2019 IN CYBERSECURITY

THE EXPERTS TALK

panda

pandasecurity.com

ÍNDICE

INTRODUCCIÓN

En el día Mundial de la Ciberseguridad, y con el final de este 2019 a la vuelta de la esquina, analizamos las principales asignaturas pendientes en seguridad de las grandes compañías.

La carrera a contrarreloj por la digitalización de las organizaciones no solo debe reflejarse en la implementación de tecnologías, sino también en la protección de los recursos. No obstante, la Online Trust Alliance (OTA), calcula que el 2018 cerró con un impacto total a nivel global que superaba los 45.000 millones de dólares. A la espera de conocer los datos de este año, tomar conciencia de esta realidad y blindar al máximo las redes y endpoints contra tales amenazas es un punto que ya no podemos obviar.

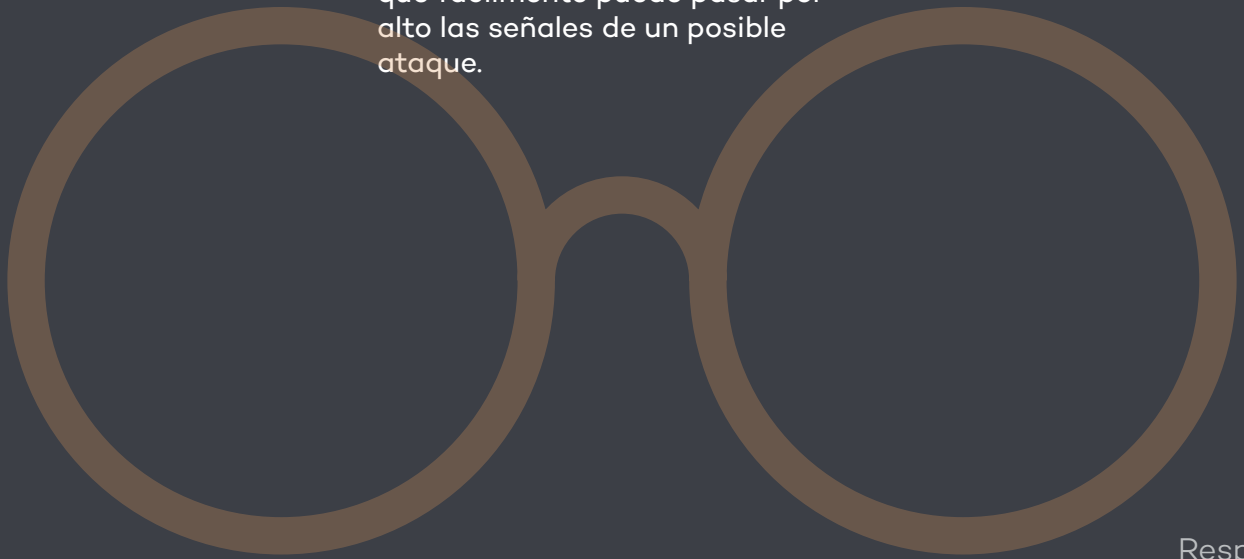
A pesar de que el efecto de un ciberataque a una empresa puede ser devastador, la gran mayoría de ellas no está preparada para afrontar un problema de esta envergadura. Aunque contemos con un buen plan de prevención y un gran equipo de seguridad, las brechas ocurren. Y es entonces cuando debemos tener listo un buen Plan de Respuesta a Incidentes: desde hacer frente a nuevas tácticas como los ataques Living off the Land, a la desaparición de algún portátil de la compañía o ataques de ransomware.

Paralelamente, no podemos olvidar que la seguridad es dinámica y que la formación debe ir a la par. Toda empresa trabaja con información valiosa sobre ella que debe mantenerse de puertas para dentro. Los empleados con acceso a dichos datos han de ser conscientes de su importancia y su obligación de mantenerlos a salvo.

Teniendo en cuenta que el factor humano continua siendo el elemento común de la mayoría de ciberataques relevantes, las empresas no deben escatimar en el presupuesto destinado a programas de formación para los trabajadores en materia de seguridad informática. Aunque parezca lógico, pautas como elegir contraseñas complejas, no reutilizar estas claves en distintas plataformas y guarder nuestras credenciales en lugares seguros son comportamientos habituales entre la plantilla.

La ansiada creación de un marco digital común se materializó con el Reglamento General de Protección de Datos europeo (GDPR). Un año después de su entrada en vigor, actualmente el 30% de las empresas europeas no cumple las reglas impuestas por el GDPR. Esto supone un gran riesgo de incurrir en multas severas por parte de las autoridades, además de una pérdida de confianza por parte de los clientes.

Finalmente, junto a una mayor seguridad de las redes corporativas, un plan de respuesta ante ciberataques, invertir en formación y adaptarse a las exigencies del GDPR, reducir la "fatiga de alerta" de los equipos de seguridad informática con tecnología de automatización y servicios avanzados es la gran asignatura pendiente. Un volumen cada vez mayor de alertas de seguridad y la escasez de profesionales abruma a los equipos de ciberseguridad, y hace que fácilmente puede pasar por alto las señales de un posible ataque.



¿Estarán de acuerdo nuestras firmas invitadas de este año?

Disfruta de la lectura de nuestra recopilación "2019 in Cybersecurity. The experts Talk".

Marta Zapata

Responsable de Comunicación
Panda Security

Román Ramírez

EL PUNTO FLACO DE LA CIBERSEGURIDAD SON LOS HUMANOS Y LA INVERSIÓN

Román Ramírez es conocido de sobra en el mundo de la ciberseguridad en España. Fundador de la RootedCon, el evento de seguridad más importante de España, y con más de veinte años de experiencia en el sector, ocupa desde hace una década el puesto de Gerente de Operaciones y Arquitectura de Seguridad de Ferrovial, donde se encarga de la gestión de las operaciones de seguridad a nivel corporativo y de la seguridad desde el diseño en proyectos y nuevos desarrollos dentro de la organización.

¿Protegen las empresas españolas su ciberseguridad lo suficiente?

Es una pregunta complicada. Una del IBEX 35 cuyo objetivo de negocio prioritario es el sector financiero protegerá más que adecuadamente sus activos y tendrá un nivel de ciberseguridad muy alto, pero una pyme unipersonal que se dedique a obras posiblemente estará en el otro extremo de madurez. En general, las empresas cuentan con el nivel de ciberseguridad que han planificado (es decir, que han decidido), aunque hay estratos donde, por razones de coste y cultura, el nivel es mejorable en muchos puntos.

¿Hay, al menos, más concienciación al respecto?

Ahora mismo la es mainstream. Todos los días hay noticias relevantes sobre el tema. Si eso no tiene a todo el mundo concienciado, nada lo va a hacer. En mi opinión, la concienciación solamente es efectiva con los que están ya concienciados: los humanos somos como somos y si para conseguir un objetivo A tenemos que pasar por encima de un obstáculo B, pasaremos. Y eso no lo va a cambiar ninguna concienciación.

¿Crees que el GDPR provocará que cuiden más su ciberseguridad? ¿O veremos un sinfín de multas a empresas por incumplir el reglamento?

Creo que cumplir con el GDPR es más sencillo que cumplir con la anterior LOPD. Pasamos a un modelo un poco más anglosajón, donde se te pedirán las garantías a posteriori (con evidencias). Creo que esto va a ayudar a que se extienda. Y sí creo que, con la preocupación creciente por la privacidad, algo ganaremos en distintos ámbitos. Sobre las multas, dada la cuantía, sospecho que van a tener mucho cuidado a la hora de sancionar.

¿Cuáles son los posibles puntos flacos de las empresas?

Siempre son los mismos: los humanos y la inversión. La ciberseguridad en cualquier ámbito es un problema de nivel de inversión. Si dedicas la inversión (económica y humana) adecuada, tendrás un nivel adecuado de ciberseguridad.

¿Puede haber una falta de ciberresiliencia?

Obviamente puede darse y se da. Puede ser que no te relajes, que sigas permanentemente pendiente de las amenazas… y que te enfrentes a una situación difícil de gestionar y donde sea complejo ser resiliente. El problema de la ciberseguridad es que es un entorno sin reglas predecibles en lo positivo (en lo negativo sí: si no inviertes te garantizo que vas a tener problemas muy serios). Invertir y gestionar bien en seguridad no es garantía de que no te vaya a pasar nada. Y si te ocurre, es complejo anticipar resultados y consecuencias.

Durante años, la actitud de las empresas ante los ataques siempre fue reactiva; ¿son cada vez más proactivas? ¿O siguen esperando a que ocurra la desgracia para actuar?

Las empresas que se toman en serio la seguridad prueban sistemáticamente sus activos, infraestructuras y personas. Con procesos de RedTeam, revisiones constantes, modelado de amenazas… es raro encontrar organizaciones que sigan pensando en modo reactivo.

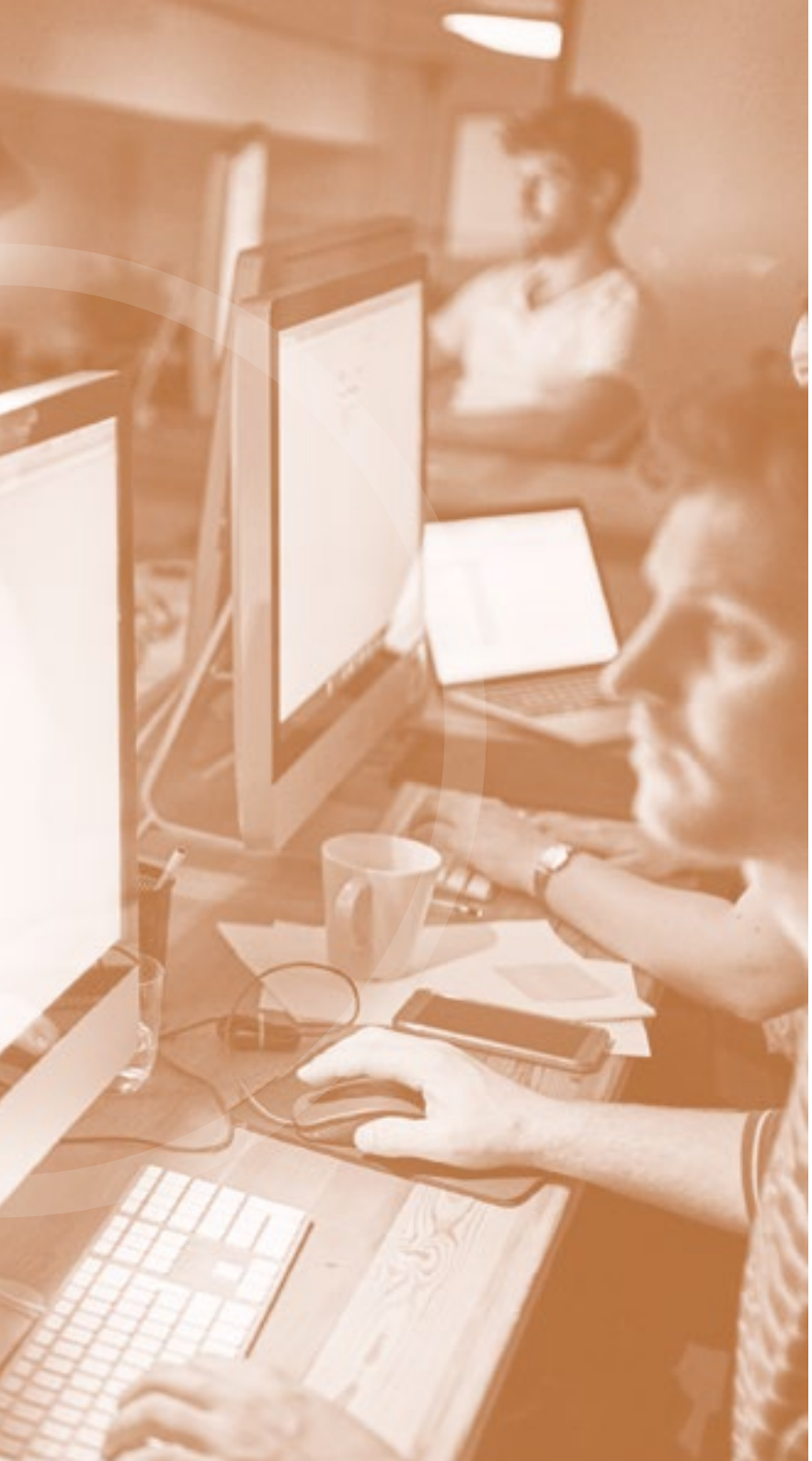
¿Qué tendencias de ciberataques ves más preocupantes a día de hoy?

Sobre todo vemos un incremento en todo aquello que es menos técnico y más industrializado: muchas campañas de phishing, mucho minero de criptomonedas… El cryptolocker, a pesar de las consecuencias que tiene, no es de lo más dañino hoy en día. El auge de las técnicas de inteligencia artificial lo veo como un potenciador de herramientas en el lado antagonista, lo que hará más complejo defenderse: habrá mucho más automatismo, con más capacidades y habilidades.

Una cosa que a mí me preocupa especialmente es que las agencias de inteligencia, donde tradicionalmente estaban en su mundo del gran juego, llevan ya muchos años en nuestro nivel más mundano. Esto tiene cada vez más consecuencias en el nivel empresarial (y ciudadano).

Imagínate que tienes delante al jefe de una pyme de 50 empleados, que te dice que a él no le afecta la preocupación por la ciberseguridad, que su empresa no es 'nadie' y nunca la van a atacar. ¿Qué le dirías?

Que está viviendo en un mundo paralelo donde cabalga sobre unicornios felices, y que sería bueno que analice si, por evitar sentir la presión de la inversión que necesita su empresa, no se está engañando y tomando decisiones con sesgo. Porque un incidente cualquiera puede conducir al cierre del negocio si se demuestra negligencia, si hay consecuencias a terceros, sanciones por parte de reguladores o robo de propiedad intelectual (y que te saquen de tu propio negocio porque alguien que te ha copiado lo hace más barato que tú) ■



Javier Diéguez

PARA AUMENTAR SU CIBERRESILIENCIA, LAS EMPRESAS DEBEN ENCONTRAR PRIMERO UN SOCIO DE CONFIANZA

En los últimos años se ha visto claramente que la ciberseguridad es un conjunto de prácticas que trascienden lo puramente tecnológico. Según Javier Diéguez, director del Basque Cybersecurity Centre, hoy comprendemos que la ciberseguridad tiene un componente de buenas prácticas, de gestión de riesgos empresariales, que han hecho que nuestra disciplina adquiera un rol mucho más transversal. La seguridad se toma ahora en cuenta como factor crítico en la capa directiva de los negocios, no tanto ya solo en la informática.

Javier cuenta con más de 15 años de experiencia en el sector de la seguridad empresarial e industrial, y ha sido el elegido para poner en marcha el centro de ciberseguridad vasco. Diéguez también formó parte del equipo de expertos que colaboró con el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) para la definición de los Planes Estratégicos Sectoriales del negocio eléctrico.

¿Cuál es tu labor como director del centro vasco de ciberseguridad?

He sido contratado para crear el BCSC desde cero, abordando una serie de objetivos a corto plazo como la propia organización del centro y el establecimiento de relaciones de confianza con otros organismos estatales y europeos. También para construir unos servicios básicos que permitan elevar la madurez de la industria vasca de ciberseguridad, fomentando una cultura empresarial de protección y defensa.

El País Vasco, además de tener una sensibilización especial para la protección y competitividad de la industria, tiene un sector emergente bastante importante en el ámbito de la ciberseguridad. No hay otro lugar con una concentración tan alta de startups y de productos de tecnología de ciberseguridad. Desde el BCSC, tenemos la obligación de desarrollar ese ecosistema y de favorecer su crecimiento, de buscarle conexiones y oportunidades internacionales porque, al ser un negocio digital, no puede entenderse solo en clave local.

En tu opinión, ¿cuáles son las mayores amenazas actuales?

El mayor tipo de denuncias que se reciben tienen que ver con el fraude, en muy diferentes modalidades: desde phishing indiscriminado hasta ataques más dirigidos como la suplantación del CEO. En un ámbito más de industria, el core económico del País Vasco, hay otros dos tipos de ataques importantes. El primero sería el sabotaje, la interrupción de las operaciones, que es menos habitual y puede tomar muy diferentes formas en un entorno industrial. Y una segunda amenaza, mucho más difícil de detectar, el ciberespionaje. Este tipo de ataque busca principalmente el robo de propiedad intelectual para ganar competitividad y perjudicar a un potencial adversario de negocios, y el robo de información de estrategias comerciales.

Has dedicado gran parte de tu carrera a las infraestructuras críticas, en especial las eléctricas. ¿Cuáles son los riesgos más comunes que afectan a esta industria?

Los ataques a negocio hasta hace pocos años se consideraban poco menos que imposibles o muy difíciles de realizar. Sin embargo, los sistemas de infraestructura crítica cada vez están más conectados y ofrecen más puntos de contacto con el exterior, sobre todo para labores de mantenimiento. Debe haber una labor de vigilancia importante para que ese perímetro, esa superficie de exposición a Internet, esté bien protegida. Y también para que la separación entre redes, dentro de la propia empresa, esté diferenciada entre redes críticas y redes menos críticas. En este ámbito, hay mucho camino por hacer: la segmentación no siempre es la debida, no están bien definidos los perímetros, ni están bien protegidos para evitar accesos no autorizados ya sean intencionados o accidentales.

También hay una serie de problemas relacionados con la longevidad y heterogeneidad de los sistemas y a los ciclos de vida de sistemas que dan soporte a las infraestructuras críticas.

En las eléctricas, los sistemas tienen ciclos de vida de décadas. Vemos que coexisten sistemas de muy diferentes generaciones; muchos de ellos son legacy que están fuera de soporte. No es extraño, por ejemplo, encontrarse con un Windows NT 4.0, un sistema operativo del año 1996. Estos softwares están completamente fuera de mantenimiento y ya no se fabrica parcheado.

Un tercer problema está derivado de la naturaleza de la tecnología y la política de soporte que tienen los fabricantes del equipamiento. Una compañía como Siemens o Honeywell suele poner limitaciones para que sus clientes, los operadores de infraestructura, puedan introducir mecanismos de control independientes o ajenos al paquete de soluciones que el fabricante le ha vendido. Esto limita la evolución de las protecciones en nuestro entorno.

¿Cómo puede una empresa aumentar su ciberresiliencia?

Las organizaciones deben diagnosticar su perfil de riesgo, hacerse un auto chequeo. Y para ello lo primero que debe hacer una empresa es encontrar un socio de confianza. Es más interesante que el socio de ciberseguridad sea independiente de la organización, guiado por el ámbito directivo de la organización que es quien conoce las prioridades del negocio, y por lo tanto puede establecer las prioridades y determinar activos y actividades más importantes que hay que proteger. A partir de esa definición de ese perfil y prioridades, empezar a dar pasos. También hay muchas medidas básicas susceptibles de ser aplicadas:

- Una protección de correo electrónico entrante.
- Filtros de navegación saliente para evitar acceder a URLs maliciosas.
- Protección de puestos de trabajo con soluciones de endpoint como puede ser la de Panda Security.
- Back-up de disco de forma habitual para hacer frente a ataques como ransomware que cifra la información de la empresa ■

Juan Antonio Calles

EL THREAT HUNTING PODRÍA MEJORAR LA CAPACIDAD DE DETECCIÓN Y RESPUESTA AL CRYPTOJACKING

CEO de Zerolynx y CSO de Osane. Previamente, ha sido responsable del laboratorio de ciberseguridad de KPMG y responsable del centro de hacking de Everis. Además, Juan Antonio cuenta con varias certificaciones de prestigio como Certified Hacking Forensic Investigator (CHFI) de Ec-Council y CISA de ISACA.

Según este experto en seguridad informática, la evolución en los últimos quince años ha sido tremenda. “Antes los trabajos de seguridad se centraban en la revisión de las páginas web de los clientes y auditorías internas para evaluar la seguridad del parque informático de los empleados. El sector ha evolucionado hasta un punto que por aquel entonces era difícil de predecir”.

A medida que las empresas adoptan cada vez más las estrategias cloud, ¿cómo garantizamos su seguridad?

Hace unos años, con disponer de un firewall de protección perimetral, muchas organizaciones se consideraban seguras, sin tener en cuenta que no solo hay que protegerse frente a las amenazas externas, las internas son igualmente importantes. Ahora las fronteras de confianza comienzan a desaparecer. Si a esto le añadimos una nube difusa con toda nuestra información distribuida entre varios CPDs repartidos por el mundo, con diferentes jurisdicciones, el entorno de seguridad se complica.

Si estamos decididos a dar el salto a la nube, es indispensable revisar si tendríamos capacidad para montar una nube sobre nuestra infraestructura. De ser posible, también habría que evaluar bien a los posibles proveedores, y una vez decidido, intentar alojar los datos de forma cifrada.

El firmware de Nintendo Switch fue hackeado el mismo día de su lanzamiento. ¿Cómo podría haber evitado Nintendo este tipo de situaciones?

El caso de la última versión del firmware (v7.0.0) de la consola de Nintendo es especial, pues no se trata de una vulnerabilidad del software, sino de un problema sobre el hardware de la consola. Lo que sucedió en enero es que habían logrado crackear las claves privadas sobre las que se firma esa versión del firmware para poder modificarlo. En este caso, para solucionarlo se debe hacer una revisión del hardware de la consola, en el cual Nintendo ya debe estar trabajando.

Por otra parte, para evitar fallos en el software, es crucial introducir la seguridad desde las primeras fases de su diseño: el llamado shift left. La integración de la seguridad en los flujos de trabajo de DevOps de una manera colaborativa, también conocido como DevSecOps, es una manera eficiente de preservar la calidad y la seguridad del trabajo en equipo, la agilidad y la velocidad de DevOps. Estos modelos de trabajo han demostrado un éxito contrastable frente a los modelos de desarrollo tradicionales, permitiendo desarrollar software con mayor calidad y seguridad, sin aumentar especialmente los tiempos y costes de desarrollo.

¿Cuáles dirías que son las mayores amenazas para la ciberseguridad empresarial en la actualidad?

Una de las mayores amenazas es el ransomware, sobre todo para pequeñas y medianas empresas que no cuentan con las medidas de seguridad habituales de las grandes organizaciones. Uno de los puntos más explotados en este tipo de ataque son los accesos remotos vía Team Viewer, VNC y similares. Para poder mitigar este tipo de ataques es vital disponer de VPNs robustas que permitan acceder de forma segura desde el exterior a los recursos de la organización, con un 2FA para asegurar que un robo de credenciales no sería suficiente para acceder remotamente, y una segmentación de red restrictiva, para contener el incidente en caso de que se produzca.

Otra amenaza que sigue en aumento es el cryptojacking, aprovechándose de igual manera de equipos expuestos para poder explotar su capacidad de cómputo para el minado de criptomonedas. Prácticas como el threat hunting permitirían encontrar de forma proactiva este tipo de amenazas dentro de las organizaciones, y mejorarían las capacidades de detección y respuesta.

También seguirán en aumento las amenazas sobre las infraestructuras críticas, sobre todo en el panorama actual de la industria 4.0. en el que las redes IT y OT comienzan a trabajar de forma coordinada, y los PLCs y demás componentes de la red OT adquieren capacidades de transmisión diferentes a la red cableada tradicional. En estas casuísticas tan complejas, es necesario crear un entorno hostil para el adversario, con una óptima segmentación entre el entorno OT-IT, evitando la exposición directa del entorno OT a internet (incluyendo los accesos a proveedores), desplegando capacidades de detección y respuesta en las máquinas de salto entre entornos y maximizando el control sobre las cuentas privilegiadas.

Finalmente, una de las amenazas que seguiremos encontrándonos en organizaciones y entornos industriales, es el espionaje industrial. Aunque las medidas de seguridad sean muy altas, siempre hay eslabones débiles que pueden pasar desapercibidos en los procesos de pentesting tradicionales. Por ejemplo, unos de los más destacados son los sistemas de videoconferencia, los cuales no suelen estar bien bastionados y raramente sus comunicaciones viajan de forma cifrada.

“

En estos últimos años, el mundo de la ciberseguridad se ha profesionalizado enormemente”

España comienza a ser un referente internacional; prueba de ello es el gran número de eventos de ciberseguridad que tenemos en nuestro país.

¿Qué importancia tienen los análisis de digital forensics en el mundo empresarial?

Antes de realizar cualquier tipo de análisis forense digital, lo primero será conocer qué ha ocurrido, cuál es el objetivo del análisis y cuáles son los activos afectados. No actuaremos de igual manera para analizar una red Windows afectada por un ransomware, que para investigar cómo se ha interceptado una factura en una estafa del CEO. Debemos adaptar nuestra metodología a cada casuística particular. El análisis forense digital es una función básica en las empresas para contestar a preguntas como: ¿qué ha ocurrido?, ¿cómo o por qué ha sido posible? Y este análisis sirve no solo para examinar un incidente, sino también para aportar luz en litigios, empleados que sustraen información, amenazas llevadas a cabo a través del email corporativo, entre otros.

¿Qué es el biohacking y qué aplicación podría tener para las empresas?

El término biohacking es una acepción muy abierta que puede hacer referencia a varias disciplinas y movimientos que van, desde la biología DIY, pasando por los grinders, que alteran sus cuerpos para añadir tecnología, hasta la nutrigenómica. Desde Zerolynx y en colaboración con Patricia Rada, doctora en bioquímica del Ciberdem (Centro de Investigación Biomédica en Red), estamos investigando para poder llevar a cabo el almacenamiento y ocultación cifrada de información en ADN. Es un estudio complejo en el que encontramos barreras difíciles de superar con la tecnología de la que se dispone a día de hoy. Hemos hecho pruebas sobre simuladores, y ahora desempeñamos pruebas reales sobre cepas de bacterias. Con los recursos adecuados, y viendo el interés de algunas organizaciones para que esto avance, creemos que en un par de décadas podríamos ver algún prototipo. Las posibilidades son casi infinitas, pero no es algo que veremos en empresas a corto plazo.

¿Cuáles son los 5 pasos más importantes de un plan de respuesta a incidentes efectivo?

Antes de que ocurra un incidente, debemos contar con un plan de continuidad de negocio y el correspondiente plan de contingencia; debemos haber formado previamente a los empleados para que sean capaces de detectar el incidente y sepan reaccionar de una forma adecuada, de acuerdo a cómo se haya establecido a nivel corporativo.

El primer paso de un SIRP (Security Incident Response Plan) debe ser la detección y la alerta al equipo de respuesta ante incidentes. Ya que no se debe actuar de igual manera ante un ransomware, una estafa del CEO, o un incendio en el CPD, los empleados que hayan detectado el incidente, deberán facilitar al equipo de respuesta la máxima información, para que en un análisis rápido puedan determinar cómo actuar ante la amenaza concreta. A continuación, y para asegurar la continuidad del negocio, deberían aislarse los entornos afectados, y recoger las evidencias correspondientes para poder investigar el origen del problema más adelante y, de ser necesario, realizar un completo análisis forense que podría acabar en una denuncia si se detecta una acción maliciosa. En ese caso, previo a cualquier actuación sobre los activos afectados, debería garantizarse la correspondiente cadena de custodia y el clonado y firmado digital de los activos afectados, para asegurar la integridad de la información contenida. Posteriormente se escalará el incidente y, si es necesario, se notificará a las autoridades correspondientes. Finalmente, se deberían catalogar, registrar todas las acciones realizadas y lecciones aprendidas, de cara a mejorar ante posteriores incidentes.

¿Cómo puede una empresa ser ciber-resiliente?

Las compañías necesitan definir un responsable de seguridad de la información (CISO) con la formación adecuada, y proveerle de los recursos necesarios para realizar su trabajo. Esta persona necesita un potente equipo de profesionales a su cargo, que puedan trabajar tanto en los aspectos normativos y de cumplimiento de la ciberseguridad, como en todos los aspectos más técnicos y operativos. Existen numerosas tecnologías para la protección de los activos corporativos: sistemas de back-up, firewalls, sondas de prevención de intrusos, SIEMs, etc. Sin embargo, sin los profesionales adecuados todas estas medidas suelen quedar rápidamente obsoletas, mal parametrizadas y dejan de servir como una barrera de protección real frente a los criminales que cada día acechan a las compañías. Todas aquellas compañías que no tengan la capacidad de tener un equipo cyber de alta calidad, deberían contratar los servicios profesionales de empresas especializadas del sector. Un proveedor de confianza, con una protección que se adapte a lo que el negocio necesita, es una opción importante para las empresas que no tienen medios de seguridad propios ■

> **“Sin los profesionales adecuados, las medidas de seguridad quedan obsoletas rápidamente”**

José Manuel Díaz-Caneja

EN OCASIONES ES MÁS FÁCIL CORROMPER A UN EMPLEADO QUE EMPLEAR CIBERATAQUES PARA REVENTAR UN SISTEMA

A la hora de proteger su ciberseguridad empresarial, las organizaciones tienen varios frentes abiertos, pero hay dos especialmente esenciales: por un lado, vigilar el factor humano, que muchas veces es el mayor desencadenante de ciberataques o fugas de información; por otro, aplicar inteligencia a todos sus procesos, de modo que la ciberdefensa avanzada no dependa de acciones reactivas, sino de desarrollos proactivos. De todo esto sabe largo y tendido José Manuel Díaz-Caneja, experto en análisis de inteligencia y profesor en el Máster de Ciberinteligencia de Campus de Ciberseguridad-UFV, con el que hemos hablado para conocer el estado actual de la ciberdefensa de las empresas y los retos que aún les quedan por delante.

En el panorama actual de la ciberseguridad, ¿qué papel juega la ciberinteligencia?

El término ciberinteligencia aparece siempre asociado a la ciberseguridad y, en la mayoría de las ocasiones, parece que se limita únicamente al análisis técnico de ciberamenazas con la finalidad de que sirva de base para mejorar las medidas de ciberseguridad de una organización. Es decir, un concepto muy reactivo, totalmente defensivo.

Si definiéramos ciberinteligencia como la inteligencia elaborada en base a la información obtenida en el ciberespacio y que apoya en los procesos de toma de decisiones y de planificación una organización, veríamos cómo su campo de actuación se ampliaba. Ya no solamente tendría como objetivo contribuir a defender una organización de las ciberamenazas, sino que además estaría dotada de un componente más ofensivo y proactivo que facilitaría el aprovechamiento de las oportunidades que brinda el ciberespacio.

La ciberinteligencia debe favorecer la elaboración de alertas estratégicas y predictivas de las ciberamenazas basadas en indicadores. El objetivo es prevenir y evitar, o por lo menos mitigar, sus riesgos asociados.

Las amenazas internas son uno de los principales riesgos a los que se enfrentan las organizaciones, ¿cuáles son las más frecuentes?

Por ahora la más frecuente es la accidental, como la difusión de información debido al uso de direcciones de email equivocadas, la no identificación de ataques de phishing o errores debidos a una mala configuración de los sistemas informáticos. Sin embargo, las acciones intencionadas están tomando gran relevancia debido a que, en muchas ocasiones, resulta más fácil corromper a un empleado que emplear sofisticados ciberataques para reventar un sistema.

Pongamos el ejemplo del SIM Swappping. ¿Por qué gastar esfuerzos en ataques de ingeniería social cuando resulta más fácil comprometer al empleado de una tienda de telefonía para que copie los datos privados de los clientes y duplicar posteriormente la SIM? Y lo mismo pasaría también en el caso de revelación de información sensible de la organización.

El problema con la amenaza interna intencionada es que muchas veces las organizaciones no son conscientes del número de empleados que tienen con privilegios para el acceso a información sensible.

¿Qué medidas deben implementar las organizaciones para estar preparadas para afrontar estas amenazas internas? ¿En qué consiste exactamente la contrainteligencia empresarial?

Antes de nada, la organización debe plantearse varias preguntas importantes:

- ¿Qué debe proteger nuestra organización?
- ¿Qué intentan descubrir nuestros competidores/ adversarios (o agencias de gobiernos extranjeros) sobre nosotros y por qué?
- ¿Cómo están tratando de hacerlo? ¿Qué capacidades tienen? ¿Aplican un enfoque técnico o están intentando sobornar a nuestros empleados?
- ¿Qué podemos hacer, y qué estamos haciendo, para reducir sus posibilidades de obtenerlo? ¿Qué tácticas legítimas de denegación y engaño podríamos emplear para salvaguardar nuestra información? ¿Y nuestras patentes o desarrollos de I+D?

> “Las acciones intencionadas están tomando gran relevancia debido a que, resulta más fácil corromper a un empleado”

Si una organización no es capaz de dar respuesta a las dos primeras preguntas de una manera clara y precisa, será incapaz de responder a las dos últimas. En este caso, el resultado sería que la organización adoptaría medidas de seguridad ineficaces para su protección.

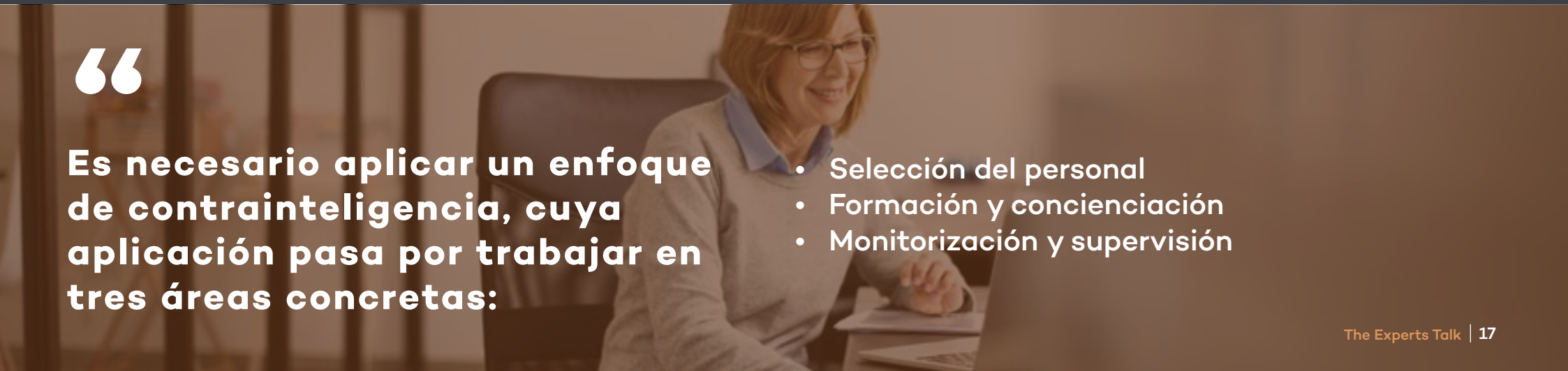
Para evitarlo, es necesario aplicar un enfoque de contrainteligencia, cuya aplicación pasa por trabajar en tres áreas concretas: selección del personal, formación y concienciación y monitorización y supervisión. En primer lugar, es fundamental realizar una adecuada selección del personal ajustada a los privilegios de accesos que vaya a tener. En segundo lugar, su formación y concienciación es clave, no solo para identificar un posible ciberataque, sino también para detectar actitudes sospechosas de compañeros que pudieran estar actuando de manera incorrecta. Esto pasa por la implementación de procedimientos, lo más discretos posibles, por medio de los cuales los empleados pudieran informar de estas supuestas actividades irregulares.

Por último, es necesario implementar un programa de monitorización e investigación que sirva como arma disuasoria, pero no solo centrado en aspectos técnicos, sino también para alcanzar un conocimiento profundo de aquellas personas que ocupan puestos clave en la organización. Hay que ser conscientes de que, en muchas ocasiones, el insider no es una persona de alto rango en la organización, sino todo lo contrario. Son personas que ocupan puestos de nivel medio o bajo y que, por distintos motivos, se encuentran insatisfechas.

Estamos acostumbrados a escuchar hablar de los procesos de inteligencia aplicados a los servicios de inteligencia gubernamentales, ¿qué ventajas tiene su implementación en cualquier tipo de organización?

La finalidad de la inteligencia en sentido amplio es reducir la incertidumbre y generar conocimiento, proporcionando productos oportunos, precisos, relevantes y, a ser posible, predictivos. De esta manera, apoyan en los procesos de toma de decisiones y en la planificación. Son procesos en los que se busca la proactividad y la anticipación para evitar que la organización se vea sorprendida.

En inteligencia no se trata de acertar, sino de reducir las probabilidades de equivocarse. Debe ser transversal a toda la organización y, en muchos casos, lo único que supone es la reordenación de los procesos internos de intercambio de información y toma de decisiones. Además, es importante señalar que para que tenga éxito tiene que conseguir involucrar a todos los interesados dentro de la organización.



> **Es necesario aplicar un enfoque de contrainteligencia, cuya aplicación pasa por trabajar en tres áreas concretas:**

- Selección del personal
- Formación y concienciación
- Monitorización y supervisión

¿Cuáles son para ti ahora mismo las principales amenazas a las que se enfrentan las empresas?

Parafraseando lo que dice la Estrategia de Seguridad Nacional del 2017, el espionaje es una de las primeras amenazas para muchas empresas. Tiene como objetivo obtener información por parte de la competencia que le facilite alcanzar una posición de predominio en el mercado a un menor coste. Si nos vamos al ámbito de las empresas que trabajan en proyectos vinculados con la seguridad nacional, nos encontramos que estas actividades de espionaje pueden poner al descubierto capacidades estratégicas vinculadas, por ejemplo, con la defensa o la protección de infraestructuras críticas.

Estamos finalizando el año, ¿qué tendencias en ciberseguridad crees que marcarán la próxima década?

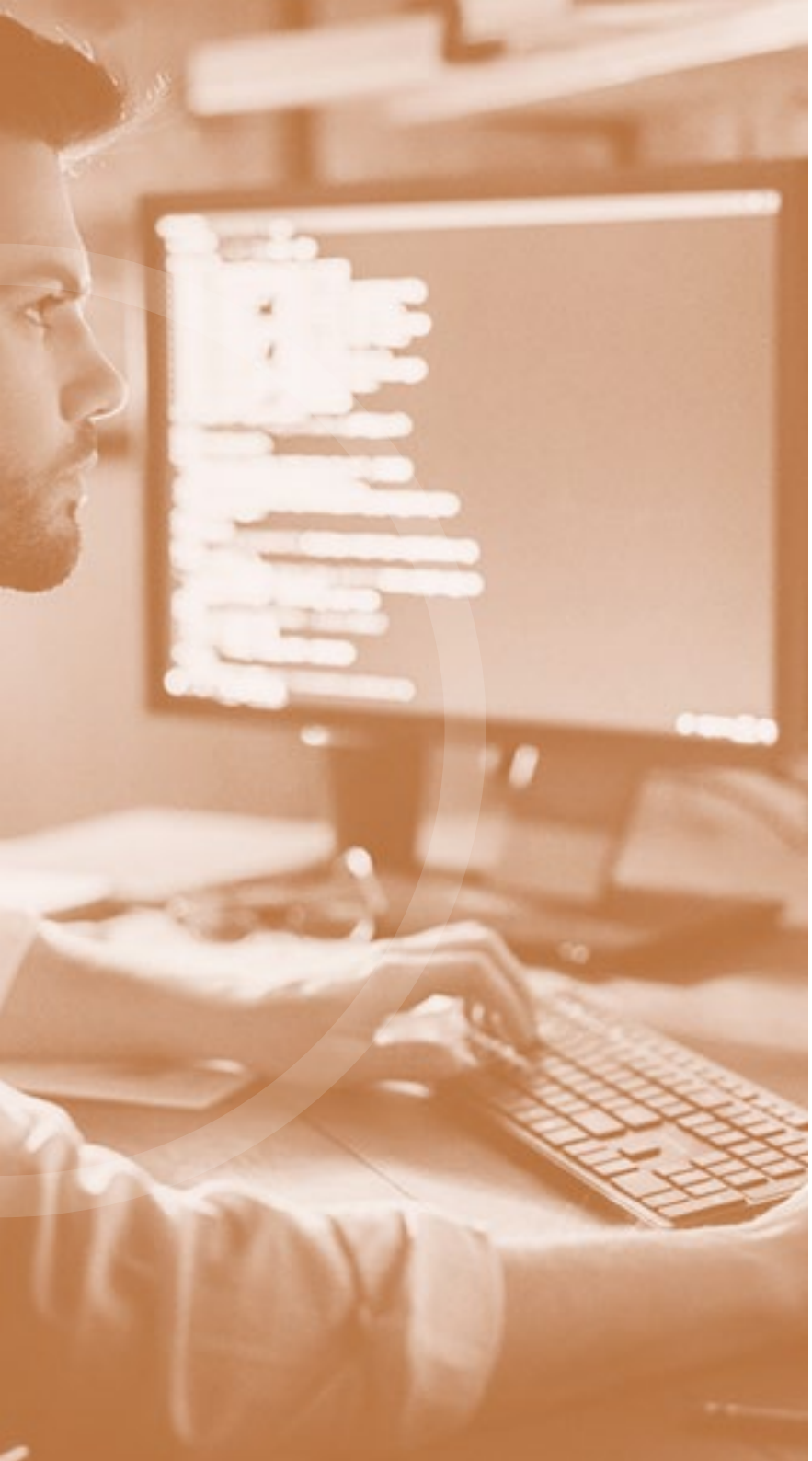
El uso del ciberespacio para llevar a cabo todo tipo de actividades ha llegado para quedarse. Por ello, la tendencia en ciberseguridad será seguir avanzando en desarrollos que permitan proteger a los individuos y organizaciones de una manera más eficiente.

Sin embargo, de nada sirve construir exclusivamente muros de protección basados en hardware y software. La historia demuestra que todos los muros o tienen puertas traseras o pueden ser perforados, por lo que hay que proporcionar una seguridad en los 360 grados. A lo anterior, se deben de añadir propuestas tecnológicas más imaginativas, basadas en la decepción y el engaño, que impidan o dificulten los ciberataques y, sobre todo, que mejoren las capacidades detección de alerta temprana.

Todo eso pasa por tener en cuenta que detrás de cada ordenador, ya sea el del atacante o del defensor, hay una persona cuyo objetivo en muchas ocasiones es provocar efectos en el mundo real.

Por eso, vincular la identificación de ciberamenazas únicamente a ciberinteligencia no es realista, ya que muchas veces la información que necesitamos para atribuir un ciberataque no la podremos obtener en el ciberespacio, sino que deberemos conseguirla con otras disciplinas de inteligencia ■

> “El uso del ciberespacio para llevar a cabo todo tipo de actividades ha llegado para quedarse”



María Campos

CREEMOS QUE SIEMPRE ES NECESARIA UNA COMBINACIÓN DE PRODUCTOS Y SERVICIOS AVANZADOS

Este año hemos sido testigos de la creación de Cytomic, la unidad de negocio de Panda Security. Cytomic busca dar respuesta a las demandas de ciberseguridad actuales del mercado, en concreto, a las necesidades más avanzadas de los clientes del segmento Enterprise, y como consecuencia del crecimiento de Panda Security.

Cytomic representa el concepto de modelo "ciberatómico", que refleja a la perfección su forma de entender la ciberseguridad. El modelo ciberatómico, más allá de quedarse en el átomo como punto de partida, va un paso más allá y se centra en analizar cómo se unen estos átomos para poder crear algo superior, ya que sólo a través de estas complejas relaciones se puede entender el proceso de formación de la materia.

Así es como Cytomic está abordando la ciberseguridad ya que, en lugar de centrar sus esfuerzos en las distintas partes, va más lejos para obtener una visión global.

Siguiendo esta máxima, intenta descifrar las relaciones entre los diferentes eventos que componen un proceso de ataque, investiga los comportamientos que tienen en común y unen eventos aparentemente aislados, desgrana y define todos los enlaces que se dan entre máquinas, personas, programas y comportamientos y que desencadenan un ataque. Y para entenderlo mejor, hablamos con María Campos, VP de Cytomic.

¿Qué es lo que viene a solucionar Cytomic?

Se crea una nueva unidad de negocio orientada a dar respuesta a las necesidades más complejas en ciberseguridad, a resolver la problemática de las organizaciones con un mayor nivel de madurez en ciberseguridad.

En Panda Security veíamos que, a pesar de tener una oferta adecuada al segmento medio, había una carencia en cuanto a servicios adicionales, plataformas que permitan meterse en todos los procesos que requiere una gran cuenta, que requiere la investigación, la respuesta de incidentes, una capa de servicios potentes, etc; Debido a esto, decidimos crear esta nueva unidad de negocio con una combinación de productos y servicios precisamente para ser mucho más concretos, precisos, para estar más adaptados y para ser muy flexibles a la hora de atender esas necesidades más avanzadas de ciberseguridad.

¿Cuál es la clave de la propuesta tecnológica de Cytomic?

Cytomic ofrece exclusividad, profesionalidad y especialización, y dentro de su propuesta de servicios y soluciones, estos elementos se traducen en efectividad, sencillez y potencia.

Creemos que siempre es necesaria una combinación de productos y servicios basados en una propuesta 100% en la nube. De hecho, hemos sido pioneros en todo el desarrollo de soluciones de ciberseguridad nativas en nube; y damos respuesta para mantener a nuestros clientes libres de amenazas y minimizar el riesgo de exposición. Por tanto, podemos concentrar esta diferenciación en tres pilares: prevención a partir de reducir la superficie de ataque basada en un modelo Zero trust, con el cual vamos catalogando aplicaciones y no dejamos que se ejecute ningún proceso que no consideramos bueno o que no conocemos hasta que realmente no lo catalogamos. Por otro lado, investigación continua y proactiva de amenazas, más allá de toda la parte de malware y los ficheros que pueden entrar a partir de una brecha de seguridad, hacemos un hunting proactivo anticipándonos a todo lo que puede ocurrir. Y por último, proporcionamos herramientas y plataformas de seguridad que hacen que los clientes sean mucho más efectivos y eficientes con esa mejora en su postura de seguridad. Por tanto, al final tenemos un modelo muy consistente que gracias a todas las tecnologías que aplicamos en la nube basadas en Security Data Analytics, en Inteligencia Artificial, en el modelo de comunidad, de aprendizaje, compartición de Inteligencia... Conseguimos dar una respuesta para toda la parte de prevención, detección de ataques, caza y remediación.

Panda Security es una empresa de canal, ¿cómo es la relación de Cytomic con el canal de distribución?

Cytomic nace con una filosofía 100% canal porque necesitamos a los partners más que nunca. Cuando hablamos de este binomio de productos y servicios avanzados consideramos que, como fabricante, y gracias al expertise que tenemos en nuestro laboratorio, podemos dar un primer nivel de servicio horizontal basado en catalogar todas las aplicaciones y con un servicio de Threat hunting.

Utilizamos además la inteligencia acumulada de muchos años en Panda, dónde almacenamos histórico de datos de 365 días para poder cubrir esa ventana de detección que, a día de hoy, es de más de 100 días. Pero necesitamos de nuestros partners especializado ya que, al fin y al cabo, son ellos los que conocen los procesos del cliente, sus flujos de trabajo, el negocio...

Y cómo aplicar toda esta tecnología en la realidad del cliente. Un ejemplo muy claro es el Threat hunting: nosotros hacemos un primer nivel muy horizontal, en el que gracias a la compartición de inteligencia somos capaces de conocer en cualquier parte del mundo y en tiempo real lo que puede estar pasando. Pero es el partner el que va a saber si estamos ante un comportamiento anómalo, si el hecho de que alguien acceda a una base de datos a las 3 de la mañana es normal o no para el cliente. Entonces, ese servicio especializado lo tiene que dar el partner. Por lo tanto, para nosotros los partners, entendiendo como partners de servicio los que realmente se especializan en la aplicación de la tecnología, son claves para Cytomic ■

“Cytomic ofrece exclusividad, profesionalidad y especialización que se traducen en efectividad, sencillez y potencia.

Más Información:

https://www.pandasecurity.com/business/

Email:

communication@pandasecurity.com