



Un entorno seguro: la base para la Transformación Digital

V-Valley
★★★★★ the Value of esprinet



CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

[Adobe Acrobat Reader](#) y [Adobe Flash Player](#)

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluida en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

Este es un documento producido por



www.ituser.es

www.itreseller.es

Accede a nuestras publicaciones digitales



La ciberseguridad afronta el reto de proteger y respaldar el negocio

Un entorno seguro: la base para la Transformación Digital

El mundo de la seguridad es tan complejo como apasionante. Además, lamentablemente, ha estado de total actualidad en las últimas semanas por el incidente WannaCry, si bien es una de esas áreas del negocio que nunca pasan de moda, porque es una prioridad indiscutible para cualquier empresa. Eso sí, en los últimos tiempos hemos ido viendo cómo cambia la aproximación a este terreno, porque nos enfrentamos a una realidad totalmente diferente que no puede ser defendida con la visión tradicional. Conozcamos los detalles.



Y para poder conocer en profundidad todo lo relacionado con las tendencias en seguridad, hemos querido recurrir a algunos expertos que nos han ofrecido su visión sobre este particular. En este sentido, una de las compañías a las que hemos recurrido ha sido Check Point Software, desde donde Fernando Herrero, director de Canal, nos pone sobre la pista de las tendencias que desde su compañía detectan en el mercado. En palabras de Herrero, “el mundo de la seguridad está en constante cambio. Los ciberdelincuentes no descansan

en su empeño por encontrar nuevas formas de ataques que penetren en los endpoints y los servidores de las empresas. Por esta razón, tenemos que actualizar constantemente nuestras tendencias, para poder adelantarnos a los malhechores. En la actualidad, la batalla contra el cibercrimen se celebra sobre todo en cinco frentes: dispositivos móviles, Internet de las Cosas, infraestructuras críticas, prevención de amenazas y cloud”.

Por su parte, desde Kaspersky Lab nos advierten de que, “como hemos observado con WannaCry, el último ciberataque a empresas de todo el mundo, el cibercrimen no desaparece, sino que cada vez es más preocupante y aparecen nuevas amenazas que ponen en riesgo la seguridad corporativa de las empresas. Como pronosticamos a principios de año, el ransomware iba a ser el protagonista en cuanto a ciberamenazas, además de los implantes pasivos, que casi no muestran señales de infección en el sistema, y se pondrán de moda y crecerá la “mercantilización” de los ciberataques financieros con recursos especializados. El ciberespionaje se dirigirá a dispositivos móviles e Internet of Things; las infecciones cortas serán más populares y el



ransomware, como el ataque de hace unas semanas, seguirá aumentando”.

Desde Microsoft nos explican que la seguridad es una parte más de una tecnología que puede transformar el panorama empresarial. “La tecnología”, nos apuntan, “tiene un carácter disruptivo que hace posible nuevos modelos de negocio, habilita nuevas fuentes de ingresos para las empresas y está dando forma a un nuevo panorama industrial. Garantizar la seguridad y la privacidad cumpliendo con la normativa vigente es fundamental en el proceso

de transformación digital de las empresas. En un contexto en el que cada vez más empleados traen sus propios dispositivos a sus empresas, usan apps y acceden a información confidencial, la protección de las empresas requiere un nuevo enfoque. El crecimiento de los ciberataques en número e impacto directo en el negocio de las empresas ha hecho que la seguridad pase a ocupar la atención de la más alta dirección”.

En una línea similar se expresa Alberto Tejero, director comercial de Panda

Security, al señalar que las empresas “sufren y sufrirán más ataques y cada vez más avanzados. Los ciberdelincuentes están continuamente buscando puntos débiles para entrar en las redes corporativas, y, una vez dentro, utilizan movimientos laterales para acceder a la información que buscan para robarla. Además, el ransomware, gran protagonista de 2016, seguirá siéndolo también a lo largo de este 2017, junto con los ataques DDoS. También hay que resaltar que vivimos un momento muy delicado en las relaciones internacionales. Diferentes amenazas de guerras comerciales, espionaje, arancelarias, que pueden tener grandes -y graves- efectos en el campo de la seguridad informática, pudiendo entorpecer las

iniciativas existentes de compartición de información con estándares y protocolos de actuación internacionales”.

“Por otro lado”, añade, “a nivel de usuarios particulares, IoT es la próxima pesadilla de seguridad, ya que estos dispositivos no han sido diseñados con la seguridad como punto fuerte; y, cómo no, los móviles, donde los dispositivos Android se llevan la peor parte”.

Desde el punto de vista de SonicWall, “y con referencia a nuestro informe anual de seguridad 2106”, señalan, “hemos observado como tendencias que el volumen de muestras únicas de malware descendió hasta los 60 millones, un descenso del 6,25%; que la creación de malware para el Punto de Venta descendió un 93% desde 2014;

LA SEGURIDAD, SEGÚN... CHECK POINT

En palabras de Fernando Herrero, “nuestra propuesta pasa por proteger absolutamente todos los puntos débiles de la compañía. Para esto, lo primero que hacemos es una consultoría a cada empresa. Después, les decimos los agujeros que existen en su estrategia de seguridad, y les ofrecemos una oferta completamente personalizada, de acuerdo con sus necesidades. En el caso de los miembros del canal de distribución, nos aseguramos de ofrecerles tecnologías que no protejan solo su información, sus equipos y sus redes, sino también toda la relativa a los demás eslabones de la cadena”.

¿Son efectivas las estrategias tradicionales?

Para Alberto Tejero, “hay que tener en cuenta que el paradigma de la seguridad digital ha cambiado. Las fórmulas tradicionales de catalogación de virus y amenazas han dejado de ser efectivas. La evolución de las amenazas y la multiplicación de endpoints (PC, móvil, tablet...) requieren un servicio basado en el análisis y monitorización continua de la actividad de las aplicaciones”. De la misma opinión son los responsables de Spamina, que señalan que “las medidas tradicionales de seguridad en el correo electrónico, como son el antivirus y el antispam, ya no son suficientes para los usuarios. El email y la mensajería instantánea son los canales más accesibles para la difusión de malware y los hackers diseñan cada vez amenazas más sofisticadas, difíciles de detectar. Hace

falta implementar soluciones con tecnologías avanzadas que permitan analizar los ficheros y las url que aparecen en tiempo real, justo cuando el usuario intenta acceder”. “Si hablamos por estrategias tradicionales, la utilización de un firewall clásico o un UTM, obviamente, no”, apuntan desde SonicWall, y añaden que “es fundamental mantener una defensa multicapa y, sobre todo, realizar toda la inspección en cada capa sobre el tráfico cifrado y aportar tecnología de Sandboxing multimotor para la protección de ATP y amenazas día cero, todo esto con entender la organización como un todo, y dotar de todas las capas de seguridad necesarias en los accesos remotos, y en la recepción y envío de correo”.

La única opinión discordante, pero con matices, la ofrece Fernando Herrero, que comenta que estas estrategias tradicionales “siguen siendo importantes en la estructura de seguridad de una empresa. De hecho, consiguen bloquear casi el 100% de todos los ataques conocidos que intentan penetrar en los servidores y los endpoints de las compañías. El problema viene con las amenazas desconocidas y las de día cero que, al no haberse detectado nunca antes, no pueden ser interceptadas. Por esto, las compañías deben implementar soluciones avanzadas, ya que no se basan en detectar las amenazas, sino que las previenen. Esto lo hacen con tecnologías como el sandbox avanzado, la extracción de amenazas y la detección a nivel de CPU”.

que el tráfico encriptado Secure Sockets Layer/Transport Layer Security ha aumentado un 38% año tras año, situándose en un promedio del 60% del total del tráfico; que los cibercriminales desviaron su atención hacia nuevas amenazas, incluyendo los ataques ransomware, que han aumentado 167 veces año tras año; y que los dispositivos vinculados al Internet de las Cosas han creado un nuevo vector de ataque,

abriendo la puerta a ataques de negación de servicio distribuidos a gran escala”.

Por último, desde Spamina, nos recuerda que “en los últimos años, las empresas han evolucionado su forma de comunicación utilizando herramientas que agilicen la interlocución, como es el caso de la mensajería instantánea a través de dispositivos móviles. Esto abre nuevas puertas de acceso a ci-

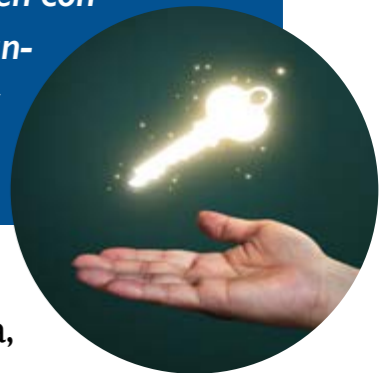
berdelincuentes, además de provocar un incremento de errores internos, ya sean intencionados o no, que causan desvío o pérdida de la información”.

Pero antes de terminar, hemos querido pulsar la opinión de un mayorista, eslabón imprescindible en la cadena de la seguridad. Y, precisamente, la llegada de una nueva normativa en cuestión de protección de datos es una de las cosas que destacan desde V-Valley. Así,

tal y como nos explican desde la firma,

“hay una gran tenden-

cia hacia la protección de las amenazas desconocidas. Hoy en día, el antivirus y el firewall tradicional no son 100% efectivos y las soluciones que hay actualmente en el mercado basadas en el análisis de comportamientos y en los firewalls de nueva generación, demuestran que estamos en un sector



LA SEGURIDAD, SEGÚN... KASPERSKY LAB

Tal y como nos explican desde el fabricante, “el enfoque efectivo en las estrategias de seguridad pasa por tratar la amenaza con un conjunto de soluciones y tecnologías de protección multi-capa. Ya no se trata sólo de prevenir incidentes, sino de predecir, detectar y responder a ellos. Y hacerlo de forma flexible, fiable y efectiva, teniendo en cuenta que la seguridad no es un estado, sino un proceso en constante evolución”.

que avanza rápidamente y que necesita estar al día de las soluciones actuales. Además, el nuevo reglamento europeo de la protección de los datos de sus ciudadanos (GDPR) obliga a hacer conscientes a los dueños de las empresas de la importancia de asegurar los datos de las mismas, para cumplir la legislación y evitar posibles sanciones económicas. Por último, el movimiento de las empresas hacia la nube, como Azure de Microsoft, abre nuevas necesidades de securizar entornos híbridos, donde la red no está tan definida como tradicionalmente”.

PRINCIPALES AMENAZAS

Para Alberto Tejero, “la mayoría de amenazas que existen hoy en día son aquellas que buscan algún beneficio económico, directo o indirecto. Uno de los tipos de ataques más prevalentes hoy en día en el mundo de la



empresa es el del ransomware, que secuestra la información y pide un rescate para poder recuperarla. A continuación, tenemos ataques protagonizados por troyanos cuyo principal objetivo es el robo de información confidencial o robo de credenciales. También hay amenazas que tratan de comprometer cuentas de correo corporativo. Es

una forma más evolucionada de realizar phishing. En este tipo de ataques hay más conocimiento acerca de las víctimas y alguien se hace pasar por el CEO o por un alto ejecutivo e instruye a una persona para que realice determinadas acciones. Por ejemplo, realizar una transferencia a una determinada cuenta”.

Una opinión similar tienen en Spamina, desde donde nos explican que “tanto las empresas como los usuarios están expuestos al robo de su información por ciberdelincuentes para enriquecerse. En el ámbito empresarial el impacto va más lejos aún, siendo la propiedad intelectual y la reputación dos factores a tener muy en cuenta. No es sólo el valor de lo que han robado, sino el impacto futuro en la actividad empresarial”.

Y es que, como nos recuerdan desde SonicWall, “las empresas y los usuarios con acceso a internet están expuestos a todas las actividades de los cibercriminales, desde las suaves, como que sus equipos estén comprometidos y pertenezcan a una red de bootnet, para ser utilizados como servidores de envío de spam o unidades de ataques de denegación de servicio distribuido,

LA SEGURIDAD, SEGÚN... SONICWALL

Según la estrategia de SonicWall, “lo primero es definir la organización como un todo, y abordar todas sus áreas, con soluciones de seguridad colaborativas, para minimizar al máximo las posibles brechas de seguridad”. Se trata de una estrategia que abarca varios elementos, tales como “securizar la red, una solución robusta de acceso remoto de usuarios, utilización de soluciones de seguridad eficaces en el punto de acceso, y protección de los servidores de correo”.

El eslabón más débil

Los responsables de Kaspersky Lab tienen claro que “la seguridad de una empresa es tan fuerte como su eslabón más débil y normalmente suelen ser los empleados. En este caso, la formación y conciencian en materia de seguridad debería incluirse como parte integral de las estrategias de seguridad con el fin de prevenir y minimizar los riesgos”.

Para Fernando Herrero, “un gran porcentaje de los ataques que sufren las empresas tienen su desencadenante en un archivo descargado por un empleado. Basándonos en esto, podríamos decir que el eslabón más débil es el factor humano. ¿Cómo evitar que se conviertan en aliados involuntarios de los ciberdelincuentes? El primer paso es la concienciación

y la formación de las plantillas. Si los trabajadores tienen unos conocimientos básicos de seguridad, dejarán de caer en las trampas puestas por los hackers, como los mensajes de phishing. Además, esta educación debe ser cumplimentada con un entorno seguro de trabajo, que les impida descargar cualquier documento sospechoso o acceder a un link peligroso”.

La misma opinión tienen los responsables de SonicWall, que comentan que “todos los ataques de Spear Phishing, ingeniería Social... tienen como destinatarios a los usuarios. La forma de solventarlo o minimizarlo es realizar una formación bastante básica, sobre la recepción de mensajes, sus enlaces y sus adjuntos. Otro aspek-



to es la prevención de utilización de dispositivos de almacenamiento extraíble” por parte de estos usuarios. “El desconocimiento, la falta de concienciación y la rápida difusión de los ataques”, apuntan desde Spamina, y añaden que “los errores internos, generalmente no intencionados, son los más extendidos. Por eso, es importante que las empresas implementen soluciones que permitan administrar políticas automáticas para la prevención de la fuga de datos”.

Por último, Alberto Tejero indica que “la movilidad y la multiplicación de endpoints suponen un reto a la seguridad de las compañías. La tecnología es una herramienta posibilitadora de la flexibilidad laboral. Pero hay que dotarse de las herramientas necesarias para garantizar la seguridad”.

hasta los más peligrosos, como ataques de día cero, ransomware, o malware en general”.

Para los responsables de Kaspersky Lab, “el crecimiento de ciberamenazas, cada vez más preparadas y dañinas, hace que tanto empresas como usua-

rios tengan que estar en alerta constante. Desde ataques DDoS a APT, pasando por el ransomware, como el ataque global de este mes, son algunas de las amenazas a las que más están expuestas las organizaciones. Los usuarios tampoco se libran de los

ciberdelincuentes, y pueden ser víctimas de numerosas amenazas. Por ejemplo, existe un tipo de malware en Android que, además de robar datos financieros de mensajes de texto y de voz, es capaz de superponer ventanas que simulan páginas oficiales de inicio de sesión

para hacerse con información personal y bancaria de los usuarios. También las infecciones por ransomware, cada vez más, afectan a usuarios finales a través de dispositivos móviles”.

En este sentido, desde Check Point añaden que “las personas y las com-

pañías tienen que hacer frente en su día a día a ciberamenazas de todos los tipos. En los últimos meses, han tomado mucha fuerza los Exploit Kits, programas maliciosos que descubren y explotan vulnerabilidades. Cuando lo hacen, descargan en el equipo infectado ransomware como WannaCry o gusanos como Slammer. Otro vector de ataque importante es el phishing, y su variante móvil smishing. A través de correos fraudulentos y webs falsas, los ciberdelincuentes engañan a los usuarios para que den información personal o instalen malware. Tampoco conviene olvidarse de las botnets, conjuntos de robots que existen en casi todas las empresas, y que se alojan en los equipos infectados a la espera de que su creador les dé una instrucción, como lanzar un ataque DDoS contra una dirección IP o robar información personal o corporativa”.

¿CÓMO RESPONDER A ESTAS AMENAZAS?

Según nos indica Fernando Herrero, desde Check Point, “al igual que las empresas están alcanzando en los últimos años la transformación digital y la omnicanalidad, también lo hacemos nosotros. Por esa razón, hemos creado

LA SEGURIDAD, SEGÚN... MICROSOFT

Según comentan desde Microsoft, la compañía cuenta con tres elementos fundamentales. Primero, “incorpora la seguridad en los productos y servicios desde el principio, ofreciendo una plataforma ágil y robusta, capaz de actuar más rápido para detectar las amenazas y responder a las infracciones de seguridad incluso en las organizaciones de mayor tamaño. En segundo lugar, la inteligencia de las inmensas fuentes de datos de Microsoft, le confiere una visión única que le permite identificar modelos sospechosos a través de machine learning e inteligencia humana para detectar pronto las amenazas y responder con rapidez. Y, tercero, Microsoft trabaja con la industria e identidades compartiendo información sobre vulnerabilidades con más de 50 partners, de forma que los clientes puedan protegerse lo más rápido posible”.



la infraestructura de seguridad del futuro, Check Point Infinity. Infinity no se encarga solo de proteger los ordenadores que hay en la sede o la sucursal de una empresa, sino también todos los dispositivos móviles que utilizan sus empleados y los entornos cloud. A través de una única plataforma de seguridad, una prevención de amenazas anticipada y un sistema de protección consolidado, Check Point Infinity permite a las empresas tomar el control de su seguridad”.

Para Kaspersky Lab, “vivimos en un mundo donde la pregunta ya no es si seremos atacados, sino cuándo y cómo de rápido serás capaz de recuperarte. No hay una única tecnología de protección perfecta y nunca la habrá. El enfoque efectivo en las estrategias de seguridad pasa por tratar la amenaza con un conjunto de soluciones y tecnologías de protección multi-capa. Ya no se trata sólo de prevenir incidentes, sino de predecir, detectar y responder a ellos. Y hacerlo de forma flexible, fiable y efectiva, teniendo en cuenta que la seguridad no es un estado, sino un proceso en constante evolución”.

Desde el punto de vista de soluciones de seguridad, apuntan desde SonicWall, “lo primero es definir la organi-

La visión del mayorista

Para conocer esta visión del mayorista, hemos conversado con V-Valley, cuyos responsables nos indicaban que “Nuestro papel principal es trabajar con los fabricantes para llegar a todos los distribuidores de informática que quieran especializarse en el mercado de la seguridad TI. La capacitación de partner y el soporte antes, durante y después del proceso de venta, es nuestra prioridad. De este modo, independientemente del tamaño del reseller, siempre estará acompañado y con soportado para garantizar el éxito de cada proyecto”.

En el caso específico de V-Valley, “nuestra especialización y capacitación, junto con la estrecha relación que tenemos con los fabricantes de seguridad con los que trabajamos, permite que trabajemos con nuestros resellers para detectar en sus clientes la oportunidad de negocio y la necesidad de estar protegidos. Les ofrecemos mensajes personalizados por cada tamaño de empresa

al que se dirigen de modo que puedan enfocar la venta directamente a las necesidades y preocupaciones que tiene cada tipo de empresa. No es el mismo el mensaje el que de-



ben utilizar los resellers que trabajan los sectores de educación, que por ejemplo los que se dedican al sector industria o a verticales específicos como el de los ERP”.

Junto con esto, “proporcionamos todas las herramientas y recursos necesarios para generar demanda, desde material para detectar oportu-

nidades, generar campañas de telemarketing y contenido para realizar webinars o eventos presenciales con sus clientes finales. Tenemos disponibles consultores pre-preven-

ta certificados y especializados que dimensionarán adecuadamente la solución y, en el caso de ser necesario, preparan un proceso de prueba o piloto para que la tecnología sea probada in-situ. Demostrar lo que la tecnología es capaz de hacer hoy en día y hacer conscientes de las amenazas y problemas que hay en

las redes informáticas, es un factor clave que acelera el proceso de decisión de compra. Por último, está la parte de puesta en marcha e implementación, donde nuestro equipo de servicios tecnológicos está a disposición de todos los partners que aún no se sientan capacitados para hacer este proceso de forma autónoma. Independientemente de si el reseller decide formarse técnicamente, nosotros apoyamos también la fase de implementación y de transferencia del conocimiento”.

Con ello, “cualquier reseller que vea que hay interés o necesidad de implementar soluciones de seguridad en sus clientes y quiera explorar esta oportunidad, puede trabajar conjuntamente con nuestro equipo que dará visibilidad el más adecuada por tamaño de cliente final y de sector vertical de los mismos. A partir de ahí es el reseller el que decide cuánto quiere capacitarse y a qué ritmo”.

zación como un todo, y abordar todas sus áreas, con soluciones de seguridad colaborativas, para minimizar al máximo las posibles brechas de seguridad. Primero, securizar la red con un firewall de nueva generación con todas las capas de protección necesarias, antimalware, filtro de acceso a web, IPS-IDS, antiBootnet, GeolP, sandboxing de nueva generación multimotor y, sobre todo, teniendo la capacidad de realizar la inspección profunda de paquetes sobre tráfico cifrado SSL /TLS y SSH, sin limitación de tamaño, ni de puertos ni de protocolos. A esto hay que añadir, una solución de acceso remoto de usuarios robusta con doble factor de autenticación, con mecanismos de control de EndPoint, basado en las propias reglas de la compañía, con capacidad de seleccionar las aplicaciones a utilizar corporativas y que estas mismas gestionen el acceso a través de túneles SSL securizados. Además, utilización de soluciones de seguridad de EndPoint eficaces y, a ser posible, de diferente tecnología que las que se tienen en el perímetro y en la red. Y, junto con ello, protección de los servidores de correo, con soluciones altamente eficaces, con diferentes motores de antivirus y con sandbo-



LA SEGURIDAD, SEGÚN... PANDA SECURITY

En opinión de Alberto Tejero, “en Panda Security apostamos por un enfoque disruptivo, proactivo y estructuralmente diferente al de los productos de seguridad tradicionales. Con Adaptive Defense ofrecemos seguridad para el endpoint a través de una plataforma cloud basada en la investigación, análisis, categorización y correlación permanente en tiempo real del comportamiento y el contexto de apertura de todas las aplicaciones que se intentan ejecutar en cada equipo. Adaptive Defense es capaz de obtener automáticamente una clasificación determinista para el 99,99% de los casos de forma directa. Los casos restantes se procesan mediante un equipo de técnicos especialistas en seguridad cuya misión es establecer el riesgo de esas aplicaciones y, sobre todo, mejorar el sistema de clasificación para que sea capaz de resolver automáticamente estos nuevos casos en el futuro”.

xing multimotor de nueva generación y con capacidad de encriptación de los correos”.

Por su parte, Microsoft promueve “una actitud renovada en materia de seguridad. La mayoría de las organizaciones tienen una estrategia contra las amenazas basada en 3 pasos: proteger, detectar y responder. Este modelo no ha cambiado en los últimos 20 años y todavía es relevante hoy. Sin embargo, hemos cambiado la forma en que se ejecuta cada uno de ellos en todos los productos: proteger, con funcionalidades que protegen la identidad, datos, aplicaciones, dispositivos e infraestructura, tanto si es en la nube como si no, y esto implica considerar todos los end-points críticos desde sensores al datacenter; detectar, a partir de señales específicas, monitorización de comportamientos y machine learning que permitan una respuesta inmediata; y responder, cerrando el gap entre el descubrimiento y la acción”.

Así, Microsoft está construyendo una plataforma “con una aproximación holística que tiene en cuenta todos los puntos críticos en un mundo regido por la movilidad y la nube. La inversión en esta plataforma se hace en cuatro categorías: identidad, aplicaciones y da-

LA SEGURIDAD, SEGÚN... SPAMINA

En Spamina, “nuestra visión es ir un paso por delante de los hackers. Nuestra estrategia se basa en considerar la comunicación empresarial como un todo, entender la cadena y los procesos de colaboración, y ofrecer una solución flexible, fácil de implementar, que sea accesible en todos los eslabones de esta cadena. La oferta de Spamina va desde soluciones para la protección del correo electrónico a soluciones de archivado y cumplimiento de normativas, y está disponible para todos los servidores de correo en modo nube pública, privada o híbrida. Además, esta experiencia nos ha llevado a desarrollar nuestra propia solución de correo, Parla con la seguridad integrada”.



tos, dispositivos e infraestructura, con un enfoque inclusivo de la tecnología que nuestros clientes ya estén utilizando. Microsoft cuenta con una amplia inteligencia en materia de seguridad cibernética creada a partir de los miles de millones de puntos de datos de las diversas fuentes que analiza y cuenta con un ecosistema de partners que mejoran los estándares del sector permitiendo a sus clientes a llevar a cabo sus procesos de transformación digital de una forma segura”.

En opinión de Spamina, “el reto pasa por movilizar las infraestructuras al Cloud. Un proceso que, si bien está adoptado por la mayor parte de las compañías, aún mantiene un nicho re-

celoso al cambio. El Cloud permite a las compañías aligerar costes de gestión e infraestructuras, pero, sobre todo, la flexibilidad de adaptar las soluciones de seguridad a los requerimientos del negocio de manera inmediata”.

Finaliza Alberto Tejero, Panda Security, indicando que disponen de “una fórmula que visibiliza y controla todo lo que sucede en el endpoint: software ejecutado, aplicaciones vulnerables y comportamiento de usuarios para ofrecer una solución 360. Con este tipo de protección podemos utilizar la tecnología para que nos ofrezca flexibilidad, ya que podemos ofrecer un altísimo nivel de seguridad en todos los dispositivos desde los que trabajemos”.

ENLACES DE INTERÉS

⇒ [Check Point Software](#)

⇒ [Kaspersky Lab](#)

⇒ [Microsoft](#)

⇒ [Panda Security](#)

⇒ [Spamina](#)

⇒ [SonicWall](#)

⇒ [V-Valley](#)