de las vulnerabilidades que más ruido ha hecho es la que afecta una vez más a los dispositivos IoT, en este caso a routers de diferentes marcas como Asus, D-Link, Linksys, Mikrotik, Netgear, etc,… que permitían a un atacan-

En 2017, Wannacry fue sin duda el malware más popular afectando a sistemas Windows que tenían activo SMBv1, una versión obsoleta del protocolo

Enlaces de interés...

- ¿Qué es VPNFilter y por qué ha sembrado el caos en Internet?
- VPNFilter es peor de lo esperado
- Cómo proteger los routers domésticos de ataques como VPNfilter

te hacerse con el control total del mismo. El ataque se denominó VPNFilter, y aunque los fabricantes publicaron rápidamente el parche, corrigiendo la vulnerabilidad mediante la aplicación de un nuevo firmware, a día de hoy sigue habiendo muchos dispositivos vulnerables a ser controlados remotamente, al no haber sido actualizados.

Y aquí es cuando un ruso que se hace llamar "Alexey", ha decidido tomar parte activa en el tema, identificando equipos vulnerables de la marca Mikrotik (algunos supongo que hasta previamente vulnerados) expuestos a Internet, parcheándolos para que no vuelvan a ser accesibles, cerrando el acceso al exterior y además, dejando un mensaje al dueño del equipo indicando que le ha arreglado una gran vulnerabilidad en su router, en el que se incluye un enlace al canal de la aplicación de mensajería Telegram, en donde pueden contactarle.

Sorprendentemente, la reacción de múltiples usuarios, lejos de darle las gracias por haberles solucionado un problema del que no eran conscientes, o que la desidia hizo que no se le prestara la importancia que realmente tiene esta vulnerabilidad, fue justo lo contrario de lo esperado: quejas por haberse metido sin permiso en su equipo y mucha preocupación por qué más podría haber hecho en sus equipos este "Robin Hood de las Redes".

Antes de entrar en cualquier debate respecto de si su actuación ha sido buena o mala, legal o ilegal, si es un héroe o no, entre otras tantas cuestiones que pueden surgir, la reflexión previa que estamos obligados a hacer es: Si fueras un usuario en esta situación, que no te ha importado tener un dispositivo vulnerable, y que al menos ese problema te lo ha resuelto "Alexey" ¿realmente ahora te preocuparías de qué acciones puede haberte hecho sobre el router? ¿y por qué preocuparse ahora y no antes, cuando incluso, te lo podrían haber vulnerado otros actores para formar parte de VPNFilter? ¿el hecho de no haberte dado cuenta de una vulneración previa, que pudo haber existido, es menos grave que la actuación de alguien que es transparente y te informa que lo ha corregido?

Y en el caso de que seas uno de esos afortunados o desafortunados a quienes "Alexey" ha dejado uno de estos mensajes ¿qué harás de ahora en adelante? ¿esperar a que otros exploten otras vulnerabilidades en tus equipos, o a que aparezca este u otro Robin Hood? ¿o decidirás preocuparte por fin de tu seguridad?

Blockchain: la tecnología con mayor potencial para redefinir el entorno digital

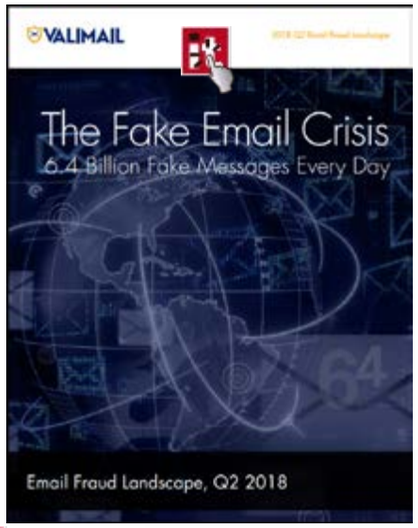
La historia es cíclica. La industria también. Vamos adoptando modas, ideas y tecnologías que aseguramos son nuevas pero que en realidad giran sobre sí mismas. Si hace unas cuantas décadas la centralización movió la industria y la economía hacia una nueva era de prosperidad, ahora es la descentralización quien tira del carro.

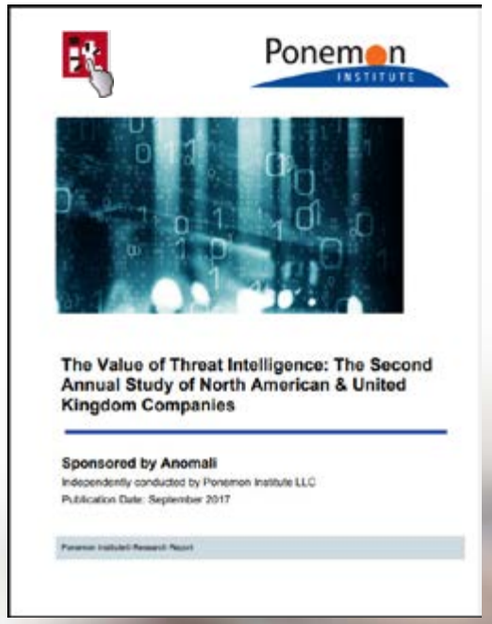
La cambiante cara de los ciberataques

Ataques cada vez más complejos continúan amenazando a las empresas en todo el mundo. La rápida evolución del panorama de las ciberamenazas ha dado lugar a una serie de ciberataques inesperados de alto perfil.
Este documento le ayudará a entender los diferentes tipos de amenazas que se están propagando actualmente. Un ataque DDoS, por ejemplo, puede ser sólo una cortina de humo para un ataque más grave, un ataque de ransomware puede ser utilizado para exfiltrar datos y un ataque IPv6 para acceder a IPv4.

La crisis del email falso

El correo electrónico sigue siendo un medio eficaz para las comunicaciones en todo el mundo, pero cada día se envían 6.400 millones de email falsos. Lejos de ser simplemente un problema de “ingeniería social”, el correo electrónico falso es el resultado directo de problemas técnicos con la forma en que se implementa el correo electrónico: carece de un mecanismo de autenticación incorporado que hace que sea muy fácil fallar a los remitentes. Sin embargo, este problema también es susceptible de solución técnica, comenzando con los estándares de autenticación de correo electrónico DMARC, SPF y DKIM.





El valor de la Inteligencia de Amenazas

Los resultados de este estudio muestran que las organizaciones están incorporando rápidamente la inteligencia de amenazas en sus programas de seguridad.
Algunos de los datos que aporta este informe: Un 84% dice que la inteligencia de amenaza es esencial para una fuerte postura de seguridad; un 80% ya usa inteligencia de amenazas en su propia organización (en comparación con 65% en 2016); un 68% dice que la inteligencia de amenaza es demasiado voluminosa y compleja.

La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

SANTIAGO ARELLANO

RESPONSABLE COMERCIAL DE ABANLEX
Delegado de Protección de Datos oficialmente certificado por AENOR (DPD-0021/2018) e ICAM.
Socio Fundador de Working Hackers
Vicepresidente de la Asociación por la Privacidad y la Ciberseguridad (AEPYC).
Con más de 15 años de experiencia en el sector de la ciberseguridad, asumiendo funciones de Dirección Financiera, Operaciones y Diversificación en compañías multinacionales de distribución de seguridad informática. Fundador de la filial en España de Exclusive Networks.

La creación de un nuevo perfil profesional: el cyberlawyer

La religión emergente más interesante es el dataísmo, que no venera ni a dioses ni al hombre: adora a los Datos. Esta sentencia extraída del libro Homo Deus: Breve historia del mañana del historiador y escritor israelí Yuval Noah Harari, pone de manifiesto algo que venimos corroborando día tras día: la importancia de los datos.

Los datos son ya el mayor activo de las compañías; el nuevo combustible de la economía; el moderno maná, pero en lugar de enviarlo el Dios Yavhé al pueblo hebreo en el desierto, los generamos los humanos en cantidades ingentes para deleite de la computación.

El término estado del arte, que descubrí tardíamente, más concretamente aplicado a la tecnología, aparece recogido en el artículo 32 del Reglamento General de Protección de Datos (RGPD) y, traducido al castellano, como estado de la técnica. El anglicismo hace referencia a lo "puntero", a "lo más avanzado", en los siguientes epígrafes aparece en el sentido de "el estado de la temática en cuestión".

El estado del arte de las amenazas y la ciberseguridad

Las empresas necesitan usar los datos para convertirlos en información que facilite la toma de decisiones acertadas y, por lo tanto, la generación de negocio. Por consiguiente, siendo lo datos el activo más importante de las compañías, también es el objeto más deseable al ser el de mayor valor. La exposición de los datos debe ser la principal preocupación de las organizaciones, más aún si cabe, con la aparición de una nueva ciberextorsión al amparo de las fuertes sanciones que trae consigo el Reglamento Europeo de Protección de Datos, consistente en secuestrar los datos per-

Se calcula que los ciber ataques, cuestan a la economía mundial más de 400 mil millones de euros cada año y, en 2017, España batió su récord de ciberataques: 120 mil

sonales que posee la organización y solicitar un rescate, a menos que se quiera que la “profanación” sea conocida por el Organismo Regulador y tener que afrontar las consecuencias económicas de la multa o, más grave aún, el daño a la imagen de conocerlo los afectados.

No hay prácticamente día que nos levantemos sin escuchar en las noticias casos de fugas de datos en las empresas, lo que continúa desgastando la confianza de los ciudadanos en la situación de la ciberseguridad. Los profesionales de ciberseguridad se enfrentan permanentemente a un horizonte de amenazas en constante evolución.

Unamos al riesgo actual, la aparición de nuevos bienes de consumo conectados como puede ser el coche autónomo y la reciente conexión de los sistemas que gestionan infraestructuras críticas, como pueden ser centrales eléctricas o señales de tráfico.

No debemos olvidarnos tampoco de la llamada amenaza interna que la mayoría de las compañías subestiman; las accidentales las podemos resolver con concienciación y formación, pero para resolver las intencionadas debemos acudir a soluciones tecnológicas que permitan monitorizar estos anómalos comportamientos. La fuga de datos e información sensible que se puede escapar y poner a la luz pública por esta vía, puede poner contra las cuerdas a cualquier organización.

Dos datos destacados que nos deben hacer reflexionar, a nivel mundial, se calcula que los ciberataques, cuestan a la economía mundial más de 400 mil millones de euros cada año y, en 2017, España batió su récord de ciberataques: 120 mil.

¿Cómo nos enfrentamos a este oscuro panorama? Pues poniendo en práctica un término que adquiere una renovada jerarquía: resiliencia. Una organización tiene resiliencia cuando posee la capacidad de resistir a la incertidumbre, a las crisis, a los cambios y situaciones conflictivas y de aprender de estas experiencias aprovechándolas para recuperarse, adaptarse y progresar.

En un entorno en cambio constante, donde los ciberdelincuentes no encuentran límite a su apetito voraz y donde se crean permanentemente nuevos

Las empresas ciber-resilientes están concienciadas sobre lo difícil que es garantizar la seguridad en sus organizaciones y han adquirido una actitud proactiva frente a los ciberataques.

y más sofisticados ciberataques, las victorias conseguidas ante las amenazas de hoy no suponen ninguna garantía de triunfo para las amenazas de mañana y así llegamos al principio de responsabilidad proactiva consagrado en la normativa de protección de datos y que deriva en el nuevo término acuñado recientemente de ciber-resiliente.

Las empresas ciber-resilientes están concienciadas sobre lo difícil que es garantizar la seguridad en sus organizaciones y han adquirido una actitud proactiva frente a los ciberataques.

El primer paso para ser una organización ciber-resiliente, será contar con soluciones de ciberseguridad apropiadas para cumplir con los niveles de protección necesarios y poder garantizar su funcionamiento correcto. El paso siguiente, supone que se debe realizar una monitorización continua de la infraestructura y conocer en todo momento qué protección se tiene y cuáles son los riesgos potenciales a los que se enfrenta, garantizando de esta manera que se está, proactivamente, protegiendo a la organización.

La ocasión que se abre para la ciberseguridad es muy notable, son las tecnologías de seguridad desarrolladas por los fabricantes, las compañías que hacen la función de "evangelización" de las soluciones emergentes y distribución de las consolidadas y las empresas integradoras que implementan las soluciones a sus clientes, las que no deben desaprovechar esta inmensa oportunidad.

El estado del arte de las ciber-regulaciones

Antes de referirme con más detalle a las ciber-regulaciones nacionales, debemos hacer una parada en Europa, en las instituciones europeas, de donde emanan las principales normas que a este respecto estamos implantando, bien por imposición directa o bien por transposición de estas.

Las compañías y los organismos públicos dependen de las redes e infraestructuras digitales para proveer sus servicios, lo que se traduce en que cualquier incidente de seguridad tiene, de facto, una gran repercusión

La reforma de la ciberseguridad en Europa aspira a fortalecer sus normas a este respecto, porque es la única manera de que el sueño de un mercado único digital sea efectivo. El Mercado Único Digital contribuirá de manera muy significativa al crecimiento de la economía europea, estimándose en 415 mil millones de euros al año y creándose, además, miles de nuevos puestos de trabajo.

Pero el riesgo está acechando permanentemente a las empresas, a las administraciones y a los ciudadanos. Por poner tan sólo un dato sobre la mesa que arroja el informe de ciberamenazas 2018 de SonicWall: el 37% de los ataques a nivel mundial de ransonware lanzados en 2017 impactaron directamente en países europeos.

Europa también es consciente de que el "internet de las cosas" o deberíamos dar un paso más y hablar del "internet de todas las cosas", es ya una realidad y prevé que para 2020 existan decenas de miles de millones de dispositivos digitales conectados en la UE.

Las compañías y los organismos públicos dependen de las redes e infraestructuras digitales para proveer sus servicios, lo que se traduce en que cualquier incidente de seguridad tiene, de facto, una gran repercusión, pues compromete la prestación de servicios e imposibilita a las empresas funcionar de manera adecuada, lo que se agrava considerablemente si la desgracia golpea a un operador de servicios esenciales.

De esta manera, Europa, además de dotarse de normativa que robustezca la ciberseguridad comunitaria, crea organismos que refuerzan su "ciber-resiliencia" como es un Equipo de Respuesta a Emergencias Informáticas, donde todos los países cooperarán en la lucha contra los ciberataques.

Y llegamos a España, y comprobamos que hay ya un compendio de ciber-regulaciones de seguridad a propuesta del Instituto Nacional de Ciberseguridad de España (INCIBE), que reúne toda la legislación española que afecta a la ciberseguridad y que, según su Secretario General, es una materia que ya resulta imprescindible para lograr una adecuada protección de empresas, instituciones y ciudadanos dentro de un estado social y democrático de derecho.

Empieza el vademécum, como no podía ser de otra manera, con la Constitución y me llama poderosamente la atención que los siete ponentes que se encargaron de la redacción allá por el año

En 2016 nos llegó de Europa el Reglamento General de Protección de Datos (RGPD) y, aún hoy, estamos esperando que se cumpla a estos efectos la llamada Ley de Chéjov

1977, pudieran estar interesados en legislar sobre la incipiente “informática”. Por cierto, en dicho año, nacieron los estudios universitarios de Informática en España.

Efectivamente el artículo 18.4 de la Constitución dice que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Me congratula pensar que hace 40 años los padres de la Constitución pudieran imaginar el uso desmesurado y, en algunos casos abusivo, que de los datos de los individuos y mediante el uso de la informática podrían hacer las organizaciones.

Poniendo el listón tan alto en aquellos momentos, no es de extrañar que hasta 1992 no se promulgara la LORTAD, que regulaba el tratamiento automatizado de datos de carácter personal y que fue derogada en 1999 por la famosa LOPD, fruto de la transposición de la Directiva 95/46 del Parlamento Europeo. Y digo famosa por varios motivos, en primer lugar, porque puede ser la única Ley que carece de “exposición e motivos”; en segundo lugar porque gran parte de los profesionales consideraban a la LORTAD de mayor riqueza y concreción; y, por último, el fracaso en su aplicación, donde menos del 25% de las empresas obligadas, cumplían.

El paseo normativo nos lleva por la senda de la Seguridad Nacional y nos damos de lleno con la Ley de Seguridad Nacional, donde se pone de manifiesto que “la seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos”, por lo tanto, la ciberseguridad es objeto de especial interés. Asistimos al nacimiento de varios Comités e Instituciones como son, el Centro Nacional de Inteligencia, el Consejo Nacional de Ciberseguridad que, entre otras funciones, verifica el cumplimiento de la Estrategia de Ciberseguridad Nacional. Nos topamos en la caminata con dos Esquemas Nacionales, el de Seguridad que regula la política de seguridad en la utilización de medios electrónicos y el de Interoperabilidad para posibilitar el intercambio de información, ambos relativos a la Administración Pública.

Finalmente, nos detenemos un rato en la reciente transposición de la Directiva NIS, en la que España y otros países europeos se quedaron evidentemente transpuestos y a la que auguro, una importante presencia en los próximos años. La Directiva que finalmente se transpuso por vía de urgencia (Real Decreto-ley) el pasado 7 de septiembre afecta a las entidades que realicen la prestación de servicios esenciales y aquellas que presten servicios digitales. Lo que nos podemos encontrar en los próximos meses, es un número considerable de empresas

Los trabajadores dedicados a la ciberseguridad cambian frecuente y voluntariamente de patrón, desincentivando la inversión en la formación y desarrollo en estos profesionales por parte de los empresarios

que posiblemente desconozcan que están afectadas por esta regulación de seguridad de las redes y sistemas de información.

Necesitamos, sin duda, un primer avituallamiento y rápidamente continuar el camino. Hablamos ahora de medidas para la protección de infraestructuras críticas, aquellas que dotan de servicios imprescindibles a la ciudadanía y las que convierten en proveedores “esenciales” a los fabricantes de ciberseguridad y a las empresas de seguridad que les prestan servicios.

Proseguimos la expedición y nos acercamos a la normativa de seguridad, donde comprobamos el alcance de la Unidad de Investigación Tecnológica de la Policía en la persecución de los ciberdelitos; la Ley de protección de la seguridad ciudadana, donde se consagra la seguridad ciudadana como un requisito imprescindible para el pleno ejercicio de los derechos fundamentales y las libertades públicas; y, también, la regulación de Seguridad Privada y su complementariedad y coordinación con las Fuerzas y Cuerpos de Seguridad.

Nos detenemos en un paso para descansar brevemente frente al Centro Criptológico Nacional y quedarnos tranquilos mientras comprobamos que existen protocolos que regulan al equipo de respuesta a incidentes de seguridad y que sabemos gestionar los incidentes de ciberseguridad que afectan a internet, garantizándose la confidencialidad, la disponibilidad y la integridad de la información.

En el ecuador del recorrido tropezamos con las normativas de Telecomunicaciones y Usuarios,

ordenanzas que regulan las telecomunicaciones para garantizar el cumplimiento de los objetivos de la Agenda Digital para Europa; que disponen obligaciones a los servicios de la sociedad de la información y de la contratación por vía electrónica; que establecen medidas para regular las comunicaciones electrónicas, el comercio electrónico, el acceso electrónico y la firma electrónica.

Tomamos un atajo, mala idea, y nos damos de bruces con los códigos que atienden la Ciberdelincuencia, se trata del Código Penal, de la normativa reguladora de la responsabilidad penal de los menores y de la Ley de Enjuiciamiento Criminal. Corroboramos que los delitos clásicos son perfectamente aplicables al mundo tecnológico, ya que

Definiendo al "cyberlawyer" podemos coincidir en referirnos a un profesional mejorado, que podría ayudar a las organizaciones en el entorno tecnológico actual y futuro

en este último también existen las amenazas, los delitos de exhibicionismo, los delitos contra la intimidad, los delitos contra el honor, los de estafas, los relativos a la propiedad intelectual e industrial, al mercado y a los consumidores…Es decir, la historia se repite, aunque los medios son distintos.

Continuamos la marcha y a duras penas, aún siendo la legislación que más me concierne, llegamos a la Protección de Datos. Ya he comentado anteriormente los antecedentes de esta importante regulación, pero en 2016 nos llegó de Europa, el Reglamento General de Protección de Datos (RGPD) y, aún hoy, estamos esperando que se cumpla a estos efectos la llamada Ley de Chéjov. ¿A qué me refiero?, pues según estableció el dramaturgo ruso, "una pistola que aparezca en el primer acto de una obra teatral será disparada inevitablemente en el tercero". El tercer acto de la implantación normativa, comenzó el 25 de mayo de 2018 con el caos de las prisas y los bombardeos de petición de consentimiento que todos recordamos, a fecha de hoy y, a pesar de llamativas "fugas de información" de datos personales, echo de menos una sanción ejemplarizante que dinamice el cumplimiento normativo. De otra manera, nos empezaremos a preguntar si estamos ante una comedia, una farsa o, realmente, para algunas entidades acabará en un melodrama y quizás en una tragedia.

A pesar de habernos dormido de nuevo en la adaptación de la legislación española a las disposiciones contenidas en el RGPD, el trámite legislativo para la ley de protección de datos ya se encuentra en el Senado y, dado el consenso político existente, esperamos su promulgación antes de finalizar el año. Hay que destacar que esta norma expande su título con la "Garantía de Derechos Digitales" y legisla aspectos como "el derecho al olvido" en internet, la desconexión digital laboral o el testamento digital, lo que podría convertir a España a juicio del portavoz socialista implicado en la tramitación de este proyecto de ley en el Congreso, en el primer país europeo con una ley que de forma sistemática garantizará derechos digitales de los ciudadanos en todos los ámbitos.

Llegamos a puerto completamente exhaustos, con las Relaciones con la Administración y, así, descubrimos los derechos de las personas en sus relaciones con las Administraciones Públicas, la regulación del Registro Electrónico y la Sede Electrónica.

El viaje legislativo que hemos realizado nos debería convencer de la importancia que un marco regulatorio claro y sólido ostenta en la actual coyuntura tecnológica y que nos deberá acompañar, acortando la distancia, en un futuro contexto de previsible incremento de amenazas.

El estado del arte del mercado laboral

El informe referido a 2017 de la consultora californiana Frost & Sullivan (2017 Global Information Security Workforce Study), arroja datos relevantes sobre la situación a nivel mundial de los profesionales de la ciberseguridad.

En efecto, más allá del déficit previsto para el año 2022 que eleva en un 20% la previsión del estudio

anterior referenciado a 2015 y establece en 1,8 millones la brecha de la fuerza laboral, el informe afirma que el 87% de los trabajadores actuales dedicados a la ciberseguridad, no iniciaron su camino por esa especialidad. Es más, el 33% de los individuos con carreras “no técnicas” ostentan en sus organizaciones posiciones de decisión, teniendo categoría de ejecutivos senior, lo que en el argot significa posiciones C-Suite.

Otro de los aspectos significativos es la puesta de manifiesto de la desconexión existente entre las compañías empleadoras y los candidatos, las habilidades principales que priorizan las empresas son las de comunicación y las analíticas, mientras que los aspirantes al empleo priman las habilidades técnicas.

Lo anterior ilustra claramente la necesidad de ampliar horizontes distintos de los tradicionales única y exclusivamente técnicos e incorporar nuevos perfiles que creen nuevas profesiones.

Otra realidad importante que afecta a las compañías es la pérdida de talento a este respecto. La tasa de desempleo entre los profesionales de la ciberseguridad es del 2% a nivel mundial. La

Si bien, con los avances de las soluciones de ciberseguridad podremos proteger cada vez mejor las comunicaciones y los datos, la libertad de información no debe suponer el sacrifico de la privacidad, la autonomía y la individualidad

combinación de la baja tasa de paro con la escasez de fuerza laboral supone salarios altos y, por consiguiente, una alta volatilidad. Los trabajadores dedicados a la ciberseguridad cambian frecuente y voluntariamente de patrón, desincentivando la inversión en la formación y desarrollo en estos profesionales por parte de los empresarios, los cuales, se cuestionan cómo contratar y conservar el talento en un entorno como este. A mi juicio, un planteamiento interesante para resolver este problema sería estimular un desarrollo profesional de los trabajadores que supusiera formación en otras áreas, como pueden ser la legal, la inteligencia artificial, la comunicación… que hagan vislumbrar un horizonte nuevo y atractivo a estos especialistas.

Los distintos “estados del arte” por los que hemos ido pasando nos sugieren la figura de un nuevo perfil profesional que ya algunos denominamos cyberlawyer, tecnoabogado o ciberlegista.

Cyberlawyer

La tecnología ha tenido y tiene un tremendo impacto que ha afectado de manera positiva pero también de forma negativa a nuestra sociedad, pero que ya es algo imprescindible para todos. Las invenciones tecnológicas, motor fundamental del progreso, mejoran nuestra calidad de vida, pero también menoscaban nuestra privacidad.

En esta nueva realidad, virtual o no, no queremos atesorar ideas y conocimientos, queremos compartirlos y ponerlos en común. El empleo y manipulación que realicemos de la información es un reto para la sociedad y se hace necesario una participa-

ción más activa y comprometida con su desarrollo e impacto generalizado.

El marco legal establece los límites y además controla su cumplimiento para que las personas decidamos lo que queremos hacer con nuestros datos y, por otra parte, las soluciones de ciberseguridad garantizan el entorno seguro y el nivel adecuado de las organizaciones que usan y aprovechan la información.

Definiendo al “cyberlawyer” podemos coincidir en referirnos a un profesional mejorado, que podría ayudar a las organizaciones en el entorno tecnológico actual y futuro. Se trataría de un experto en derecho, especializado en protección de datos, con un conocimiento tecnológico importante o, dicho de otra manera, un especialista en tecnología con aptitudes de ciberseguridad, que mediante una formación importante en las llamadas ciber-regulaciones le permita acceso al difícil mundo interpretativo de las normas.

El culto al dato hace que la barrera entre abogados y técnicos se desplome y que emerja la figura de un único profesional que unifique las disciplinas legal y informática, componiendo alianzas sobre las actuales grietas académicas y expanda de manera sencilla ideas e innovaciones a través de los límites de ambas disciplinas.

No soy Abogado, y no menos importante, he de decir que tampoco soy “Informático”. Con razón cabe preguntarse qué hago opinando entonces y esa, precisamente, es la razón: no pertenezco a ninguno de estos dos mundos y estoy vinculado a ambos. Esta situación privilegiada es la que me habilita para expresar de manera contundente que los dos campos deben unirse o, al menos, interrelacionarse para cumplir con los mejores estándares de la privacidad y la seguridad. Ambos tienen, es más, necesitan desarrollar nuevas capacidades que les permitan una visión más integral de la problemática que gira en torno a los datos.

El marco legislativo y la adopción de medidas de ciberseguridad colocarán en una situación inmejorable a las empresas que coordinen ambas especialidades. Además, la protección con garantías de los derechos y libertades de las personas será un acicate para el desarrollo tecnológico que se verá libre de sospechas al incrementarse la confianza de los interesados dentro de un marco de cumplimiento legal de las organizaciones.

No lo digo yo, la AEPD en la guía para la gestión y notificación de brechas de seguridad dice que

El 87% de los trabajadores actuales dedicados a la ciberseguridad, no iniciaron su camino por esa especialidad

“La gestión de la privacidad y de la seguridad son entidades distintas con objetivos comunes: salvaguardar los derechos y libertades de las personas y garantizar la seguridad de la información. Responsables de seguridad y delegados de protección de datos están obligados a trabajar juntos estableciendo vínculos colaborativos y ambos son clave cuando se trata de salvaguardar la seguridad de los tratamientos”

Reflexión final

El dataísmo según cuenta Harari, posee también mandamientos, el primero y principal indica que se debe maximizar el flujo de datos conectándose cada vez a más medios y produciendo y consumiendo más información y, salvo raras excepciones, esto ya está ocurriendo. El siguiente precepto, apunta a que todo debe ser conectado, incluidos los “herejes” que no quieren ser conectados y, aquí, con la iglesia no dataísta, obviamente, hemos topado.

Si bien, con los avances de las soluciones de ciberseguridad podremos proteger cada vez mejor las comunicaciones y los datos, no soy partidario de la libertad de información que suponga sacrificar la privacidad, la autonomía y la individualidad de las personas, al menos, en aquello que consciente e informadamente no convengan de acuerdo con el marco legal que lo regule.

El propio Presidente Ejecutivo de Apple, Tim Cook defiende la ley RGPD europea y la plantea para el resto del mundo. En una parte de su discurso ante el Parlamento Europeo referida a la inteligencia artificial dice lo siguiente: Si queremos que ésta sea verdaderamente inteligente, debe respetar los valores humanos incluyendo la privacidad. Los peligros son muy grandes si no lo conseguimos. Podemos conseguir al mismo tiempo una gran inteligencia artificial y unos grandes estándares de privacidad. No es sólo una posibilidad, es una responsabilidad.

Y de esta responsabilidad que atañe a la sociedad emerge como figura reveladora el Cyberlawyer.

Enlaces de interés...

- Empleo en ciberseguridad: INCIBE publica una convocatoria para cubrir 27 puestos
- ¿Sabes si necesitas Delegado de Protección de Datos?
- CISO, CSO y DPO son los perfiles de ciberseguridad más demandados