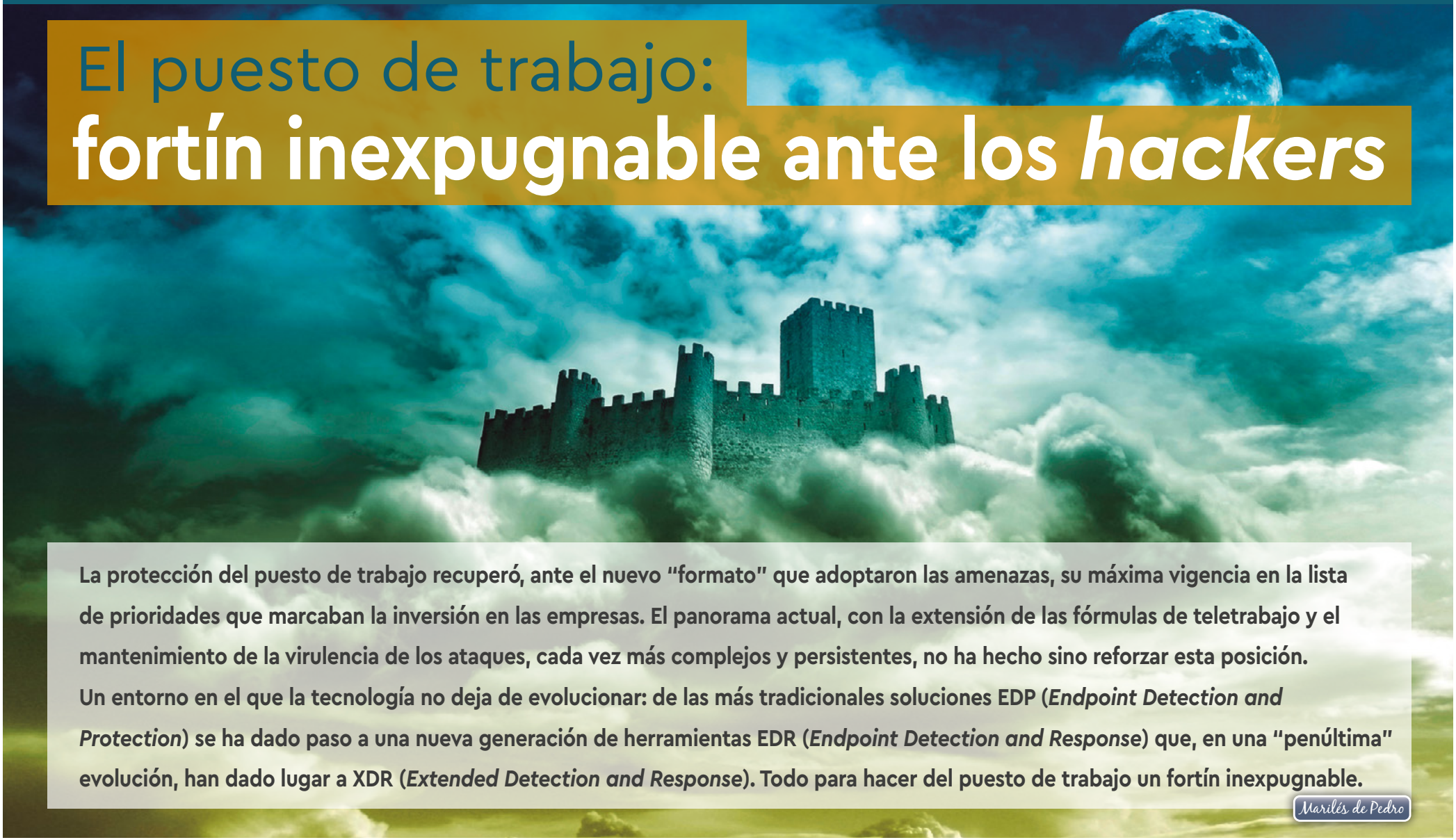
Los fabricantes prevén que continúe la inversión en el entorno del puesto de trabajo en 2022

El puesto de trabajo: fortín inexpugnable ante los *hackers*



La protección del puesto de trabajo recuperó, ante el nuevo "formato" que adoptaron las amenazas, su máxima vigencia en la lista de prioridades que marcaban la inversión en las empresas. El panorama actual, con la extensión de las fórmulas de teletrabajo y el mantenimiento de la virulencia de los ataques, cada vez más complejos y persistentes, no ha hecho sino reforzar esta posición.

Un entorno en el que la tecnología no deja de evolucionar: de las más tradicionales soluciones EDP (*Endpoint Detection and Protection*) se ha dado paso a una nueva generación de herramientas EDR (*Endpoint Detection and Response*) que, en una "penúltima" evolución, han dado lugar a XDR (*Extended Detection and Response*). Todo para hacer del puesto de trabajo un fortín inexpugnable.

Marilés de Pedro

El teletrabajo y la consiguiente rotura del tradicional perímetro ha exigido una mayor inversión en el puesto de trabajo. "Se ha vuelto mucho más crítico puesto que se ha convertido en un punto vulnerable para la seguridad de los sistemas de TI de cualquier compañía", explica Carlos Vieira, *country manager* de WatchGuard Technologies en España y Portugal. Con ello, los desarrollos en torno a la seguridad perimetral han evolucionado para adaptarse a los nuevos requerimientos del mercado. "Hemos destinado muchos recursos e inversión en innovación para que las soluciones abarcaran esta crítica protección del *endpoint*". Vieira recuerda que la extensión de los entornos híbridos ha provocado la aparición de los "pacientes cero", lo que supone un problema añadido. "Los usuarios que trabajan desde su casa con su equipo personal o corporativo pueden introducir *malware* en la empresa cuando regresan al puesto de trabajo físico".

"Solo se tarda una media de 8 horas en forzar una contraseña"

La explosión de la inversión en este ámbito también se explica por la tradicional cultura española del gusto por el trabajo presencial. Lo apunta Carlos Galdón, director de canal de Sophos en Iberia, que también puntualiza que este boom se está extendiendo a toda la protección de la empresa de forma integral. "En la última edición del World Economic Forum la ciberseguridad se posicionó como una de las cuatro prioridades para el futuro", reivindica.

El desarrollo del BYOD (*Bring Your Own Device*), que lleva años de implantación, se ha sumado a este incremento. Un estudio de Kaspersky, llevado a cabo entre más de 6.000 trabajadores de todo el mundo, reveló que solo el 53 % de los empleados usaba una VPN para conectarse a las redes corporativas y que únicamente un 32 % de las empresas había proporcionado a su personal una solución de seguridad para usar en dispositivos personales con fines de trabajo desde que comenzó la transición hacia el trabajo en remoto con el confinamiento. "Además de la conexión vía VPN, el hecho de que los empleados utilicen dispositivos personales para acceder a los recursos de su empresa (BYOD) o usen aplicaciones no aprobadas por la compañía para intercambiar información hace imprescindible la implementación de políticas de ciberseguridad que indiquen claramente qué dispositivos y aplicaciones están permitidos, qué medidas de seguridad deben implementarse y cómo pueden compartirse los datos de la empresa", recomienda Alfonso Ramírez, director general de Kaspersky en España y Portugal.

Este desarrollo del área del *endpoint* ha conducido a una mayor inversión de las marcas en el apartado de la innovación. Sergio Bravo, director de ventas de Bitdefender, explica que ésta debe centrarse no solo en las capacida-

des de detección y respuesta, sino también en toda la infraestructura de la organización. "Los algoritmos de aprendizaje automático encuentran relaciones entre eventos de todos los enpoints e identidades que pueden haber evadido las tecnologías preventivas", alerta. La innovación se ha centrado en la mejora del análisis y en una mayor eficiencia en la entrada de los datos en el sistema. "Con ello, los motores de correlación pueden identificar sistemas ya comprometidos, deteniendo la cadena de destrucción antes de que pueda expandirse por completo. Gracias a una baja tasa de falsos positivos en vectores de ataque conocidos, la detección de *endpoints* se puede expandir aún más al añadirle otros sensores, como Microsoft 365, sin abrumar a los equipos de seguridad".

Panorama de amenazas

No deja de crecer la complejidad de las amenazas. Junto al uso del *malware* de nueva generación, combinan diversas técnicas de ataque (herramientas legítimas, varias familias de *malware*, ataques a vulnerabilidades, etc.), lo que obliga a las empresas a armar una defensa dinámica y efectiva. "Nunca hemos estado tan expuestos" concluye Sergio Martínez, director general de SonicWall en España y Portugal. Se impone, por tanto, el diseño de una ciberdefensa, por capas, preparada para detectar todo tipo de ataques de corte conocido y desconocido, con visibilidad central para poder responder en tiempo real, y a un TCO asequible para una pyme. "La puesta en marcha de antivirus de nueva generación, con capacidad de *roll-back*, como última línea de

"La protección del puesto de trabajo se ha vuelto mucho más crítica puesto que se ha convertido en un punto vulnerable para la seguridad de los sistemas de TI de cualquier compañía"

defensa, es fundamental", completa Martínez. Una solución para el puesto de trabajo que debe estar integrada "con el resto de sistemas de protección existentes y con los sistemas utilizados en los centros de operaciones de seguridad (SOC)", completa José Luis Laguna, *director systems engineering* de Fortinet en España y Portugal.

El uso intensivo de *kits* de *Malware as a service* (MaaS) se ha disparado y el crecimiento del *ransomware* en Europa se ha elevado por encima del 230 % en algunos meses. "Cualquier aspirante a atacante puede ser extremadamente peligroso con estos *kits* de ataque", explica Martínez. "Como le dijo un miembro del IRA a Margaret Thatcher, "nosotros necesitamos tener suerte una vez. Ustedes necesitan tener suerte todo el tiempo".

Calcula Check Point Software que en 2021 se produjo un aumento del 50 % en el número de amenazas que las redes corporativas soportaron por semana. Una peligrosa tendencia que alcanzó un máximo histórico a finales de año, llegando a 925 amenazas a la semana por organización. Junto a estos números, el fabricante comunicó que el pasado mes de octubre 1 de cada 61 organizaciones en todo el mundo estaban viéndose afectadas por el *ransomware* cada semana. "Va a continuar siendo imprescindible que las compañías aumenten en sus presupuestos la inversión en ciberseguridad", razona Mario García, director general de Check Point Software en España y Portugal.

Según el Security Report 2021 de la marca israelí la seguridad en la nube pública continuaba siendo una de las principales preocupaciones para el 75 % de las empresas a principios de 2021. "Más del 80% de las compañías comprobó que sus herramientas de seguridad no funcionaban en absoluto o sólo tenían funciones limitadas en la nube, una plataforma indispensable para sacar adelante las tareas diarias con el teletrabajo".

Contar con una política de seguridad que incluya una gestión de contraseñas segura es clave. Carlos Vieira recuerda que durante años hemos pensado que poner una contraseña de 8 dígitos con letras, números, símbolos, mayúsculas y minúsculas, era segura. "Sin embargo, solo se tarda una media de 8 horas en forzarla", alerta. "Muchas empresas se han visto forzadas a publicar servicios internos para que sus trabajadores pudieran seguir trabajando y

"Aún son pocas las empresas que saben sacarle el jugo a soluciones más avanzadas como las EDR"

hay que confiar en que el usuario usa contraseñas suficientemente fuertes. Es un gran error, pues la mayoría de los usuarios usarán contraseñas realmente sencillas con el fin de ser capaces de recordarlas".

Del EDP al EDR...

Hace tiempo que las soluciones EDP (*Endpoint Detection and Protection*) dejaron de ser suficientes para hacer frente a los ataques de los ciberdelincuentes. A medida que aumentaba la complejidad y la sofisticación de los mismos, también evolucionaban las técnicas de seguridad, dando lugar a una nueva generación de herramientas EDR (*Endpoint Detection and Response*) que, no sólo previene los ataques antes y después de su ejecución, sino que es capaz de detectar las amenazas que eluden la capa de prevención y responder rápidamente para minimizar el impacto en la organización.

Se trata de una tecnología capaz de prevenir y detectar amenazas, automatizando los procesos requeridos para conseguirlo, sin que afecten a los usuarios, que siguen disfrutando de una experiencia óptima. Permite a las empresas gozar de una completa visibilidad sobre lo que sucede en el sistema, reduciendo la superficie de ataque de los *endpoints* con un agente ligero cuyo funcionamiento es totalmente transparente para los usuarios.

Unas herramientas que aún no disfrutan de un despliegue masivo en las empresas. "Vectores de ataque considerados como clásicos siguen consiguiendo un elevado porcentaje de éxito", reconoce Josep Albors, director de investigación y concienciación de ESET España. "Aún son pocas las empresas que saben sacarle el jugo a soluciones más avanzadas como las

Errores más frecuentes

Según Gartner, en 2025 más del 85 % de los ataques hacia los *endpoints* corporativos se deberán a errores de configuración o por parte de los usuarios. "El eslabón débil y la puerta de entrada de cualquier ataque sigue siendo el ser humano", recuerda Sergio Martínez. Por tanto, "las credenciales se han convertido en las nuevas joyas de la corona a proteger".

Los errores más frecuentes, a juicio de Borja Pérez, *country manager* de Stormshield Iberia, son la falta de actualización de los sistemas o su falta de aplicación a todo el parque empresarial. "De nada sirve tener implantada una solución que roce el 100% de efectividad, si esta no está implementada en toda la organización. Se crean puntos vulnerables".

Contar con una protección inadecuada es otro de los errores más habituales. "Existe la convicción de que basta con desplegar un antivirus de puesto de trabajo o un *firewall* cuando la realidad es que es necesario identificar todos los flujos de comunicación de la compañía, lo que incluye la navegación, el correo, el acceso al *cloud*, etc.; y protegerlos adecuadamente", recuerda José de la Cruz, director técnico de Trend Micro Iberia, que insiste en la formación al usuario. "Debemos ayudarle a convertirse en un eslabón más robusto, lo que se logra con formación y concienciación que le ayuden a identificar tanto las posibles amenazas a las que se enfrentan, como sus consecuencias". Una formación que, recuerda, debe ir acompañada de "una evaluación continua con campañas de simulación de ataques de *phishing*".

EDR o no saben cómo aplicar metodologías Zero Trust para limitar el impacto de los ataques y conocer qué sucede en su red en todo momento", analiza.

Borja Pérez aboga por la "unificación". "Hace unos años había más diferencia entre unas y otras, pero hoy en día se ha producido una integración entre ambas. Aquellas que ofrecían detección y respuesta, con una filosofía de herramientas más forenses, ahora proporcionan protección; mientras que las que procuraban protección, en la actualidad han añadido capacidades de detección y respuesta".

Una integración que, a juicio de Carlos Galdón, deberá producirse, pero no es así en la actualidad. "No todas las compañías están preparadas para abordar una solución unificada, ya que muchas aún no tienen la capacidad de integrar una solución EDR que tienen que gestionar". Por tanto, aunque la evolución señala un horizonte integrado, "a corto plazo, debemos mantener el uso de ambas soluciones por separado para adaptarnos a las necesidades de las empresas actuales, mante-

niendo las soluciones de EDP, pero que sean capaces de hacer frente también a amenazas cada vez más sofisticadas".

Y al XDR

El siguiente paso lo representan las soluciones XDR (*Extended Detection and Response*), para la detección y respuesta a incidentes de seguridad que analiza y correlaciona automáticamente información de seguridad compartida desde diversas fuentes. "XDR ayuda a las empresas a poder adaptarse al ritmo cambiante del panorama de amenazas actual, incluso para las organizaciones con limitaciones de recursos humanos o de otro tipo, proporcionando una forma inteligente y automatizada de unir soluciones tradicionalmente aisladas en un único sistema", relata José Luis Laguna. A su juicio, se irán implantando gradualmente. "Serán impulsadas por la inteligencia artificial y ayudarán a reducir el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR), a la vez que mejorará la eficiencia de las operaciones de seguridad detectando etapas más tempranas de la cadena de ciberataques y ofreciendo un amplio abanico de respuestas automatizadas para mitigar el impacto de un ataque y/o brecha de seguridad de forma más efectiva".

José de la Cruz asegura que se alinean con la realidad de los ataques que sufrimos actualmente: de múltiple vector, complejos y distribuidos. "Las organizaciones se enfrentan a amenazas sofisticadas que pueden eludir incluso la protección avanzada. Sin embargo, la mayoría de los enfoques actuales de detección y respuesta son aislados, incompletos y sobrecargan a los limitados equipos de seguridad con alertas desconectadas que carecen de información procesable. Los profesionales de seguridad informan actualmente de que pueden encontrar alertas críticas, pero no necesariamente tienen la claridad necesaria para resolver el problema debido a la falta de detalles adicionales".

"No todas las compañías están preparadas para abordar una solución unificada, ya que muchas aún no tienen la capacidad de integrar una solución EDR que tienen que gestionar"

Según calcula Trend Micro solo el 30 % de las organizaciones se muestra muy confiada en que sus funciones de detección y respuesta a amenazas pueden funcionar a la velocidad necesaria para mantenerse al día con las amenazas en los próximos 12-24 meses. De media, las organizaciones y los sobrecargados equipos de TI ignoran el 32% de las alertas de seguridad. "Si se usan tecnologías XDR las empresas disfrutan de mejores resultados de seguridad. Por ejemplo, generalmente son capaces de restaurar en horas frente a días en un ratio del 83 % frente al 66 %", calcula de la Cruz.

El enfoque global que implica el uso de los servicios XDR da respuesta, explica Carlos Galdón, a dos situaciones. "En primer lugar, al funcionamiento actual de las empresas. Hoy en día las compañías están trabajando en un modelo híbrido de *endpoints*, en el que ya no solo se cuenta con ordenadores, sino que también se añaden tabletas, *smartphones*, etc. Además, el modelo de integración *cloud* y la dispersión de los trabajadores que se conectan en remoto desde cualquier lugar, ya no solo desde casa sino desde cualquier otra ubicación a la que se desplacen y desde redes menos seguras, aumenta la complejidad". Según los informes State of IT Security 2021 y State of Ransomware 2021 de Sophos los ciberataques crecieron en un 54 % el año pasado y de estos ataques, el 50 % fueron demasiado sofisticados para que los equipos de TI de las empresas pudieran hacerles frente, lo que exige esta ciberseguridad entendida "como un estrategia global e integrada en la que no podemos ya segmentar la ciberprotección por dispositivos o procesos, sino que tenemos que encaminar la protección de las empresas en un modelo unificado".

2022

Todo apunta a que la poderosa inversión desplegada en los últimos años en el entorno del puesto de trabajo continuará en los próximos meses. "Seguirá siendo prioritario", asegura Carlos Vieira. "Cada vez estamos viendo una mayor adopción de soluciones de EDR en España y durante este año los clientes y *partners* empezarán a demandar más herramientas XDR que permitan extender la detección y la respuesta más allá, sincronizando la protección del perímetro con el *endpoint*". Espera que los CIO ya hayan entendido que invertir en ciberseguridad es una tarea continua. "De

una vez por todas deben entender que es tan importante tener una buena cadena de producción como mantener la seguridad de la misma. Es tan importante tener unos usuarios protegidos en su perímetro como lo es que estén protegidos cuando están en teletrabajo".

Vieira preconiza que en este entorno de la seguridad, los MSP van a jugar un papel crucial para las empresas. "Aquellas con menos recursos (económicos, técnicos, humanos) pueden encontrar en ellos una respuesta a sus problemas".

También Alfonso Ramírez apuesta por una mayor inversión. "La digitalización, el trabajo remoto y el uso creciente de la nube genera una complejidad que puede impactar en la visibilidad de las amenazas y la respuesta a los incidentes de las organizaciones", razona. Una complejidad que estimula la inversión. "Garantizar la seguridad de unos entornos corporativos cada vez más complejos se ha convertido en un verdadero reto para casi la mitad de las empresas europeas (43 %), solo por debajo de la preocupación por la protección de los datos (55 %)", argumenta.

Los fondos NextGenerationEU representan una enorme oportunidad para el segmento de la seguridad en este 2022. David Sánchez García, director comercial de ESET España, destaca su impacto sobre las pymes. "Se calcula un montante en torno a los 4.459 millones de euros en ayudas directas que se espera que alcancen a 1 millón y medio de pymes españolas".

El despliegue del 5G también influirá en el panorama de seguridad de este año. "Esta tecnología dotará de más caos al entorno, al multiplicar la superficie de exposición de nuestras organizaciones de forma dramática", alerta Sergio Martínez.