Debates en Newsbook

No habrá paz para los malvados

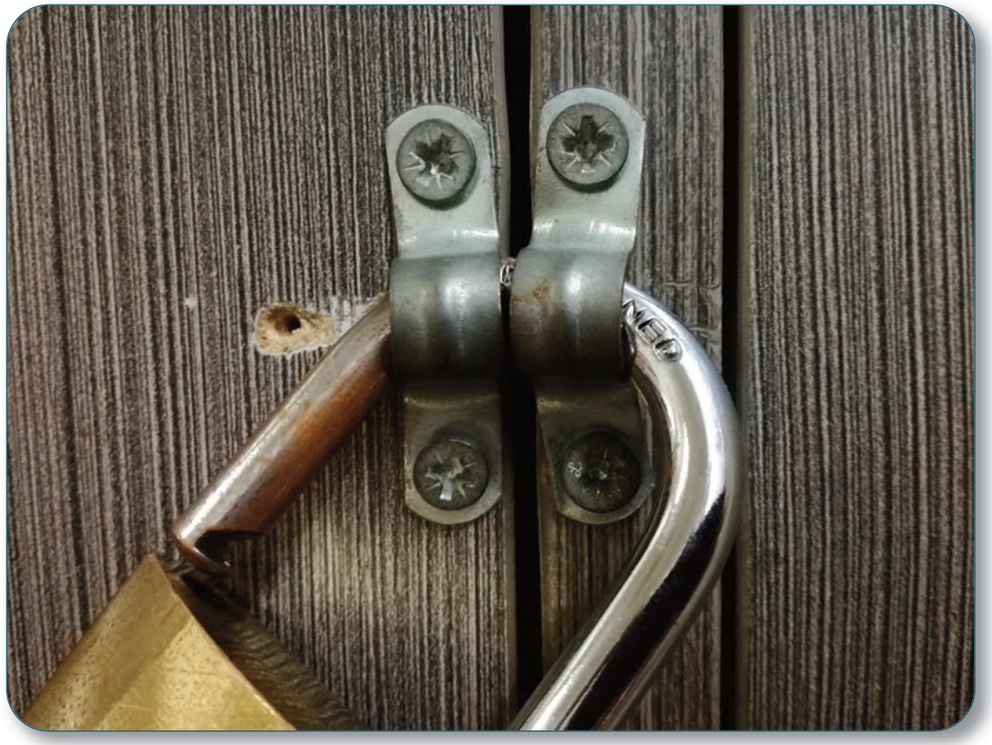
No descansan los *hackers*. Año a año, los malvados de la Red siguen perfeccionando sus técnicas para seguir, incansables, atacando a las empresas para sacar todo el rendimiento posible. Los ciberdelincuentes se han profesionalizado en los últimos tiempos, actuando, incluso en organizaciones cada vez más potentes. Los ataques, cada vez más sofisticados y dirigidos, han crecido, demostrando la "profesionalidad" de los *hackers*. Una escalada de maldad que, afortunadamente, ha ido acompañada de un esfuerzo de la industria de la ciberseguridad en pos de bloquear estos ataques e incrementar la protección de consumidores y empresas. Y no darles paz a los *hackers*.

Siempre el *ransomware*

El *ransomware* sigue siendo la tormenta perfecta para los *hackers*. Se calcula, según Forrester, que el pasado año este tipo de ataques se incrementó en un 500 %, con una clara tendencia hacia el *ransomware* dirigido. En España ha habido sonados ataques, tanto en el sector público como el privado, con Crysis como el *ransomware* más dañino. Según ha publicado Global Security, ha sido el culpable del 40,6 % de los ataques. Se trata de un *ransomware*, detectado en el año 2016, cuya variante tiene la capacidad de cifrar archivos, tanto los almacenados de forma local como aquellos que están en la red; incluyendo también los dispositivos extraíbles. Tras él, se situó GandCrab que a mitad de año, mutó a Sodinokibi. Por último, y famoso por los objetivos que logró, más que por su "difusión", hay que nombrar a Ryuk, responsable de los ataques a la Cadena Ser, Prosegur o el ayuntamiento de Jerez.

Bosco Espinosa de los Monteros, *channel account manager* de Kaspersky, cree que, a pesar de todo, se ha avanzado mucho en la concienciación de los usuarios. "Debemos continuar en esta misma línea ya que, a pesar de ello, las empresas todavía no están invirtiendo todo lo que deberían invertir". Unos ataques que, recuerda, no solo afectan a las pymes, "sino también a las grandes empresas como comprobamos el pasado año en España".

A pesar de la inversión, el *ransomware* va a continuar creciendo. Borja Pérez, director general de Stormshield Iberia, recuerda que las campañas de concienciación que se llevaron a cabo durante los años 2016 y 2017 contribuyeron a aumentar la inversión. "Aunque queda mucho por hacer, ha aumentado la concienciación", corrobora. "Una gran parte de las empresas y de las administraciones públicas se dieron cuenta de que la seguridad afectaba a todo tipo de empresas, cualquiera que fuera su tamaño".



Con los años, los ataques de *ransomware* han incrementado su sofisticación pero, por otro lado, son mucho más sencillos de llevar a cabo y más asequibles de contratar, con un riesgo mínimo para el ciberdelincuente y unos beneficios muy altos. "Los grupos de ciberdelincuentes atacan a las empresas que detectan que son vulnerables", recuerda Ricardo Maté, director general de Sophos Iberia. "Y pagar un rescate no salva de ser atacado de nuevo. Las empresas, si no toman medidas, van a seguir sufriendo ataques", especifica.

Según explica el directivo de Sophos, el incremento de ataques que se está produciendo en España es más elevado que el que exhiben otros países europeos. "Deberíamos reflexionar por qué se están produciendo todos estos ataques en España", valora. "Y con tanto éxito", completa. "Sin duda hay muchísimo por hacer en la empresa".

Ante este panorama, la previsión es, como apunta Daniel Martín, *sales manager* de Panda Security, un crecimiento exponencial de este tipo de ataques. A su juicio, España exhibe un mayor ratio de *ransomware* por la configuración de nuestro tejido empresarial, constituido por una enorme cantidad de pymes, entre las que la concienciación toda-

vía no ha calado en toda su extensión. "Tenemos, por tanto, un reto importante y muchísimo trabajo por hacer".

Brechas y filtraciones de datos

2019 fue también un año especialmente relevante en brechas y filtraciones de datos. En España sonados fueron, por ejemplo, la filtración de datos de los 4,5 millones de usuarios que habían comprado entradas en la Alhambra o, a nivel mundial, la filtración más grande de la historia (1.200 millones de usuarios) de Facebook y Linkedin.

Tras la entrada en vigor el pasado año de la GDPR, la responsabilidad que compete a las empresas que almacenan y gestionan esos datos ha quedado perfectamente regulada; así como las sanciones en el caso de que se produzcan brechas y filtraciones. "Las agencias de protección de datos sí están haciendo su labor y si están abriendo expedientes sancionadores; aunque no todos se hayan hecho públicos", desvela Borja Pérez.

En la lista de los que sí se han desvelado, ya aparecen algunas multas importantes. Quizás los casos más relevantes fueron los que afectaron a British Airways o a Marriot, con sendas multas por encima de los 100 millones de euro; o a Google en Francia, con 50 millones de euros. "Ya hemos comprobado que aquellas empresas que han tenido una brecha de seguridad y no han sido capaces de proteger la información que están almacenando de clientes, usuarios o empleados, los organismos reguladores están empezando a penalizarlo", apunta Ricardo Maté.

Carlos Tortosa, director de canal y de grandes cuentas de Eset, cree que, en materia de protección de datos, en España los usuarios parece que siempre "esperan" la multa. "Somos así. Incluso antes de implementar las soluciones que el propio reglamento, bien aconseja u obliga, esperamos la multa". A su juicio, la empresa española cuenta con un nivel de cumplimiento a las normas más bajo que en otros países europeos.

También hay que apuntar que alguna de las llamadas "brechas de seguridad" tiene su explicación en errores de configuración. Uno de los últimos, reconocido por Microsoft, afectó a 250 millones de usuarios, que vieron publicados sus datos privados.

Ataques de *phishing*

A pesar de ser una de las técnicas maliciosas más tradicionales, el *phishing* sigue cobrándose, año a año, nuevas víctimas. Y aunque no está entre los mecanismos que gozan de mayor complejidad, los maleantes van modificando sus ganchos. El pasado año uno de los métodos de *phishing* más novedoso que identificaron los expertos de Kaspersky fue la utilización de los servicios y sistemas de almacenamiento en la nube para disfrazar los *emails* de *phishing* como

Servicios gestionados

Calculaba IDC que los servicios gestionados supondrían el 50 % de la inversión realizada en ciberseguridad a lo largo del pasado año, en torno a dos áreas: los servicios de integración, necesarios para adaptar las estrategias de ciberseguridad a los nuevos entornos *multicloud*, donde se traslada la protección hacia el dato; y los propios servicios gestionados, en un marco de operación centrado en las nuevas plataformas integrales de ciberseguridad, que deberán complementarse con diversos servicios que en su mayoría estará gestionado por un tercero para ayudar a las organizaciones a optimizar las capacidades y los tiempos de respuesta ante el nuevo mapa de riesgos.

La consultora predijo que más del 50 % de los clientes de servicios de seguridad gestionados incluirán el ciclo de vida de amenazas, en un contexto de confianza cero (*zero trust*) y en el que será imprescindible conocer cómo las nuevas amenazas llegan al dato y se propagan por la red de usuarios haciendo cada vez más difícil su detección. Por todo ello, los nuevos servicios de ciberseguridad deberán consolidarse bajo una plataforma de ciberseguridad que dé cabida a tantos proveedores como sea necesario y que consolide la información para tener una visión global del dato. Un dato que se mueve con libertad en el contexto *multicloud* y que ya no entiende ni de redes ni de dispositivos.

Borja Pérez asegura que el paso a los servicios gestionados va más lento de lo que creía. "Hay distintos niveles de *partners* en relación a su nivel de madurez. Por un lado, hay compañías que ya ofrecían este tipo de servicios antes de que las marcas les ofreciésemos ese modelo", reconoce. Ahora, con una oferta concreta en este apartado, asegura que hay *partners* pequeños que "sorprende lo avanzados que están en este sentido. Sus clientes se lo demandaron hace tiempo y su oferta se adaptó a esa exigencia".

Carlos Tortosa asegura que el suministro de servicios gestionados es una manera de "fidelizar a los clientes a través de un modelo eficaz de suministro de la tecnología"; un modelo que permite al canal ofrecer a sus clientes un servicio que incluya la gestión de soluciones de varias marcas.

Todos los fabricantes disponen de una oferta concreta para facilitar al canal el desarrollo de este tipo de servicios. "Se trata, no de hablar de soluciones concretas, sino de las tecnologías que permitan al distribuidor ofrecerlo a sus clientes", explica Espinosa de los Monteros. El directivo de Kaspersky tiene grandes esperanzas puestas en el desarrollo de este modelo en 2020. "Puede ser un *boom*", prevé. "El año pasado sembramos y educamos al canal, poniendo a su disposición las herramientas adecuadas para permitirlos el despliegue del servicio".

mensajes auténticos. Al incluir en el *email* un enlace con un dominio legítimo, por ejemplo, de Google Drive, el mensaje genera mayor confianza en el usuario y además evita la detección por los filtros de *spam*. También los ciberdelincuentes enviaron enlaces de *phishing* dentro de falsas convocatorias para eventos, enviadas a través de Google Calendar, o imágenes a través de Google Photos acompañados por una petición de ingresar una comisión en una cuenta bancaria, a cambio de recibir una transferencia de una gran suma de dinero.

Asimismo, los defraudadores aprovecharon la campaña de la Renta para atraer a los usuarios a webs falsas con la promesa de abonar la devolución de los impuestos. Otro gancho fue Instagram: los malean-tes, aprovechando su popularidad, la utilizaron como herramienta para lanzar sus ataques.

"La curiosidad de los usuarios sigue siendo muy elevada y además están convencidos de que la empresa en la que trabajan ya se encargará de poner las medidas adecuadas", recuerda Bosco Espinosa de los

Monteros, para quien la explicación a la efectividad que tiene esta técnica reside en el "ROI" tan elevado que permite a los ciberdelincuentes. "Si se quiere atacar a una empresa, sólo se necesita hacer un perfilado; una tarea que, observando la actividad que tienen los usuarios en las redes sociales, es sencilla". Como recuerda Carlos Tortosa, apenas existen ataques de *phishing* avanzados, ahora bien, puntualiza, lo que sí se está produciendo es una "mejora" en la ejecución. "Hay correos en los que se está suplantando el idioma de escritura, lo que complica detectar que se trata de un *phishing*". Los ciberdelincuentes cuidan, por tanto, la apariencia del correo para tratar de concederle el mejor disfraz posible. "Al igual que existen amenazas persistentes, hay usuarios persistentes", insiste Borja Pérez que reconoce que los maleantes cuidan, cada vez más, el "contenido" de los correos para engañar a los usuarios. "Es un problema complejo y va a seguir creciendo: es sencillo de ejecutar y cada vez es más complicado distinguirlos".

El *malware* móvil: la amenaza fantasma

A pesar de que se habla, insistentemente, de la "falta" de perímetro y de la necesidad de extender la seguridad a todos y cada uno de los dispositivos, la seguridad de los dispositivos móviles sigue siendo la asignatura pendiente. Según un estudio de Eset, en 2019 Android cerró con menos detecciones y vulnerabilidades, mientras que las detecciones de *malware* para iOS crecieron un 98 %. Carlos Tortosa reconoce que la protección ha crecido, ahora bien, no suficientemente. "Quizás debamos ser mejores divulgadores para concienciar a los usuarios de la necesidad de proteger el dispositivo".

Daniel Martín asegura que, tras el *boom* que hubo hace unos años en torno a la protección de los dispositivos móviles, "ha existido un estancamiento en la implantación de soluciones de seguridad en este entorno".

Precisamente Panda Security alertaba acerca de la necesidad de actualizar las aplicaciones que tenemos en el teléfono móvil para evitar que los *hackers* utilicen esa laxitud para atacar. Según la multinacional, una de cada dos incidencias relacionadas con la ciberseguridad en teléfonos móviles se produce por brechas de seguridad en sus *apps*: muchos usuarios deciden no instalar las últimas versiones porque saturan la memoria de sus teléfonos. Incluso hay usuarios que bloquean su actualización automática.

Unas vulnerabilidades en las aplicaciones que no solo afectan a la vida personal de sus usuarios: el riesgo se multiplica si los usuarios colaboran con compañeros o con personas de otras organizaciones: si un móvil está infectado por un código malicioso, este podría propagarse entre los miembros de un pequeño equipo de trabajo o incluso saltar a toda una organización. Según los datos de Panda Security, uno de cada cinco empleados causará una bre-

cha de seguridad a su empresa por el mal uso de su teléfono móvil en los próximos años.

¿En qué áreas está invirtiendo más las empresas españolas?

El mercado de la ciberseguridad mantuvo su tendencia alcista en España a lo largo del pasado 2019. Según calcula IDC, movió una cifra cercana a los 1.307 millones de euros, lo que supuso un crecimiento del 7 %. Una tendencia alcista en la inversión en ciberseguridad que se mantendrá durante los 3 próximos años, alcanzando un crecimiento sostenido entre 2019 y 2022 del 7,1 % (CAGR).

Según el estudio Hiscox Cyber Readiness Report elaborado por Hiscox a nivel internacional, donde se analiza la ciberpreparación de más de 5.000 compañías del tejido empresarial de 7 países: España, EEUU, Gran Bretaña, Alemania, Holanda, Francia y Bélgica; España era el tercer país con la mayor previsión de inversión en ciberseguridad: el 67 % de las empresas iba a aumentar su presupuesto en 2019, seis puntos más que en 2018.

Ricardo Maté reconoce que en España se está invirtiendo en ciberseguridad y que su crecimiento está muy por encima de cualquier otro mercado. "Sin embargo, no es suficiente: haría falta invertir mucho más, porque el *gap* que hay todavía es muy alto", analiza. Todos están de acuerdo en que la situación de la gran cuenta es muy diferente a la que exhibe la pyme. Asegura Maté que la protección debe considerarse como un todo. No en vano, la marca desveló en su Sophos Day que el 90 % de las empresas que había sufrido un ataque contaba con soluciones tradicionales de seguridad. "No vale con proteger diferentes componentes, sino diseñar una seguridad completa que comprenda la protección de los puestos de trabajo, los servidores, los dispositivos móviles, el correo, las redes, las cargas que están en nube, etc.". A su juicio, sobre todo son las pymes las que tienen que empezar a verlo como "una solución completa de su entorno de ciberseguridad".

> "A pesar de ser una de las técnicas maliciosas más tradicionales, el *phishing* sigue cobrándose, año a año, nuevas víctimas"

Una pyme que, en muchos casos, está externalizando su servicio de seguridad, con un soporte plenamente profesional. "Las empresas están invirtiendo en soluciones que les permitan protegerse de las amenazas persistentes", recuerda Carlos Tortosa. "Es esencial, además, la protección en sí del propio dato con soluciones de cifrado o las tradicionales DLP". Por último, también crecerá la inversión "en torno a la autenticación del usuario o a la identificación para acceder a redes".

En este entorno de la pyme, Borja Pérez recuerda lo importante que es el canal. "El departamento de TI de la pyme es su canal", opina. "Es el encargado de proponerle soluciones al cliente". Un soporte que, a su juicio, también se está extendiendo a las grandes cuentas que, en muchos casos, externalizan servicios o cuentan con departamentos de TI cada vez más pequeños. Ahora bien, grandes o pequeñas, el máximo responsable de Stormshield en España recuerda que cualquier política de seguridad de cualquier empresa, lo primero con lo que tiene que contar es con un *backup* correcto. "Después se implantan las soluciones propias de seguridad".

Un canal que, a juicio de Daniel Martín, debe cumplir con la premisa de la especialización. "Es la clave para que se posicione como un consultor de cara a sus clientes", continúa.

A pesar de que el recorrido de la pyme en el campo de la seguridad debe ser mayor, Espinosa de los Monteros asegura que en muchos casos ya ha dado un paso más en su seguridad; "algo más lento por la capacidad de inversión", eso sí. "Ha pasado de usar un software, en algunos casos casi gratuitos, o

soluciones muy tradicionales a soluciones más avanzadas, basadas en reputación en la nube, en *machine learning*, en listas de reputación y que no solo son *antimalware*", relata. "Ahora bien, hay que seguir avanzando".

El "retorno" al *endpoint*

La personalidad de las amenazas, con el *ransomware* como principal punta de lanza, ha permitido devolver al entorno del puesto de trabajo la importancia que siempre debió tener. Según la consultora Gartner, el crecimiento previsto para 2019 era de un 7 %. Se trata de un apartado "atestado", en el que han aparecido nuevos jugadores junto a otros, más tradicionales, que han intensificado su propuesta en este apartado.

La mayor parte de las marcas cuenta con soluciones específicas para este entorno, que exhiben distintas filosofías. Las tradicionales soluciones de EDP (*Endpoint Detection and Protection*) ya añaden funcionalidades de EDR (*Endpoint Detection and Response*). Igualmente existen soluciones puras de EDR. Dos vías de desarrollo, que tienden a fusionarse, a pesar de que la consultora Gartner las distingue en su cuadrante mágico. Muy pocas áreas tecnológicas, además, cuenta con tantos fabricantes y tantas tecnologías.

A juicio de Daniel Martín el crecimiento del 7 % que pronosticaba Gartner para este segmento el pasado año, se queda muy corto para las expectativas en España. "En el entorno del *endpoint*, todas las nuevas oportunidades de negocio están vinculadas a la tecnología EDR, ya que ha crecido la concienciación y las empresas son consciente de que es necesario una protección más completa", asegura.

El camino en España exhibe un mayor recorrido que en otros países. Sophos llevó a cabo una encuesta a 3.200 empresas a nivel mundial (el 50 % ubicadas en los Estados Unidos), en la que el 50 % de las mismas aseguraba que ya contaba con una solución EDR. Ricardo Maté recuerda que la situación en España es radicalmente distinta. "En el mercado español estamos todavía muy lejos de ese porcentaje por lo que los crecimientos tienen que ser sensiblemente superiores a los que marcan el mercado mundial", prevé. "Prácticamente todas las nuevas operaciones que hacemos en clientes que cuentan con más de 100 usuarios incluyen soluciones EDR".

Seguridad en la nube, el gran reto

Casi un 20 % de las empresas sufrió algún tipo de incidente de seguridad en la nube en 2019. Dos son los mayores riesgos: la configuración incorrecta de la plataforma *cloud* y, sobre todo, una incorrecta política de gestión de identidades. Ahora bien, como asegura Espinosa de los Monteros, es un entorno que no es ni más ni menos seguro. "Depende de las medidas que se tomen y de los *partners* que elija la compañía para diseñar la protección de ese entorno".

La subida de cargas a la nube va más allá de la seguridad. Como bien recuerda Maté, han "surgido" mu-

chas compañías, algunas de ellas grandes integradores y otras más pequeñas con un alto grado de especialización en la labor de elevar a las empresas a la nube. "Una tarea que requiere consultoría, definir perfectamente qué necesitan, cómo hacerlo, qué cargas de trabajo se llevan a este entorno, sobre qué infraestructura y qué aplicaciones", enumera. Maté alerta, entre otros ámbitos, sobre la seguridad que deben tener estas últimas. En la actualidad hay, según IDC, 500 millones de aplicaciones disponibles en el mercado; un número que se va a duplicar en los próximos tres años, lo que exige una capacidad y una velocidad de desarrollo brutal. "Muchas empresas están desarrollando aplicaciones a una enorme velocidad sin tener en cuenta el componente de seguridad", alerta. Para un desarrollador, lo prioritario es tener disponible la aplicación, no la seguridad que ésta debe integrar. "Es primordial proteger todos los entornos de desarrollo que están en la nube, lo que obliga a desplegar las herramientas que permiten su protección".

Otro área clave es la identificación de los usuarios. "Es una necesidad", insiste Carlos Tortosa. "Hasta cierto punto, hacerse pasar por un tercero gracias a un ataque de fuerza bruta permite acceder a datos e informaciones críticas para las empresas", alerta. El directivo de Eset insiste en la necesidad de asegurar la identificación y autenticación de los usuarios.

La oportunidad para el canal está clara. "Es enorme", insiste Daniel Martín. "Aunque queda muchísimo trabajo por hacer", especifica. "Es importante elevar a la nube los servicios de seguridad de los que las empresas disfrutan en el puesto de trabajo", alerta. "A pesar de que es necesario, no podemos quedarnos solo en el clásico *backup*, ni confiar únicamente en la seguridad que pueda proporcionarnos el proveedor *cloud* que tenga la empresa".

> "Según calcula IDC, el mercado de la seguridad movió una cifra cercana a los 1.307 millones de euros, lo que supuso un crecimiento del 7 %"

Recomendaciones al distribuidor

"El *partner* tiene que tener una visión 360", recomienda Carlos Tortosa. "No se puede centrar únicamente en el producto que está acostumbrado a vender, que no le resulta complicado de configurar, o focalizarse únicamente en el cliente que no le da problemas", continúa. "El canal debería ser capaz de abarcar cualquier tipo de cliente; lo que le exige, eso sí, un conocimiento completo de la oferta". Para ello, puntualiza, cuenta con el apoyo de la marca, en este caso de Eset. "Es vital que ofrezca siempre una solución completa".

La especialización es básica. "Estamos en un entorno que gira en torno al servicio y al valor", apunta Daniel Martín. "La reventa está muerta", continúa. "La enorme complejidad que tiene la seguridad para el cliente final exige al canal especializarse y acompañarle como consultor y ser un asesor que le dé confianza".

Se trata, en definitiva, de llevar a cabo una venta consultiva. "De lo contrario va a dejar agujeros de seguridad", alerta Espinosa de los Monteros. "Es fundamental asegurar que el canal esté suficientemente preparado para ofrecer este servicio".

Ahora bien, es clave aliarse con las compañías adecuadas. "El integrador debe elegir muy bien a los fabricantes que nutran su oferta", alerta Ricardo Maté. "Hoy en día no todas las tecnologías valen, ni todos los fabricantes tienen el mismo nivel, ni ofrecen una solución completa de ciberseguridad", explica. "Muchos *partners* están vendiendo un SIMO: solo distribuyen productos y no venden valor".

La oportunidad sigue siendo enorme. Y, como remata Borja Pérez, exige al distribuidor dos premisas. "Formación y especialización".

"El canal, ante el reto de la seguridad en 2020"

2´ 43". El *ransomware* sigue siendo la tormenta perfecta para los *hackers*. En 2019 hubo sonados ataques en España, tanto en el sector público como en el privado. ¿Qué nos espera en 2020 en torno a esta amenaza?

11´ 20". No hay duda de que 2019 ha sido un año especialmente relevante en brechas y filtraciones de datos. ¿Seguirá así este año? ¿Qué falla?

20´ 42". Junto a ellos, los ataques de *phishing* siguen manteniendo su posición. ¿Qué técnicas se están utilizando para provocar que una y otra vez los usuarios "piquen"?

29´ 40". Incremento del *malware* móvil. ¿Por qué sigue sin despegar la protección móvil?

33´ 07". ¿En qué áreas están invirtiendo más las empresas españolas?

42´ 53". ¿Cuál es la participación del canal en el desarrollo de los servicios gestionados?

50´ 37". El "retorno" al *endpoint*. ¿Qué estrategias sigue cada una de las marcas en este apartado?

1 hora 24". La seguridad en el *cloud*. ¿Está el canal haciendo una adecuada política de evangelización de sus clientes en este apartado?

1 hora 8´ 44 ". ¿Es este entorno *cloud* la mayor oportunidad que tiene el canal?

1 hora 12´ 10". Seguridad en los entornos industriales

1 hora 20´ 24". Recomendaciones al distribuidor

"El mercado de la ciberseguridad seguirá creciendo en los próximos años"

La inversión en las herramientas que aseguren a las empresas una adecuada protección de sus sistemas seguirá creciendo en los próximos años. Carlos Tortosa, director de grandes cuentas y canal en Eset, asegura que uno de los entornos de inversión será el *endpoint*, con la inclusión de soluciones que incorporen tecnologías de EDR. Junto a él, la protección del dato es otro apartado clave que debe ser observado como una gran oportunidad. "Hay que contar con soluciones de cifrado y de DLP", recomienda.

VER VÍDEO

Carlos Tortosa, director de grandes cuentas y canal en **Eset**

"La especialización del *partner* es fundamental para Kaspersky"

El canal es un socio de confianza para los clientes. Bosco Espinosa de los Monteros, *channel account manager* de Kasperky, recuerda el papel fundamental que tiene el canal en el negocio de la compañía, con especial incidencia en que se especialice.

La marca estrenó el pasado año un nuevo programa de canal, Kaspersky United, que, exhibía, precisamente la especialización como materia troncal y que buscaba mantener la fidelidad del canal a través de la rentabilidad.

kaspersky

VER VÍDEO

Bosco Espinosa de los Monteros, *channel account manager* de **Kasperky**

"La protección de los dispositivos móviles, que no crece al ritmo que debería, señala un apartado de oportunidad"

Tres son las áreas de oportunidad que señala Daniel Martín, *sales manager* de Panda Security, para que puedan ser aprovechadas por el canal de distribución de la marca en el campo de la seguridad. Las soluciones orientadas a evitar la suplantación de identidad que, desde el correo, también empezarán a darse en las redes sociales. La protección de los dispositivos móviles, que no crece al ritmo que debería, señala otro apartado de oportunidad. Y, por último, los ciberseguros.

VER VÍDEO

Daniel Martín, *sales manager* de **Panda Security**

"Hay muchas oportunidades de negocio para los *partners* de Sophos"

Ricardo Maté, director general de Sophos Iberia, asegura que en 2020 las oportunidades de negocio en el mercado de la seguridad para el canal de distribución de la marca son enormes. Y en todo tipo de entornos. Maté recuerda la necesidad de protección que hay en el entorno del puesto de trabajo. "El punto de entrada de todas las amenazas es el correo y hay una enorme oportunidad, por ejemplo, en el entorno del Office 365", identifica. No olvida su vinculación con la necesaria concienciación de los usuarios; ni la necesaria protección de la red, con la nueva versión 18 de su *firewall*, "que ofrece nuevas funcionalidades".

VER VÍDEO

Ricardo Maté, director general de **Sophos** Iberia

SOPHOS

La protección de las infraestructuras críticas, foco para Stormshield

En este 2020 se vislumbran importantes oportunidades para el canal de las marcas de seguridad. Stormshield no es una excepción. Borja Pérez, director general de Stormshield Iberia, señala que es muy importante que sus *partners* desarrollen el mercado de la protección de todas aquellas empresas que cuentan con infraestructuras críticas. Junto a ella, las soluciones de seguridad en torno al cifrado de datos, unido a Office 365 y a las soluciones de correo, junto al cumplimiento del GDPR, abren otras vías de oportunidad.

STORMSHIELD

VER VÍDEO

Borja Pérez, director general de **Stormshield** Iberia