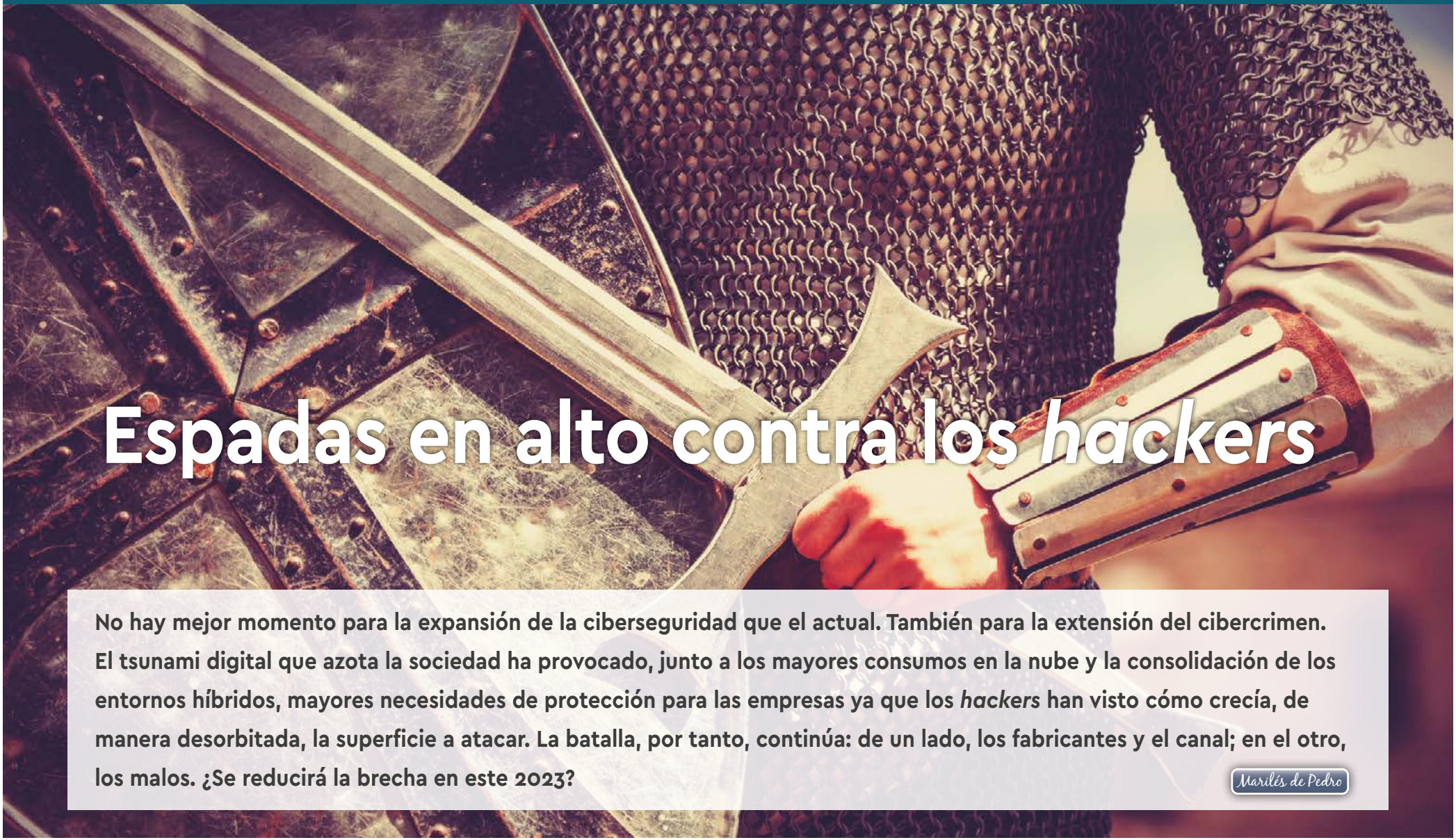
IDC prevé un crecimiento sostenido del 8 % para el mercado de la seguridad en España hasta 2024



Espadas en alto contra los *hackers*

No hay mejor momento para la expansión de la ciberseguridad que el actual. También para la extensión del cibercrimen. El tsunami digital que azota la sociedad ha provocado, junto a los mayores consumos en la nube y la consolidación de los entornos híbridos, mayores necesidades de protección para las empresas ya que los *hackers* han visto cómo crecía, de manera desorbitada, la superficie a atacar. La batalla, por tanto, continúa: de un lado, los fabricantes y el canal; en el otro, los malos. ¿Se reducirá la brecha en este 2023?

Marilés de Pedro

Complejo panorama de amenazas

En este 2023 seguirán evolucionando los ataques avivados por el modelo de Cibercrimen como Servicio (CaaS). Acacio Martín, director regional de Fortinet en España y Portugal, asegura que los malos seguirán aprovechando nuevos *exploits* en entornos no tradicionales, como los dispositivos alojados en el perímetro o los mundos virtuales.

La tecnología actúa en una doble "dirección". Martín recuerda que también juega a favor de los ciberdelicuentes que siguen transformando en "armas" las nuevas tecnologías. "No sólo atacan la superficie tradicional, sino lo que hay detrás de ella, es decir, tanto fuera como dentro de los entornos de red tradicionales. Al mismo tiempo, tienen un mayor conocimiento de su objetivo de ataque ya que dedican más tiempo a recopilar información para intentar evadir la detección, la inteligencia y los controles".

Unos ataques que alcanzarán a todos los sectores industriales. Según el "Global Risks Report 2022" publicado por el World Economic Forum en el tercer trimestre de 2022 los ciberataques se incrementaron un 23 %. "Las previsiones apuntan un crecimiento aún más fuerte en todo el mundo, impulsado por prácticas como el mayor uso de los *exploits* y el *ransomware*, el *hacktivismo* movilizado por el Estado o las herramientas incipientes, como es el caso de la inteligencia artificial", relata Mario García, director general de Check Point Software en España y Portugal.

> "El mercado negro de la ciberdelincuencia es de tal magnitud que hay oferta y demanda no solo de datos, sino de vulnerabilidades, que incluso son adquiridas por algunos gobiernos"

Según el informe de predicciones para 2023 de Trend Micro las empresas se enfrentan a un incremento de los ataques dirigidos a los puntos ciegos de la seguridad en la oficina doméstica, la cadena de suministro de software y la nube.

"Un perímetro corporativo cada vez mayor y superficies de ataque a menudo olvidadas, como es el caso del software de código abierto, dejan más expuestas a las organizaciones", analiza Raúl Guillén, responsable de alianzas estratégicas en Trend Micro en Iberia. "Los ciberdelincuentes seguirán explotando protocolos obsoletos y las vulnerabilidades en los dispositivos conectados a Internet y se aprovecharán de la sobrecarga de trabajo que tienen los equipos de seguridad actuales", continúa.

Las VPN representarán un objetivo especialmente atractivo ya que una única "solución" puede explotarse para atacar varias redes

"La ciberseguridad, impulsada por los procesos de digitalización y la cada vez mayor concienciación, está pasando a tomar un papel más protagonista en la estrategia de las compañías"

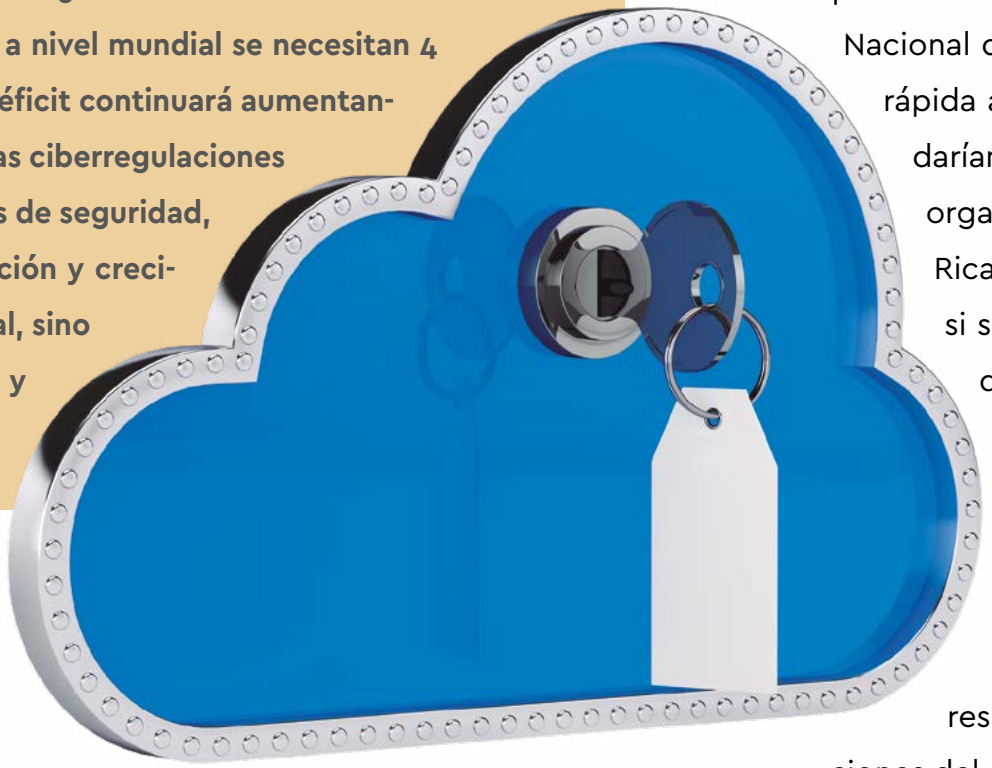
corporativas. "Los *routers* domésticos serán objetivo de los ataques ya que no reciben parches ni son gestionados por el departamento central de tecnología. Igualmente, las técnicas "*living off the cloud*" pueden convertirse en la norma para que los grupos que atacan la infraestructura de la nube permanezcan ocultos a las herramientas de seguridad convencionales", completa el responsable de alianzas de Trend Micro.

No faltarán las amenazas más "tradicionales". A juicio de Miguel de Castro, ingeniero de ventas en CrowdStrike, el *ransomware*, que se diversificará hacia modelos comerciales completamente nuevos, y el robo de información liderarán la lista. Unas amenazas que tendrán como principales vectores de entrada "el correo electrónico, el software desactualizado o vulnerable a *exploits zero-day* y los accesos mediante cuentas de usuario válidas o ataques a la identidad". Muchos *hackers* "recurrirán a la explotación de métodos de ataque ya probados como la ingeniería social, el *business email* compromiso (BEC)-*as-a-service* y los *deepfakes*", completa Guillén.

Ricardo de Ena, *area sales manager* de la zona norte de WatchGuard España, recuerda la "hiperespecialización" que exhiben los ciberdelincuentes. "En numerosas ocasiones llevan mucho tiempo en la organización sin levantar sospechas, a modo de auditoría, y cuando ya saben por dónde pueden atacar, venden el proyecto de ataque a otro grupo cibercriminal

La falta de talento

La falta de talento cualificado en materia de ciberseguridad señala uno de los principales retos que debe solucionar el sector. Según los datos del INCIBE la fuerza laboral en esta materia cuenta con una gran brecha de talento que se estima que alcanzará más de 83.000 profesionales en 2024. Se espera un incremento del 300 % en la demanda de talento en los próximos 3 años. Mario García calcula que a nivel mundial se necesitan 4 millones de profesionales. "A pesar de que este déficit continuará aumentando se espera que los gobiernos introduzcan nuevas ciberregulaciones para proteger a los ciudadanos contra las brechas de seguridad, así como una mayor inversión no sólo en la creación y crecimiento de los departamentos de seguridad digital, sino de la propia formación en ciberseguridad dentro y fuera de las empresas".



y este, a su vez, lo revende o lo saca incluso a concurso. El mercado negro de la ciberdelincuencia es de tal magnitud que hay oferta y demanda no solo de datos, sino de vulnerabilidades, que incluso son adquiridas por los gobiernos".

Cualquier segmento y empresa es susceptible de ser atacado. Ya nada ni nadie escapa de la visión de los *hackers*. Segmentos como la sanidad, la banca o el sector público seguirán en el foco de los ciberdelincuentes.

"Tampoco hay que olvidar que las infraestructuras críticas son, cada vez más, objetivo de ataques de grupos de cibercrimen o de Estados enemigos", señala Borja Pérez, *country manager* de Stormshield Iberia. "Un cumplimiento exhaustivo del Esquema Nacional de Seguridad (ENS) y la rápida adecuación a NIS2 ayudarían mucho a este tipo de organizaciones".

Ricardo de Ena apunta que, si se analizan los objetivos que más ataques han recibido, y tras los que está un Estado, son "los gobiernos, las entidades financieras, las instituciones militares y diferentes organizaciones del ámbito de la tecnología o las telecomunicaciones".

Borja Pérez no olvida a las pymes. "Cuando hablamos de ataques masivos no dirigidos,

que durante 2023 se repetirán, sabemos que quienes más van a sufrir son las pequeñas y medianas empresas. Por regla general, su inversión y formación en ciberseguridad sigue siendo baja".

La movilidad sigue siendo una de las áreas con más recorrido en la aplicación de la seguridad. Isabel López, *sales engineer manager* de Samsung, desvela que durante los últimos años los dispositivos móviles han tenido más posibilidades de sufrir un ataque que un PC. "En una época en la que las empresas realizan una gestión multidispositivo, los ataques pueden acceder a través de muchas vías: correos electrónicos, SMS de contactos conocidos, descargas de software o clics involuntarios en páginas web que insertan un programa malicioso en el sistema".

Inversión creciente

Según las previsiones que manejaba IDC el crecimiento del mercado de la ciberseguridad en España se situará en un 7,7 % en 2022 con un CAGR previsto del 8 % hasta 2024. Además, en 2025, IDC pronostica que la inversión en ciberseguridad podría superar los 2.200 millones de euros, con ritmos de crecimiento cercanos al doble dígito. "La ciberseguridad, impulsada por los procesos de digitalización y la cada vez mayor concienciación, está pasando a tomar un papel más protagonista en la estrategia de las compañías, por lo que se espera un aumento general en la inversión por parte de todos los sectores", valora Mario García.

> "El mundo será cada vez más un lugar más peligroso y seguirá yendo a peor en términos de ciberseguridad"

Sergio Martínez, director general de Sonicwall en Iberia, cree que 2023 será un año excelente para la ciberseguridad y el canal TI. "El mundo será cada vez más un lugar más peligroso y seguirá yendo a peor en términos de ciberseguridad". El incremento exponencial de la superficie de exposición y la hiperconectividad (sobre todo por 5G), unido a la creciente militarización y sofisticación del cibercrimen, empujan, a su juicio, en este sentido. La marca prevé un crecimiento entre el 7 y el 8 % en 2023. "Las oportunidades no dejarán de crecer. Nunca la ciberseguridad ha sido tan necesaria".

Tan solo el 11 % de las empresas considera que tiene suficiente capacidad informática interna para hacer frente a cualquier ciberataque. Se calcula que más del 50 % de las empresas que sufre un ciberataque importante, tarda más de cinco horas en detectarlo y un número importante de ellas convive con él durante algunas semanas e incluso meses. "Nunca hemos estado tan expuestos", valora el responsable de Soni-

cWall. Según datos del fabricante una empresa recibió, de media, 1.014 ataques de *ransomware* durante los 3 primeros trimestres de 2022.

Aunque cada sector tiene sus peculiaridades, Ricardo de Ena prevé un incremento de los ataques en el sector financiero. "Lo que está ocurriendo con las criptomonedas está dando pie a nuevas estafas, lo que debe conducir a un aumento de la inversión en los segmentos de banca y seguros, junto a la Administración Pública". También las energéticas aumentarán sus inversiones en este 2023. "El turismo y la automoción se encuentran también entre los principales motores económicos", completa Isabel López, Ricardo Maté, *regional vicepresident south EMEA & emerging* de Sophos, abre el abanico de inversión a todas aquellas empresas que están abordando su transformación digital. "Cada vez disponen de más servicios y procesos digitales, lo que las hace más susceptibles de sufrir un ciberataque que afecte a sus negocios e incluso a su supervivencia. Por ese motivo, están llevando a cabo procesos de revisión de su ciberseguridad y una mayor adecuación de sus modelos de protección, detección y de respuesta, así como de la formación de sus empleados".

> Una empresa recibió, de media, 1.014 ataques de *ransomware* durante los 3 primeros trimestres de 2022

Inversión en la formación del empleado

Según un estudio del Foro Económico Mundial el 95 % de los ciberataques comienza por un error humano ya que las personas caen en las trampas de ingeniería social de estas amenazas. "Que los trabajadores estén formados es más importante que nunca", valora Mario García. En este terreno destaca, por ejemplo, la iniciativa que ha puesto en marcha el Banco Santander en la que ha incorporado la respuesta de los empleados ante los ciberataques de *phishing* en su política de cobro de bonus. El máximo responsable de Check Point en España y Portugal asegura que, aunque no se conozca la cuantía exacta de la compensación, se trata de un coste tremendamente rentable en comparación con los que supone ser víctima de un ciberataque. "El coste total puede llegar a ser hasta siete veces superior al de los propios rescates".

Alrededor del 20 % de las brechas de ciberseguridad son causadas por personas curiosas que vulneran sistemas informáticos y aplicaciones sin el ánimo de ocasionar daños. "El principal reto es invertir en la formación de los empleados y en desarrollar una cultura de ciberseguridad y responsabilidad asociada al correcto uso de la información y los datos sensibles de las empresas. Las consecuencias

La protección de la pyme, ¿el mayor reto?

Las pymes son también diana para los ciberdelincuentes. Según un estudio de Kaspersky más del 60 % de las pymes reconocieron haber sufrido un ataque en 2022. Una gran parte de las amenazas va dirigida a los propietarios de este tipo de empresas, a su cadena de suministro y también en forma de ataques DDoS que ponen al límite sus recursos, como su página web.

"Son las organizaciones que lógicamente cuentan con recursos más limitados para implementar las adecuadas medidas de seguridad para enfrentarse a las cada vez más complejas y diversificadas ciberamenazas", recuerda Acacio Martín.

La encuesta realizada por ESET entre este público señala el presupuesto como factor clave. David Sánchez, director comercial de la compañía en España, asegura que es su limitación y la falta de inversión en ciberseguridad lo que más preocupa en los departamentos de TI, "por delante de los ataques dirigidos y las vulnerabilidades".

Según los datos que manejaba Check Point, el pasado mes de julio, por ejemplo, la media semanal global de organizaciones impactadas por el *ransomware* llegó a alcanzar a una de cada 40 empresas, lo que suponía un incremento del 59 %. Mario García especifica que el ascenso era aún más alarmante entre los minoristas y mayoristas: un 182 %. "Se espera que las pymes comiencen a tomar mayores medidas para protegerse contra este tipo de amenazas que frena su crecimiento".

Sin duda, queda mucho por hacer en el tejido pyme. A juicio de Raúl Guillén, el canal juega un factor fundamental ofreciendo servicios gestionados de seguridad para aquellas compañías que no pueden dotarse de estructura propia. "Los *partners* que estén más cerca de sus clientes saldrán reforzados; claramente es una oportunidad de crecimiento".

de cualquier ciberataque son numerosísimas y pueden, incluso, provocar la extinción o el cierre de un negocio o una empresa", completa Sergio Martínez.

La inversión de la Administración Pública

El sector público es uno de los principales objetivos de los *hackers*. Un segmento que cuenta con muchas vulnerabilidades. "Disponen de datos u otros activos de gran valor", recuerda Acacio Martín. "Debido a la sensibilidad de la información que poseen y a la persistencia de sus atacantes, los or-

ganismos gubernamentales no pueden permitirse el lujo de operar con una ciberseguridad deficiente poniendo los datos de los ciudadanos y los posibles servicios esenciales en niveles de riesgo inaceptables". Disponen de recursos limitados y suelen estar conectados con una gran variedad de subcontratas y terceros "lo que las hace más vulnerables al robo de credenciales para obtener acceso a sus redes", completa. "Son un objetivo preferente de los ataques provenientes de los estados-nación".

En cuanto al tipo de ataques, Miguel de Castro apunta los relacionados con la identidad y el software desactualizado o susceptible a un Zero Day. "El correo electrónico continuará siendo el principal vector de entrada para los atacantes".

La sanidad es diana preferente. Un segmento crítico que debe ser especialmente cuidadoso en su protección. Mario García señala el ejemplo del gobierno de Singapur que ha creado equipos especiales interinstitucionales para luchar contra el *ransomware* y la ciberdelincuencia, reuniendo a empresas, departamentos estatales y fuerzas de seguridad para combatir la creciente amenaza. "Espero que nuestro gobierno lleve a cabo iniciativas similares".

> "Que los trabajadores estén formados es más importante que nunca"

El sector público español ha incrementado la inversión en seguridad: durante el primer semestre del año pasado el montante se elevó por encima de los 120 millones de euros. Borja Pérez señala al Centro Criptológico Nacional (CCN) como un vector de ayuda. "La obligatoriedad del cumplimiento del ENS será una baza importante para crear las condiciones de seguridad necesarias para el uso de medios electrónicos y garantizar la seguridad de sistemas, datos, comunicaciones, etc.".

Puesto de trabajo

El puesto de trabajo se ha convertido en entorno crítico para la protección. El crecimiento y posterior asentamiento del teletrabajo ha incrementado su criticidad. También la profesionalización del cibercrimen y el traslado de cargas de trabajo a la nube se han sumado como factores claves. Ricardo Maté apunta tanto a las herramientas EDR (*Endpoint Detection & Response*) como a las dedicadas a la protección de la nube, mediante la adopción de las diferentes soluciones de SASE entre las que se encuentra ZTNA (*Zero Trust Network Access*), como los principales escudos de protección. Unas herramientas que deben estar arropadas por servicios de detección y respuesta 24/7 que exigen profesionales cualificados en la búsqueda de amenazas. "Ante la dificultad de encontrarlos y, posteriormente, retenerlos,

se está produciendo un incremento importante en la implantación de servicios de detección y respuesta MDR (*Managed Detection and Response*)", completa el directivo de Sophos.

Las inversiones en torno al teletrabajo crecieron exponencialmente durante la pandemia. "Ahora es el momento de sentarse y planificar", analiza Ricardo de Ena. "Dentro de este plan de inversión, cuando la conectividad ya está asegurada, hay que reforzar la seguridad, siendo especialmente esencial garantizar la identidad y los accesos a los sistemas de la compañía, para lo que hay apostar por soluciones de autenticación multifactor (MFA) y por herramientas con capacidad de inspeccionar el tráfico".

Y, ¿la brecha?

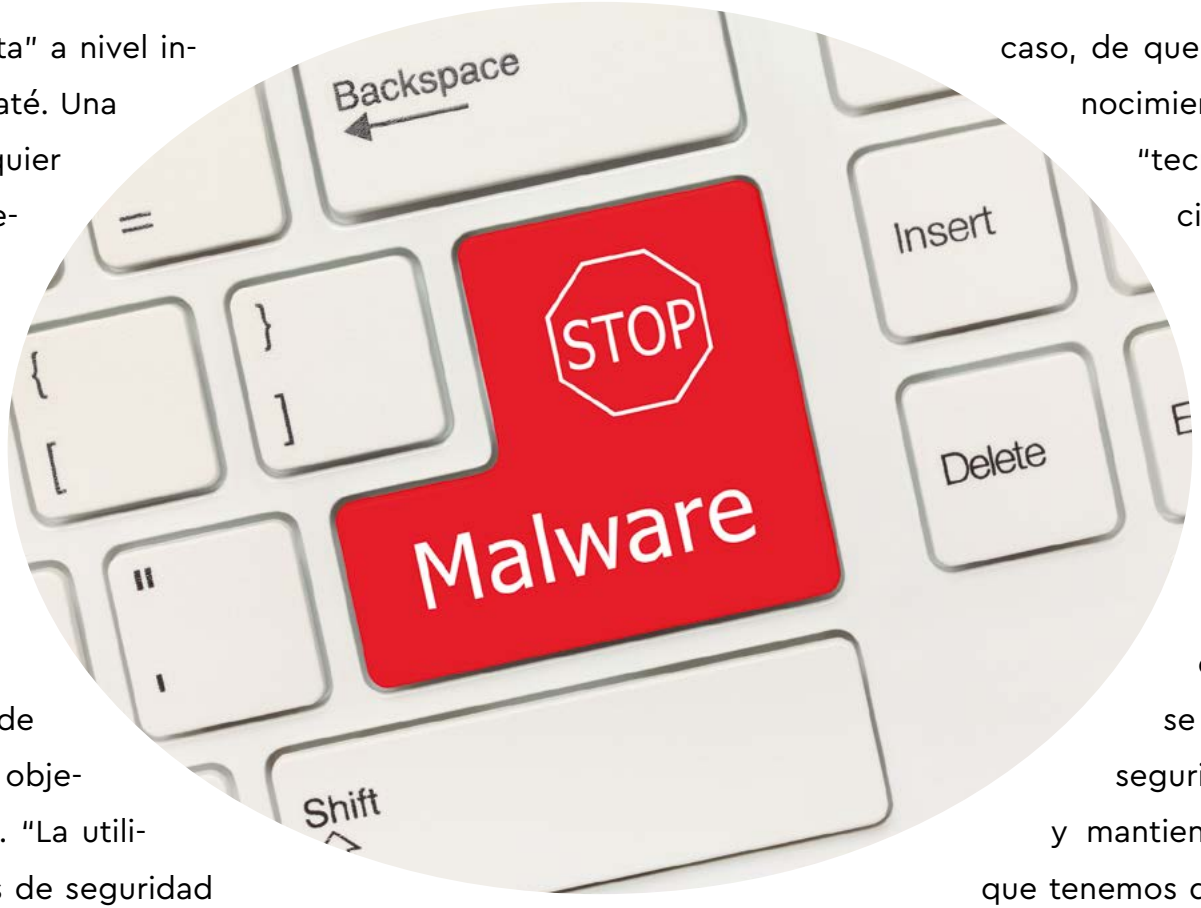
La enorme innovación que se ha ido imprimiendo a las tecnologías de seguridad parece que va pareja a la creciente complejidad e "inteligencia" que siguen exhibiendo los ataques. Ricardo de Ena apunta que existe un tira y afloja. "Tenemos que tratar de que la industria de la seguridad vaya un paso por delante o, al menos, al mismo ritmo, pero muchas veces es al contrario", valora. "Sigue habiendo una brecha de compensación entre las contramedidas que tenemos en el sector para paliar y combatir a la ciberdelincuencia y el propio presupuesto que manejan los ciberdelincuentes que en muchas ocasiones es muy grande".

La industria del cibercrimen alcanza continuamente nuevos niveles de comercialización y estandarización. "Cada vez más grupos de

cibercriminales utilizan metodología propia de la industria del software e implementan modelos como servicio para escalar su "oferta" a nivel industrial", recuerda Ricardo Maté. Una situación que reduce cualquier barrera de entrada y da acceso, de manera mayoritaria, a herramientas y técnicas que antes solo estaban disponibles para los *hackers* más sofisticados.

El incremento en el robo y comercialización de credenciales permite a los cibercriminales encontrar maneras de infiltrarse en las redes de sus objetivos de una manera efectiva. "La utilización de herramientas licitas de seguridad hace que los atacantes ejecuten comandos del sistema que les permitan sobrepasar las opciones de seguridad, descargar y ejecutar ficheros remotos maliciosos y moverse lateralmente entre diferentes redes", completa Maté.

> "La mayoría de los ciberataques tiene éxito, más por demérito de los defensores que por mérito de los atacantes"



No se trata, en ningún caso, de que los *hackers* tengan más conocimientos o dispongan de mejores "tecnologías". "La mayoría de los ciberataques tiene éxito, más por demérito de los defensores que por mérito de los atacantes, por lo que no debemos presuponer capacidades superiores a las que realmente poseen estos últimos cuando, en realidad, lo que sucede es que no se aplican siquiera medidas de seguridad básicas o se configuran y mantienen adecuadamente aquellas que tenemos disponibles", analiza Josep Albors, director de investigación y concienciación de ESET España.