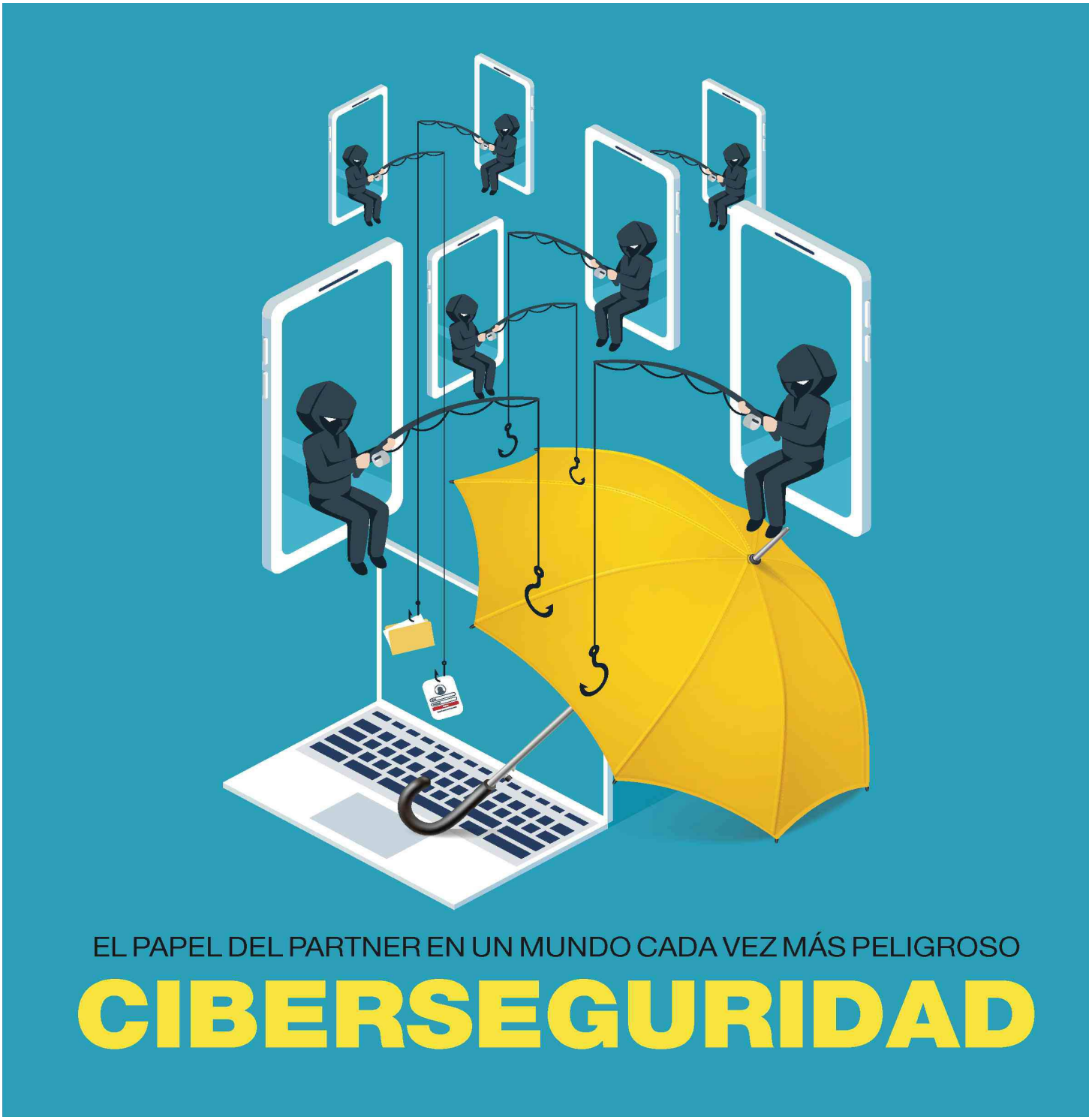
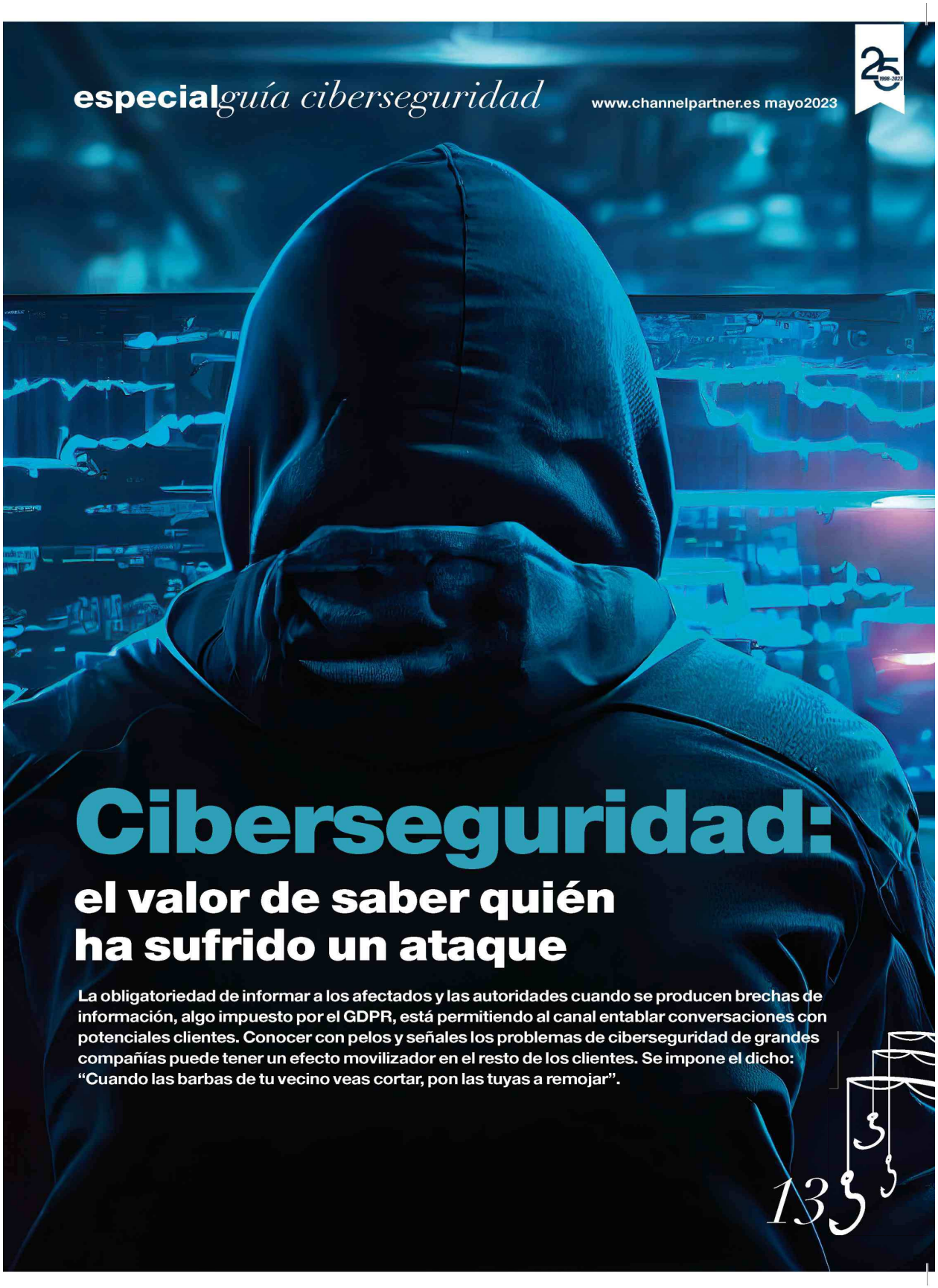
Publicación	Channel Partner General, 1	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	455,60 cm² (73,1%)
Audiencia	25 500	V.Publicitario	2933 EUR (3234 USD)



Channel PARTNER

Publicación	Channel Partner General, 13	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	570,39 cm² (91,5%)
Audiencia	25 500	V.Publicitario	3440 EUR (3793 USD)

UNION PROFESIONAL



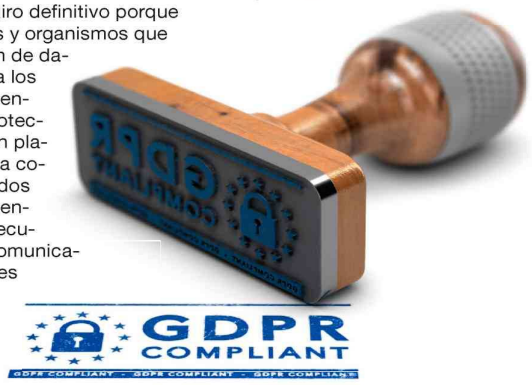
Channel Partner

Publicación	Channel Partner General, 14	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	552,91 cm² (88,7%)
Audiencia	25 500	V.Publicitario	3363 EUR (3708 USD)

Las cifras de ataques y de incidencia de la ciberdelincuencia asustan. Y las referidas a España todavía más. Para muestra, algunos de los titulares de prensa aparecidos en este país en los últimos meses: "España, el tercer país del mundo con más ciberataques a empresas"; "España, el cuarto país europeo con más ciberataques al sector industrial"; "Las instituciones públicas, la investigación y la educación, en el punto de mira de los ciberataques en España en 2022"; "España es el séptimo país más ciberatacado por ransomware en 2022"… Como dice un fabricante de ciberseguridad basándose en un estudio interno, las cosas "van a peor" en este mundo de la seguridad informática porque cada vez las empresas tienen que cubrir un área de ataque mayor (sobre todo después de la popularización del trabajo en remoto), cada vez tenemos más dispositivos y cada vez la infraestructura de una compañía es más compleja y variada (el cloud es el último capítulo). Es decir, es lógico que se multipliquen las amenazas y los ataques, y el daño que causan. Era una evolución esperable. Lo que no era tan esperable hace un tiempo es que a estas alturas supiéramos las entidades y empresas concretas que sufren sustracciones y cifrados malintencionados de su información. En este ámbito sí que ha habido un cambio de tercio. Hace unos años era un secreto a voces que las grandes compañías de servicios públicos o los bancos podían estar sufriendo ataques, pero nada trascendía. Sin embargo, la entrada plenamente en vigor, en mayo de 2018, del GDPR (siglas del Reglamento General de Protección de Datos de la Unión Europea) supuso en giro definitivo porque obliga a compañías y organismos que sufren una filtración de datos a comunicarlo a los afectados y a la Agencia Española de Protección de Datos en un plazo de 72 horas. Si la comunidad de afectados es muy amplia, las entidades atacadas recurren a medios de comunicación o redes sociales para informar de lo que ha pasado, de las implicaciones que tiene para los clientes o de las recomendaciones a seguir por estos para minimizar los efectos del ataque, tal como prescribe el GDPR.

Abrir el debate es más fácil

En consecuencia, los medios de comunicación se han poblado en los dos últimos años de informaciones donde entidades con nombres y apellidos dan cuenta de amenazas y ataques que las llegan a paralizar y que provocan el consecuente daño reputacional. Pero no está claro hasta qué punto fabricantes y partners especializados en ciberseguridad están aprovechando este torrente de información para incrementar la conciencia de los clientes e incluso iniciar un proceso de venta. Los hay que agradecen estas noticias porque sirven para "abrir el debate", como **Isabel López, sales ingineer manager de Samsung**. También hay quien asegura que en el momento en que sale la noticia de un ataque todo el mundo habla y se preocupa, pero luego el efecto pasa y todo se olvida rápidamente. Es el caso de **Álvaro Fraile, director del centro de excelencia de ciberseguridad de Ibermática**. Aunque Fraile anima al canal a estar al tanto de todo lo que pasa a nivel de ataques, porque cuando hay que hacerle una propuesta a un cliente del mismo sector que la empresa afectada, es más fácil convencerlo. "Los clientes tienen que saber que estos ataques existen y les pueden pasar. Hay que hacer que el cliente tenga la mosca detrás de la oreja. Que se pregunte: ¿Y si me pasa a mí?". Se impone el dicho: "Cuando las barbas de tu vecino veas cortar, pon las tuyas a remojar". ■



Cuando la seguridad se rompe

En este reportaje hemos querido rescatar los ciberataques más significativos ocurridos en España desde principios de 2021. Sorprende la variedad de tipos de compañías y entidades que los han sufrido. Pero, en líneas generales, se puede decir que los delincuentes se han cebado con los hospitales, incluso cuando estaban contra las cuerdas en el peor momento de la pandemia, y con organismos públicos, bancos, entidades de investigación, operadoras, bancos, aseguradoras y firmas de energía. En fin, con todo aquel que atesora grandes registros de datos de clientes, e información confidencial y atractiva de cada uno de ellos.

SEPE: marzo 2021

El ataque al Servicio Público de Empleo (SEPE) supuso un antes y un después. Por su magnitud, al provocar que centenares de miles de citas sufrieran retrasos y que miles de personas tuvieran que esperar más de la cuenta por sus prestaciones de desempleo. El causante del desaguisado: el ransomware Ryuk, un viejo conocido que lleva años causando problemas a las empresas.

Glovo: abril 2021

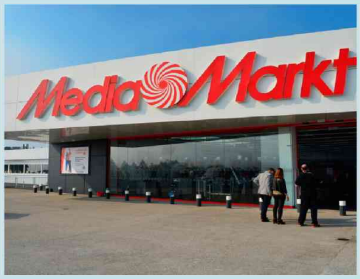
La firma española de reparto a domicilio hizo público el 29 de abril que había sufrido un acceso no autorizado a sus sistemas. Se llevó a publicar que el hacker había puesto en venta en internet los datos bancarios de clientes y repartidores. Al final no hubo tal revelación, pero sí se supo que los datos sensibles no estaban cifrados de forma correcta.

Channel PARTNER

Publicación	Channel Partner General, 15	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	551,98 cm² (88,6%)
Audiencia	25 500	V.Publicitario	3359 EUR (3704 USD)

Phone House: abril 2021

Fue otro bombazo en la primavera de 2021, un tiempo en el que la pandemia de Covid acaparaba buena parte de la atención informativa. La cadena de tiendas de telefonía sufrió un ataque que dejó al descubierto datos sensibles de millones de clientes. Los delincuentes aseguraban que se habían hecho con información de más de tres millones de personas. Y pedían un rescate por la misma.



MediaMarkt: noviembre 2021

En plena preparación de la campaña de Black Friday, momento culminante para el sector del comercio, el gigante MediaMarkt sufrió un ataque de ransomware que bloqueó sus servidores. Más de 3.000 equipos con Windows se vieron afectados. Entre ellos muchos servidores y las TPV conectadas a los mismos. Tuvieron problemas tiendas de España, Alemania, Bélgica y Holanda.

Hospital de Lucena: enero 2022

El Hospital Centro de Andalucía, en Lucena (Córdoba), vio como miles de datos de sus pacientes quedaban expuestos debido a un ataque de ransomware. El centro sanitario lo denunció a la Policía Nacional y se puso en manos de Telefónica para resolver el incidente.

Hospital Vall d´Hebron: febrero 2022

En este caso los hackers se hicieron con datos de ensayos clínicos y amenazaron con divulgarlos. Para ello atacaron la división de investigación del centro: el Vall d'Hebron Research Institute (VHIR).

Iberdrola: marzo 2022

En la primavera del pasado año cayeron en manos de ciberdelincuentes los datos de 1,3 millones de clientes de la eléctrica Iberdrola. Según la compañía, accedieron a datos personales como nombres y apellidos, DNI, domicilio o número de teléfono, pero no a datos bancarios o de cifras de consumo de eléctrico.

Ayuntamientos de Navarra: mayo 2022

Hasta 137 ayuntamientos de Navarra tuvieron que volver al papel debido a un ataque informático que duró varias semanas. El ciberataque provino de un servidor ubicado en Lituania y también fue del tipo ransomware. Provocó caídas de servicios, como páginas web, correos y sedes electrónicas.

CSIC: julio 2022

El Consejo Superior de Investigaciones Científicas (CSIC) fue víctima de un ciberataque de ransomware que lo tuvo dos semanas sin conexión a Internet. El origen del ataque estaba en Rusia.

Laboral Kutxa: mayo 2022

Laboral Kutxa comunicaba a finales de mes que había conseguido bloquear un ciberataque que había afectado a sus sistemas informáticos, y en concreto a su servicio de intercambio de documentos con los clientes.

Glovo: julio 2022

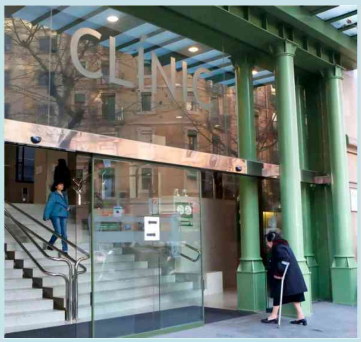
Glovo volvió a los titulares en el verano de 2022. Se filtraron datos de más de cinco millones de clientes y 37.000 repartidores de la compañía fundada en Barcelona en 2015, y se pusieron a la venta en la dark web.

Telefónica: octubre 2022

La operadora informó de que había sufrido un ataque que dejó al descubierto y comprometió millones de contraseñas de los routers de los usuarios residenciales y empresariales. La compañía alertó a los clientes y les envió un aviso para actualizar las passwords de estos aparatos.

Holaluz: noviembre 2022

La compañía de energía eléctrica de origen renovable sufrió un acceso no autorizado a sus sistemas que afectó a algunos clientes y datos sensibles, según comunicó la propia firma a las autoridades.



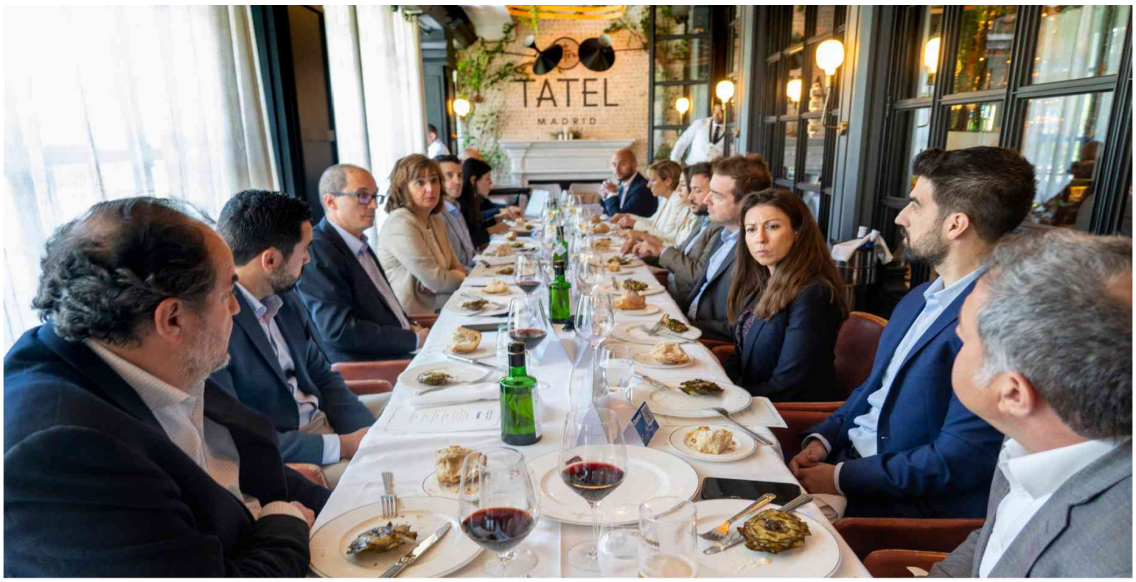
Hospital Clínic de Barcelona: marzo 2023

Ha sido el último incidente grave y mediático. Este centro hospitalario sufrió el pasado 5 de marzo un ataque de ransomware que logró encriptar sus sistemas. En consecuencia, se cancelaron servicios de urgencia, laboratorios y farmacia. Y se dejaron de hacer miles de análisis a pacientes ambulatorios y cientos de intervenciones. Además, el centro reconoció al cabo de las semanas que la confidencialidad de los datos personales de los pacientes estaba comprometida.

Channel PARTNER

Publicación	Channel Partner General, 16	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	536,53 cm² (86,0%)
Audiencia	25 500	V.Publicitario	3290 EUR (3628 USD)

UNIÓN PROFESIONAL



CHANNEL PARTNER reúne a una docena de expertos en ciberseguridad

El partner de seguridad clave para defender a los clientes en un mundo cada vez más complejo

La ciberseguridad es uno de los mercados tecnológicos que más avanza en los últimos años. En España, y según previsiones iniciales de IDC, movió casi 1.750 millones de euros en 2022. Y en 2025 podría superar la barrera de los 2.200 millones, lo que supone que cada año tendrá un ritmo de crecimiento cercano al doble dígito (10%). Las principales áreas de inversión son la gestión unificada de amenazas, la integración de sistemas y los servicios de externalización de redes y endpoint. En las pymes, la prioridad es la protección del dispositivo.

Juan Cabrera

Hoy las empresas de cualquier tamaño empiezan a ser conscientes de que van a ser atacadas en algún momento, y de que deberán estar preparadas para ello. El phishing o la extorsión por ransomware están a la orden del día. Además, la obligatoriedad de informar a las víctimas de robo de información, establecida por el GDPR, está permitiendo airear ataques un día sí y otro también. Ataques, además, que afectan a miles e incluso millones de usuarios de a pie, como el reciente del Hospital Clínic de Barcelona o el que a principios de 2021 sufrió el SEPE y que paralizó 700 oficinas y obligó a los técnicos del servicio público a trabajar 19.000 horas extra para subsanar los problemas. El escenario es pues luminoso para los fabricantes y canales dedicados a llevar la ciberseguridad a compañías y administraciones públicas de este país. Aunque también se enfrentan a retos importantes, como la falta de talento para llevar a cabo las implantaciones de esta tecnología, la falta de cultura en ciberseguridad de los empleados, que son la puerta de entrada de los ciberdelincuentes en la mayor parte de los casos, o el escaso aprovechamiento que hacen los propios clientes de la tecnología de protección que han adquirido, y que muchas veces está desactualizada. De todo ello hablaron los fabricantes, mayoristas e integradores reunidos por CHANNEL PARTNER en torno a una mesa. Expertos en negocio, pero también en tecnología y en aspectos legales, puesto que ciberseguridad y legislación se dan la mano en muchos momentos, sobre todo a la hora de que las compañías aborden las exigencias regulatorias de su mercado (compliance).

Phishing y ransomware son las principales amenazas

Paul Canales, responsable del canal en Iberia de HornetSecurity, aseguró que las amenazas que más preocupan hoy a las empresas españolas son el phishing y ransomware. Y se refirió al empleado como el eslabón más débil de la cadena de protección: "Podemos poner barreras pa-

Channel PARTNER

Publicación	Channel Partner General, 17	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	533,23 cm² (85,5%)
Audiencia	25 500	V.Publicitario	3276 EUR (3612 USD)

UNION PROFESIONAL

1. Marisol Bauzá (Azuba); **2. Esther Santiago** (Bravent); **3 Elena Lim** (Cipher); **4. Daniel López** (Evolutio); **5. David López** (Factum IT); **6. Paul Canales** (Hornetsecurity); **7. Álvaro Fraile** (Ibermática); **8. Isabel López** (Samsung); **9. Juan Manuel Valiente** (Secure & IT); **10. Sergio Martínez** (SonicWall); **11. David Gasca** (V-Valley); **12. Enrique Delgado** (Zertia); **13. Ruperto García-Soto** (Zyxel).

ra evitarlo, pero al final es la persona que recibe el correo la que pincha en el lugar equivocado. Y por eso la concienciación de los empleados en materia de ciberseguridad será un elemento clave este año. Muchas empresas están preguntándose ahora cómo explican a sus plantillas lo qué es bueno y malo". **David Gasca, responsable de ventas y marketing del área de ciberseguridad de V-Valley**, coincidió con el diagnóstico de que el mayor problema hoy está en la falta de concienciación de los empleados. Y añadió el de las implantaciones deficientes: "Muchas empresas tienen la tecnología para protegerse, pero no están implementadas correctamente". Gasca también señaló como reto la falta de profesionales cualificados en el sector. Y dijo que el cliente tiene en el canal al mejor aliado para dar respuesta a todas estas dificultades. "Los clientes tienen que pasar de contar con un informático que se dedica, entre otras cosas, a la seguridad, a tener una empresa especializada que aborde estas cuestiones". Para **Sergio Martínez, manager en Iberia de SonicWall,** las cosas "van a peor" en el mundo de la ciberseguridad porque hoy empresas y usuarios se enfrentan a una infraestructura tecnológica mucho más compleja que en el pasado. "Ahora no vamos en una moto pequeña, sino que vamos en una moto de gran cilindrada. Cada vez estamos más expuestos porque cada vez hay más dispositivos conectados". **Marisol Bauzá, CEO de Azuba**, recordó que el ransomware y los ataques en general se han "industrializado". "Esto ha llevado a las empresas a estar analizando continuamente su superficie de ataque, que cada vez es mayor. Los CISO se ven desbordados porque tienen que proteger miles de dispositivos. Por eso necesitan herramientas de automatización". Y explicó que incluso hay estados que son hackers y que, contra eso, sólo se puede oponer "una supervisión permanente".

Desprotección de los dispositivos móviles

Por su parte, **Isabel López, sales engineer manager de Samsung**, insistió en la dificultad que supone que no haya profesionales con conocimientos suficientes para desplegar mucha tecnología y servicios de ciberseguridad en las empresas. Y se refirió a la desprotección habitual de los teléfonos móviles. "En el ámbito de la movilidad, también faltan profesionales que sepan aplicar políticas. Con el móvil accedemos a mucha información confidencial. Solemos darle a aceptar permisos de muchas aplicaciones y no nos planteamos por qué. Sin embargo, no tenemos software de protección y políticas que garanticen la información confidencial. En este sentido, nuestros móviles vienen de fábrica con la plataforma de seguridad Knox", explicó. **Juan Manuel Valiente, responsable del área jurídica del integrador Secure & IT,** coincidió en señalar el ransomware y los despistes de los propios empleados como los mayores quebraderos de cabeza para los profesionales de la ciberseguridad. "Las labores de sensibilización y concienciación son totalmente necesarias. Para que los usuarios sepan qué hacer y qué no hacer". **Esther Santiago, sales manager de Bravent,** se refirió a ChatGPT para advertir de que la información que sube una empresa a esta plataforma de inteligencia artificial pasa a ser de la misma, y que por eso conviene extremar la precaución sobre la confidencialidad de los datos que se comparten. **Elena Lim, manager de ventas globales por canal de Cipher,** insistió en la falta concienciación de los empleados y la escasez de talento como los dos grandes retos a los que se enfrenta el sector en estos momentos. "El software es ilimitado, pero la capacidad de implantarlo es limitada, porque requiere

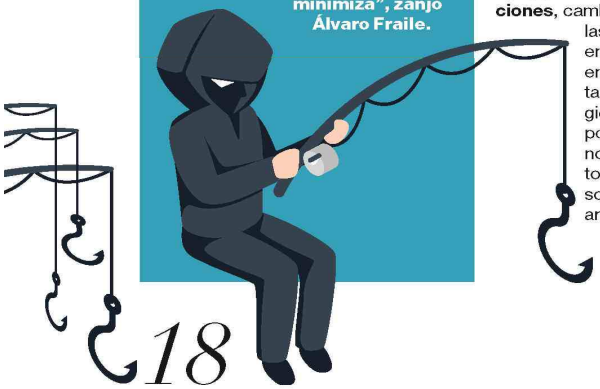
Channel PARTNER

Publicación	Channel Partner General, 18	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	578,75 cm² (92,8%)
Audiencia	25 500	V.Publicitario	3478 EUR (3835 USD)

UNION PROFESIONAL

Cuesta asentar el modelo de servicios gestionados

La ciberseguridad, como otros muchos ámbitos de la tecnología, migra en los últimos años a modelos de pago por uso. Sin embargo, en el sur de Europa la adopción de un esquema de servicios gestionados está costando más de lo previsto, según Sergio Martínez, de SonicWall. Aunque el directivo aseguró que hay figuras a las que les está yendo bien en este nuevo escenario. David Gasca también señaló que en España está costando más asentar este negocio, aunque hay empresas nuevas que no conciben otra opción que el alquiler de tecnología. Para Álvaro Fraile, de Ibermática, muchas veces es un tema de números: "Los financieros hacen la cuenta de cuánto les cuesta esto al cabo de 5 años, y no acaban viéndolo. Y en la administración pública, no se asume porque temen al que al año siguiente les reduzcan el presupuesto". Sin embargo, para Elena Lim, las ventajas están claras: disponibilidad permanente de expertos y actualizaciones. "Hay que educar al cliente para que dé el salto". "Si los clientes ven que un partner sabe de tecnología, de legislación o de procesos, es más fácil que te contraten el servicio. Además, con la falta de talento, las empresas corren el riesgo de quedarse sin personal en un momento dado, y con el pago por uso este problema se minimiza", zanjó Álvaro Fraile.



personal. Tenemos una alta demanda de profesionales que sepan implantar, en todas las categorías de producto", abundó **Daniel López, especialista en ventas de seguridad en Evolutio.** Por su parte, **Ruperto García-Soto, ingeniero de preventa de seguridad en Zyxel**, advirtió de que la tecnología no lo es todo: "Los fabricantes ponemos las herramientas, pero no podemos garantizar una seguridad total". Sin embargo, David Gasca, de V-Valley, apuntó que casi nunca el cliente final se queda al descubierto cuando ocurre un incidente, y que en algunos casos fabricantes ajenos a la empresa afectada corren en su ayuda para resolver la situación en el menor tiempo posible. Daniel López, de Evolutio, recomendó a las compañías hacer periódicamente simulaciones de ataques, para que sepan cómo enfrentarse a una situación crítica. "Además, las empresas deben tener servicios gestionados. Esto es un proceso de mejora continua". Y también se refirió a un ataque muy mediático ocurrido recientemente en España, el del Hospital Clínic de Barcelona, que comprometió la confidencialidad de los datos de miles de pacientes y dificultó la operativa del centro sanitario durante semanas. "El caso del Clínic es grave porque es información muy crítica y por la superficie de exposición. En un hospital todo lo que mide la vida es electrónica y tiene que estar protegido 24x7". **Álvaro Fraile, director del centro de excelencia (CoE) de ciberseguridad de Ibermática**, recordó que proteger los datos en una organización es "un proceso complejo que incluye a tecnologías y personas". Y que es un proceso que hay que revisar "todos los días". Y abogó por que los CISO tengan mucha visibilidad en las empresas y se sienten en el consejo de dirección.

Las implicaciones de GDPR

Enrique Delgado, responsable de alianzas y jurídico de Zertia Telecomunicaciones, cambió de tercio para referirse a las implicaciones de la entrada en vigor definitiva del GDPR, en 2018. "El legislador ha optado por la neutralidad tecnológica. Aquí en Europa ha optado por la autorregulación. Cuando nos enfrentemos a un proyecto de ciberseguridad es incluso más importante la parte de arquitectura y estrategia que la técnica. Hay que demostrar que hemos sido proactivos a la hora de predecir las amenazas y los problemas". También señaló el experto legal que la cultura del cumplimiento en una empresa debe "manar de arriba abajo". Y cerró su intervención diciendo que la ciberseguridad es un tema de "corresponsabilidad" porque si hay un ataque "luego hay que dirimir la culpa de cada uno". El otro experto legal de la mesa, Juan Manuel Valiente, de Secure & IT, recordó que la Agencia Española de Protección de Datos no sanciona a una empresa o un organismo por tener un ataque, "sino por no haber hecho lo posible por evitarlo o solucionarlo". Por su parte, **David López, director de operaciones de Factum IT,** comentó que hay empresas que no tienen un buen análisis de riesgos, que es la base para alinearse con GDPR. Y dijo que compañías como la suya están para ayudar a los clientes a crear un gobierno de la seguridad, "que es un asunto técnico, pero también organizativo".

El valor del partner

Los invitados a la mesa de ciberseguridad de CHANNEL PARTNER también valoraron específicamente el valor que da el partner tecnológico en un ámbito tan complejo como este. Paul Canales, de Hornetsecurity, habló de los servicios profesionales que ofrece el integrador. "No puede ser que hayas contratado la mejor tecnología del mundo, y nadie lo monitorice. Ahora cualquiera entra en los sistemas del cliente y llega a su CPD. Más que nunca es necesario alguien que ofrezca monitorización continua de esos sistemas". Para Álvaro Fraile, de Ibermática, el canal es más imprescindible que nunca porque la ciberseguridad requiere de muchas especializaciones, y los clientes se ven desbordados para atender todos los frentes. En el propio canal está habiendo compras y consolidación empresarial precisamente para poder mantener este conocimiento experto y encontrar el talento necesario, según recordó Sergio Martínez, de SonicWall. "En el canal mayorista también se está produciendo esta consolidación", añadió. Asimismo, varios portavoces se refirieron a la decepción que está siendo el Kit Digital a la hora de animar las ventas de ciberseguridad a las pymes. Así lo vio David Gasca, de V-Valley, que añadió que el proceso burocrático ha sido complejo para los partners. Además, Álvaro Fraile, de Ibermática, recordó que el Kit Digital es el punto de partida, pero que el cliente debe mantener en el tiempo esa tecnología y servicios que adquiere. Y que está por ver si esa inversión se hará. ■

Channel Partner

Publicación	Channel Partner General, 20	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	539,28 cm² (86,5%)
Audiencia	25 500	V.Publicitario	3303 EUR (3642 USD)

arcserve®

Preparados y resilientes: claves del Disaster Recovery

Es un hecho que a día de hoy la mayoría de las empresas no cuentan con un plan integral de recuperación ante desastres, quedando completamente expuestas a, en caso de ser víctimas de un ciberataque o un desastre natural o provocado por el hombre, sufrir grandes daños, en muchos casos irreparables. Estos impactos suelen ser fatales. De hecho, el 93 % de las empresas que perdieron su centro de datos durante diez días se declararon en bancarrota en el plazo de un año.

ESPERAR A QUE NO PASE NADA NO ES UN BUEN PLAN

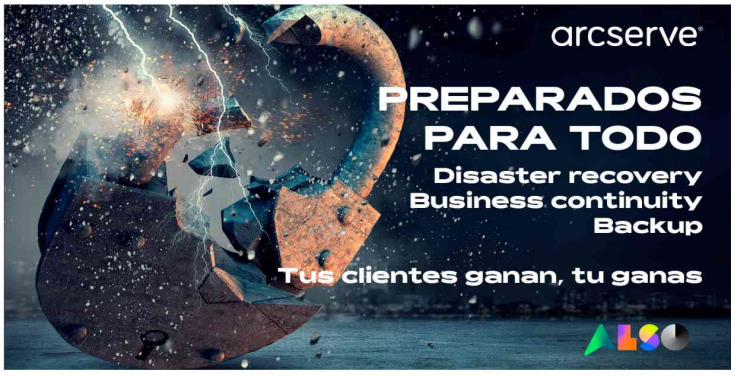
Convencer y concienciar a las empresas de que esperar a que no pase nada no es un buen plan, los desastres son prácticamente inevitables. De hecho, especialmente las PYMES, no tienen la capacidad de gestionar la recuperación de datos y la continuidad del negocio por su cuenta. Pero ¿cómo puede un MSP convencer a las empresas de la necesidad de pensar más allá del paso esencial de realizar un simple backup de sus datos e invertir en una solución profesional de recuperación ante desastres?

LA DIFERENCIA ENTRE BACKUP Y DISASTER RECOVERY

Ambos protegen los datos de una empresa, pero son diferentes. Las copias de seguridad son esenciales para tener una réplica de los datos críticos disponible en caso de que los datos originales se pierdan o se pongan en peligro, pero no son suficiente para lograr una recuperación rápida y completa de un desastre. Un plan sólido e integral de recuperación ante desastres garantiza una recuperación rápida y completa tras un desastre, establece los pasos necesarios para una completa recuperación, y sí, incluye backup, pero va más allá: define los objetivos de recuperación, traza todas las respuestas requeridas del personal y requiere pruebas periódicas de las copias de seguridad para asegurarse de que sean realmente recuperables. Dicho de otra manera: el backup es solo una parte de un plan de recuperación ante desastres.

TRANSMITIR UN MENSAJE POSITIVO PARA CONCIENCIAR A LAS EMPRESAS

El miedo es un poderoso motivador, pero Arcserve apuesta por utilizar un mensaje positivo para convencer a las empresas de la necesidad de un plan recuperación ante desastres. Se trata de una inversión que garantiza los ingresos y mejora el rendimiento. Hay que enfatizar que la recuperación ante desastres va más allá de volver a poner los sistemas operativos. Un buen plan garantiza que el negocio esté siempre disponible y, por tanto, la continuidad total del negocio.



CONTACTOS

Arcserve
Federico Gongora
Territory Account Manager Iberia
Federico.gongora@arcserve.com
+34 935 48 41 34

ALSO Spain
Martín Pérez
Business Development Manager
Martin.perez@also.com
+34 680 460 527
www.arcserve.com/es

DRAAS ES TODO BENEFICIO PARA LAS EMPRESAS ACTUALES

DRaaS (Disaster Recovery as a Service) es un plan de recuperación ante desastres que implica la utilización de servicios en la nube para garantizar que los datos y sistemas críticos de una organización puedan recuperarse en caso de un desastre natural o provocado por el hombre sin necesidad de disponer de recursos específicos ni de aumentar los costes de personal de TI interno, puesto que todas esas funciones TI que antes se manejaban en las instalaciones ahora son gestionadas por su MSP, aportando mayor eficiencia y rentabilidad, ya que no requiere inversión en nueva infraestructura. DRaaS es una garantía de tranquilidad para toda empresa. Con un proveedor DRaaS como Arcserve, saben que cuentan con profesionales experimentados para manejar todos los desafíos de recuperación y administrar sistemáticamente todos los aspectos de la recuperación. Pueden estar seguros de que un desastre, en caso de que ocurra, no los dejará fuera del negocio. Así como nadie debería conducir un coche sin asegurar, parece inconcebible que haya negocios sin un plan de recuperación tras desastres. No es una buena práctica, y, hoy en día y con proveedores experimentados, es completamente innecesario.

Channel PARTNER

Publicación	Channel Partner General, 21	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	533,60 cm² (85,6%)
Audiencia	25 500	V.Publicitario	3277 EUR (3613 USD)

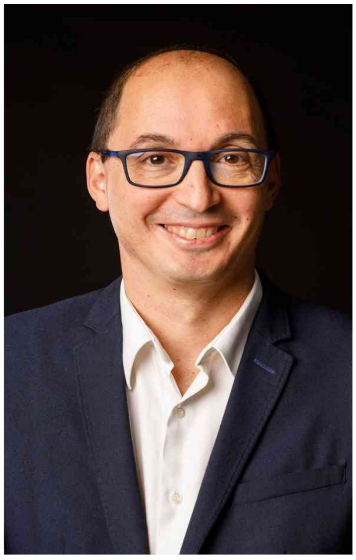
HORNETSECURITY

Menos es más a la hora de concienciar a los empleados

PAUL CANALES, HEAD OF CHANNEL IBERIA, ITALY & LATAM HORNETSECURITY

Según diferentes estudios, la gran mayoría de los incidentes de ciberseguridad se deben a errores humanos. En las empresas, los atacantes de ingeniería social prefieren explotar la vulnerabilidad de los empleados porque requiere mucha menos experiencia y esfuerzo que el hackeo de vulnerabilidades técnicas. Es cierto que las empresas hacen bien en proteger sus sistemas de forma exhaustiva con las últimas medidas de seguridad técnicas y organizativas. Sin embargo, para establecer una cultura de seguridad sostenible, las empresas deben aprovechar los hábitos de los usuarios más vulnerables a los ciberataques. La forma de ingeniería social más extendida hoy en día es el phishing. Esto abarca desde los correos masivos indiscriminados hasta los correos personalizados. Según el Informe de Ciberseguridad 2023 de Hornetsecurity, más del 40% de todo el tráfico de correo electrónico ya supone una amenaza potencial. Con la proliferación de modelos generativos de IA, como ChatGPT, se espera que esta tasa aumente, ya que las cadenas de ataques de phishing pueden automatizarse por completo y simplificarse significativamente.

Por lo tanto, las empresas deben centrarse en una formación de concienciación en materia de seguridad que prepare a los empleados para los ataques de phishing y los motive para manejar los emails entrantes con precaución. Además de los métodos clásicos para impartir conocimientos -como el e-learning o los webinars-, las simulaciones de phishing son especialmente eficaces para inducir un cambio de comportamiento duradero y establecer hábitos de usuario seguros. Esto se debe a que refuerzan las decisiones impulsivas responsables de los clics rápidos en correos electrónicos sospechosos. También aprovechan el "momento más enseñable" de un empleado al educarle sobre su comportamiento potencialmente malicioso justo en el momento adecuado, lo que les enseña a dejar de abrir automáticamente un correo electrónico, aunque este apele ingeniosamente a sus sentimientos espontáneos.



"El aumento de los ciberataques contra los empleados obliga a las empresas a intensificar la formación en materia de seguridad"

Esta escalada de amenazas exige una mayor formación en materia de seguridad, y actualmente existen en el mercado numerosas opciones. Pero cuidado: las empresas no deben sobrecargar a sus empleados con medidas de información y formación, ya que esto sólo suele provocar reacciones defensivas y resistencia interna. Tienen que hacer una elección inteligente para no abrumar a los usuarios, es importante que los responsables de seguridad informática den a los empleados tiempo suficiente y no les pidan que hagan todo a la vez para no sobrecargarlos. Si se castiga la mala conducta, se corre el riesgo de asustar e intimidar a los empleados. En el peor de los casos, esto puede condicionar la actitud defensiva ante la necesidad de repensar y cambiar su propio comportamiento en materia de seguridad informática.

Para llevarlo a cabo, Hornetsecurity ha desarrollado una solución integral basada en inteligencia artificial que combina formatos de aprendizaje innovadores y gamificación, con una de las simulaciones de phishing más avanzadas. A través del uso de una combinación de e-learning interactivo, videos cortos y cuestionarios, los participantes reciben información importante sobre los crecientes riesgos cibernéticos, reforzando su concienciación sobre las amenazas en ciberseguridad.

Security Awareness Service de Hornetsecurity funciona de forma totalmente automatizada y mide continuamente el comportamiento de seguridad de los empleados, lo que significa que la formación y las simulaciones de phishing se adaptan a las necesidades individuales de cada usuario, sin que los administradores o responsables de seguridad informática tengan que intervenir. El resultado es una cultura proactiva de la seguridad y unos empleados formados que reconocen los ciberataques y los rechazan con eficacia y, de esta manera, conocen y tienen en cuenta su responsabilidad con la empresa. ■

Empresa: Hornetsecurity Iberia S.L
Dirección: Vía de las Dos Castillas 33, 3ºD 28224. Pozuelo de Alarcón, Madrid. España
Teléfono: +34 93 470 07 78
Web: www.hornetsecurity.com
Mail de contacto: info@hornetsecurity.com
LinkedIn: www.linkedin.com/company/hornetsecurity/
Facebook: www.facebook.com/antispameurope?fref=nf
Twitter: twitter.com/Hornetsecurity

Channel PARTNER

Publicación	Channel Partner General, 22	Fecha	06/05/2023
Soporte	Prensa Escrita	País	España
Circulación	8755	V. Comunicación	44 487 EUR (49,053 USD)
Difusión	8462	Tamaño	523,82 cm² (84,0%)
Audiencia	25 500	V.Publicitario	3234 EUR (3566 USD)

UNIÓN PROFESIONAL

SAMSUNG

KME, herramienta de gestión empresarial para la era móvil

ISABEL LÓPEZ, RESPONSABLE DE SOLUCIONES Y SERVICIOS B2B DE SAMSUNG ESPAÑA

Dirección: Avenida de la Transición 32, Edif. C - P-E. Omega, 28108 Alcobendas (Madrid)
Teléfono: 917 143 600
Web: www.samsung.com/es
Correo: partners@samsung.com

Los dispositivos móviles se han convertido en una herramienta imprescindible. La movilidad permite tener un acceso directo a la información, responder de forma inmediata a las necesidades de negocio y gestionar en tiempo real posibles crisis. Las empresas españolas conocen estas ventajas y están llevando a cabo sus procesos de digitalización, independientemente de su tamaño y sector de actividad. En cualquier caso, es muy importante que tengan un control sobre los terminales corporativos, y que cada uno de ellos esté protegido frente a posibles ciberataques. Ciertas amenazas no requieren un clic y basta con que los usuarios reciban un archivo para acceder a los sistemas.

Los MDM (Mobile Device Management) son servicios que ayudan a las empresas a monitorizar estos dispositivos y que permiten aplicar todo tipo de configuraciones y restricciones en remoto. Para comunicar el teléfono de cada empleado con el MDM es necesario realizar una instalación en cada terminal. Este proceso puede ser muy tedioso si el administrador de la empresa lo hace de forma individual con cada dispositivo, lo que además supone un impacto económico y posibles fallos humanos. Sin embargo, este procedimiento puede ser mucho más efectivo mediante la automatización de la descarga e instalación de estas herramientas.

"Knox Mobile Enrollment no tiene coste asociado y permite incluir los terminales de la empresa en el MDM de la compañía"

Knox Mobile Enrollment es un servicio disponible en los terminales Samsung, sin coste asociado, que permite incluir los terminales de la empresa en el MDM de la compañía, sin interacción del usuario. Esta solución, que es compatible con los principales MDM del mercado, se ha mejorado con nuevos controles. Por ejemplo, para bloquear un terminal que no se ha registrado en el MDM pasados unos días, o porque haya perdido la conexión con el MDM. Para disponer de esta funcionalidad extra, el administrador debe de crear un perfil avanzado en KME. Además de automatizar el registro en el MDM, Knox Mobile Enrollment añade una capa extra de seguridad. Por ejemplo, si en algún momento el terminal pierde la comunicación con el MDM, cuando recupera la conexión con Internet, el perfil de Knox Mobile Enrollment se instalará en el terminal y realizará el registro en el MDM especificado.

DESARROLLOS FUTUROS

Por otro lado, Knox Mobile Enrollment permite desbloquear cualquier terminal. Esto es algo que ocurre a menudo en las compañías: el trabajador deja el teléfono móvil bloqueado con su cuenta de Google y este nos pide introducir la contraseña para avanzar. Gracias a Knox Mobile Enrollment evitamos realizar este paso y podemos recuperar la operatividad del dispositivo. En cualquier caso, las capacidades del perfil avanzado de Knox Mobile Enrollment irán desarrollándose aún más, para mejorar sus posibilidades e implementar nuevos controles. Estas nuevas capacidades estarán disponibles en la licencia de Knox Suite, que está incorporada en el diseño de los terminales Enterprise Edition. En Samsung seguiremos mejorando nuestros productos y servicios de acuerdo con las necesidades y demandas de los negocios en una nueva era móvil. ■

CONTENIDO OFRECIDO POR SAMSUNG