SOPHOS

El problema de la falta de conocimientos de ciberseguridad en las pymes

Analizamos las repercusiones directas de la escasez de personal cualificado en ciberseguridad en las pequeñas y medianas empresas y cómo abordar esos retos dentro de las limitaciones presupuestarias y de recursos.

Monográficos de Sophos. Octubre de 2024

Introducción

La escasez mundial de competencias en ciberseguridad es bien conocida y está bien documentada. Tampoco es un problema que vaya a desaparecer a corto plazo, por lo que es esencial que las pequeñas y medianas organizaciones tomen medidas para paliar su impacto.

Comprender el reto es el primer paso para hacerle frente. Este informe comparte los resultados de una encuesta independiente realizada a profesionales en primera línea de todo el mundo, y revela cómo la escasez de competencias repercute en el día a día de las pymes. A partir de estas conclusiones, ofrece una guía práctica para abordar estos retos dentro de las limitaciones presupuestarias y de recursos existentes. También estudia las soluciones de Sophos que permiten a las organizaciones pequeñas obtener mejores resultados en ciberseguridad.

Acerca de la encuesta

Sophos encargó una encuesta independiente y desvinculada de cualquier proveedor a 5000 profesionales de TI/ciberseguridad en primera línea en 14 países. 1402 encuestados trabajan en organizaciones con entre 100 y 500 empleados, el segmento considerado pequeñas y medianas empresas (pymes) en este informe. La investigación se realizó durante el primer trimestre de 2024.

Las organizaciones pequeñas sufren de forma desproporcionada los efectos de la escasez de personal cualificado

La falta de competencias pesa mucho y de forma desproporcionada sobre las pymes. La encuesta revela que **las organizaciones con menos de 500 empleados consideran que la escasez de conocimientos y experiencia internos en ciberseguridad son su segundo mayor riesgo de ciberseguridad**, solo superado por las amenazas de día cero. En cambio, para las que tienen más de 500 empleados, ocupa el séptimo lugar.

Clasificación relativa de la "escasez de conocimientos/experiencia internos en ciberseguridad" como riesgo de ciberseguridad para la empresa

PYMES (n=1402)	ORGANIZACIONES MÁS GRANDES (n=3598)	
100 - 500 EMPLEADOS	501 - 1000 EMPLEADOS	1001 - 5000 EMPLEADOS
N.º 2	N.º 7	N.º 7

¿Quiénes o cuáles considera que son los tres mayores riesgos de ciberseguridad para su organización? Posición relativa de la "escasez de conocimientos/experiencia internos en ciberseguridad" entre las respuestas clasificadas en primer lugar (números base en la tabla)

Aunque organizaciones de todos los tamaños se ven afectadas por la escasez de personal cualificado, está claro que las pymes acusan más su impacto. Los riesgos que ocupan un lugar destacado para las organizaciones grandes, como la escasez de herramientas de ciberseguridad (2.º mayor riesgo percibido por las que tienen entre 501 y 1000 empleados) y el robo de datos de acceso y credenciales (2.º mayor riesgo percibido por las que tienen entre 1001 y 5000 empleados), son preocupaciones secundarias para las empresas pequeñas que lidian con el reto más básico de disponer de personal para gestionar sus inversiones actuales.

Escasez de competencias: un doble desafío

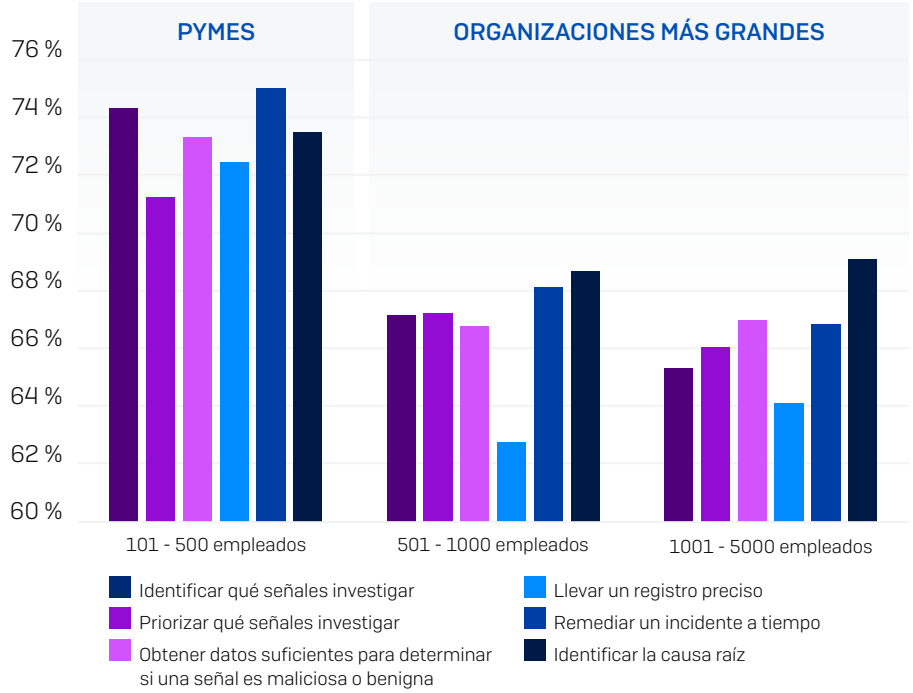
La realidad que se esconde tras la escasez de competencias es que no hay suficientes profesionales cualificados en ciberseguridad. Esto afecta a las pymes de dos maneras.

Falta de experiencia

Las ciberamenazas y la tecnología de seguridad son complejas. Gestionar bien la ciberseguridad es una competencia avanzada que requiere altos grados de especialización, y el listón está cada vez más alto. A medida que los ciberataques se vuelven más complejos, se necesita un mayor nivel de conocimientos para detenerlos.

La encuesta revela que **al 96 % de los responsables de pequeñas empresas les resulta difícil al menos un aspecto de la investigación de alertas sospechosas**. Aunque las organizaciones más grandes también suelen tener dificultades con las operaciones de seguridad, el reto es mayor en las pymes.

Porcentaje de organizaciones para las que las tareas de operaciones de seguridad suponen un reto



Si su organización investiga las alertas de seguridad a nivel interno, ¿en qué medida suponen un reto para su organización los siguientes pasos a la hora de investigar alertas sospechosas? "Muy difícil" y "Bastante difícil" (números base en el gráfico)

La practicidad de ampliar los conocimientos en materia de ciberseguridad supone un reto particularmente difícil para quienes trabajan en pymes. Cuando solo hay un puñado de personas en el equipo de TI/seguridad, es todo un reto dedicar tiempo a la formación continua de forma regular. Además, con menos compañeros de trabajo, los empleados tienen menos oportunidades de aprender entre ellos.

Falta de capacidad

Los adversarios no trabajan de 9 a 5, lo que convierte a la ciberseguridad en una necesidad constante. De hecho, el 91 % de los ataques de ransomware se inician fuera del horario laboral estándar, ya que los atacantes buscan infiltrarse en las organizaciones sin ser detectados[1].

La experiencia de los operadores de primera línea apunta a que ofrecer una cobertura de ciberseguridad 24/7 requiere un mínimo de cuatro o cinco empleados a tiempo completo para cubrir las vacaciones, las bajas por enfermedad y los fines de semana. Para la mayoría de las pymes, esto es sencillamente inalcanzable solo con recursos internos.

Como prueba de ello, la encuesta revela que **un tercio (33 %) de las veces, las pymes no tienen a nadie que supervise, investigue y responda activamente a las alertas**. Sin un experto en respuesta activo, las organizaciones pequeñas están totalmente expuestas a los ataques.

33 %

Porcentaje de veces que las pymes no tienen a nadie que supervise e investigue las alertas de seguridad

En el último año (incluyendo noches, fines de semana y días festivos), ¿qué porcentaje del tiempo tuvo su organización un experto en respuesta activo supervisando e investigando las alertas de seguridad? n=1402 organizaciones con 100-500 empleados.

1 Detenga a los adversarios activos: Lecciones desde la primera línea de combate cibernética, Sophos

El impacto de la falta de competencias en ciberseguridad en las pequeñas empresas

La escasez de conocimientos afecta a las pymes de muchas maneras. Son el segmento con más probabilidades de sufrir el cifrado de datos en un ataque de ransomware: el 74 % de los incidentes se saldaron con el cifrado de datos. Es muy probable que esto refleje su menor capacidad para detectar y detener a los adversarios antes de que el ransomware pueda ser detonado.

Porcentaje de ataques de ransomware que comportaron el cifrado de datos

PYMES (n=1402)	ORGANIZACIONES MÁS GRANDES (n=3598)	
100 - 500 EMPLEADOS	501 - 1000 EMPLEADOS	1001 - 5000 EMPLEADOS
74 %	72 %	66 %

Fuente: El estado del ransomware 2024, Sophos. ¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Sí. Números base en la tabla.

Además, si hay menos personas para compartir la carga que conlleva la ciberseguridad, las posibilidades de desgaste del personal son elevadas. En una investigación independiente encargada por Sophos en Asia Pacífico y Japón, **el 85 % de las organizaciones afirmaron que sus profesionales de ciberseguridad y TI sufrían agotamiento y desgaste**: casi 1 de cada 4 (23 %) lo experimentaba "a menudo" y, el 62 %, "de vez en cuando". Lo preocupante es que el 90 % de las empresas aseguran que el desgaste y el agotamiento han aumentado en los últimos 12 meses, y el 30 % de ellas afirman que el aumento ha sido "significativo".

85 %

Porcentaje de organizaciones con profesionales de ciberseguridad o TI que sufren agotamiento y desgaste

Cómo paliar las carencias en materia de conocimientos en las pymes

Contratar a más personas no es una opción viable para la mayoría de las pymes. Añadir personal de ciberseguridad es un gasto presupuestario considerable que repercutirá desproporcionadamente más en los presupuestos de personal de las organizaciones pequeñas que en los de las grandes. Paralelamente, las organizaciones compiten por un número limitado de expertos. Las personas con habilidades demandadas pueden ser selectivas y a menudo prefieren trabajar en organizaciones grandes que ofrecen mayores oportunidades de desarrollo entre iguales. La solución para hacer frente a los retos de experiencia y capacidad es trabajar con especialistas en seguridad externos y utilizar soluciones de ciberseguridad diseñadas para las pymes.

Trabajar con especialistas en seguridad externos

Contratar a especialistas en ciberseguridad externos suele ser la forma más fácil y rentable de añadir experiencia y capacidad. Los dos enfoques más comunes son el uso de servicios de detección y respuesta gestionadas (MDR) y de proveedores de servicios gestionados (MSP).

Por lo general, los servicios de **MDR** ofrecen búsqueda, detección y respuesta a amenazas 24/7 en todo su entorno prestadas por expertos. Los analistas monitorizan la organización, identifican y responden a las actividades sospechosas y neutralizan los ataques antes de que afecten al negocio.

Busque un proveedor que se adapte a sus necesidades y a la forma de trabajar que prefiera, tanto si desea externalizar por completo la detección y respuesta a amenazas como si prefiere colaborar con los analistas de su proveedor. Y, con unos presupuestos invariablemente ajustados, es importante trabajar con un servicio que pueda sacar partido de sus tecnologías de seguridad actuales, evitando así el coste y las interrupciones que supondría eliminarlas o reemplazarlas.

El problema de la falta de conocimientos de ciberseguridad en las pymes

Para ayudar a sufragar los servicios de MDR, puede aprovechar los ahorros en el ciberseguro. Los usuarios de MDR suelen ser considerados "clientes de primer nivel" por las aseguradoras porque corren un riesgo menor de presentar una reclamación. Como resultado, las aseguradoras suelen ofrecer descuentos importantes a las organizaciones que utilizan los servicios de MDR, dinero que puede destinarse a financiar el propio servicio.

Estudio de caso de Sophos: organización sin ánimo de lucro con 350 empleados
Una organización sin ánimo de lucro de Carolina del Norte (EE. UU.) con 350 empleados pudo reducir la prima de su ciberseguro en 8000 USD porque utilizaban el servicio Sophos MDR. Como su suscripción anual a Sophos MDR ascendía a 8467 USD, pudieron disfrutar de una detección y respuesta a amenazas 24/7 a cargo de expertos por un gasto incremental de solo 467 USD.

Durante muchos años, los **MSP** han prestado soporte de TI y ciberseguridad a las empresas pequeñas, asumiendo las funciones de su equipo interno. A medida que las ciberamenazas aumentan en complejidad, las organizaciones medianas optan cada vez más por trabajar con MSP para complementar sus recursos internos.

La MDR y los MSP no son mutuamente excluyentes; un estudio independiente de Sophos revela que la mayoría de los MSP (81 %) ofrecen servicios de MDR[2], lo que le permite beneficiarse de ambas capas de soporte con un único proveedor. Algunos MSP prefieren ofrecer servicios de MDR únicamente de forma interna, mientras que otros recurren a proveedores externos especializados en MDR.

Opte por soluciones diseñadas expresamente para las pymes

La mayoría de las soluciones de ciberseguridad están diseñadas y desarrolladas para grandes organizaciones con amplios equipos para desplegarlas y gestionarlas. Aunque el uso de soluciones de nivel empresarial puede parecer atractivo, a las organizaciones pequeñas a menudo les cuesta ver los beneficios en materia de seguridad y retorno de la inversión (ROI) de estas soluciones, ya que no son capaces de utilizarlas con eficacia.

En su lugar, opte por herramientas de seguridad que sean técnicamente avanzadas pero diseñadas para que los equipos de TI sobrecargados puedan usarlas con facilidad. Cambiar el enfoque de compra no debería aumentar el gasto, e incluso puede brindar la oportunidad de reducir tanto los gastos tecnológicos como los de gestión. Al sopesar las soluciones de seguridad, tenga en cuenta tanto las características de la plataforma como las de los productos.

Plataforma

- Una plataforma de ciberseguridad es una herramienta centralizada que le permite desplegar, supervisar y gestionar varias soluciones de ciberseguridad en un solo lugar, por ejemplo, la protección para endpoints/seguridad antivirus, la seguridad del correo electrónico y el firewall.
- La consolidación de las soluciones de ciberseguridad en una única plataforma reduce considerablemente la carga administrativa diaria: no es necesario ir de consola en consola para ver qué ocurre. Reducir el número de proveedores con los que trabaja ayuda a reducir los gastos de gestión de proveedores.
- Una plataforma eficaz también permitirá que sus soluciones de seguridad funcionen de forma conjunta, compartiendo telemetría, políticas basadas en el usuario y mucho más para reforzar sus ciberdefensas.

Funciones de los productos

- Los proveedores ofrecen largas listas de prestaciones y capacidades en sus sitios web. Antes de valorar las soluciones, tómese su tiempo para comprender exactamente lo que necesita y lo que no para evitar pagar por tecnologías que no aprovechará.
- Para sacar el máximo partido a sus inversiones en ciberseguridad, debe poder desplegarlas y utilizarlas con eficacia. Apueste por soluciones que implementen automáticamente los parámetros de configuración recomendados desde el primer día, de forma que no tenga que llevar a cabo una configuración manual laboriosa y arriesgada. Además, busque controles intuitivos diseñados para entornos reales que sean fáciles de usar.
- Los errores de configuración de las herramientas de seguridad son un riesgo importante para las pymes. Mantener una buena postura es esencial para una protección continua, lo que significa elegir soluciones que ofrezcan una visibilidad clara de los despliegues por debajo de los niveles óptimos y asistencia para una rápida solución.
- Como empresa pequeña, es poco probable que su equipo pueda centrarse únicamente en la ciberseguridad. Por eso es especialmente importante elegir soluciones que respondan automáticamente a los ataques hasta que usted pueda intervenir.

2 Perspectivas de los MSP 2024 - Sophos

Cómo puede ayudar Sophos

Sophos tiene una amplia experiencia en la protección de pequeñas y medianas empresas frente a ciberamenazas avanzadas, y hemos creado muchos de nuestros productos y servicios para responder específicamente a sus necesidades.

Especialistas de seguridad de terceros

MDR

Sophos MDR es el servicio de MDR en el que más confía el mundo, ya que protege a más pymes que cualquier otro proveedor. Disponemos de información exhaustiva sobre ataques a pequeñas empresas y utilizamos la telemetría de toda nuestra base de clientes para reforzar la protección de todos los usuarios.

El servicio Sophos MDR está entre los mejor valorados tanto por los clientes como por los analistas. Entre los reconocimientos más recientes se encuentran:

- Distinción Gartner® Peer Insights™ Customers' Choice durante los dos últimos años, con una puntuación de 4,8 sobre 5 basada en 647 reseñas a 17 de septiembre de 2024.
- Líder de G2 para MDR, incluida la mejor solución MDR en el segmento de medianas empresas.
- Sophos es nombrado líder en la evaluación de proveedores IDC MarketScape 2024 para la detección y respuesta gestionadas (MDR) globales.

"Para las empresas que buscan un proveedor de MDR con una gran experiencia en seguridad y un servicio dirigido por expertos que pueda ayudarles desde el principio hasta la resolución de un incidente, Sophos es una opción de lo más atractiva".
- Richard Thurston, director de investigación de servicios de seguridad europeos, IDC

MSP

Sophos cuenta con un amplio ecosistema de rápido crecimiento de Partners MSP que ofrecen productos y servicios de Sophos, incluido Sophos MDR, a pymes de todo el mundo.

Soluciones diseñadas expresamente para las pymes

Plataforma

Sophos Central es la plataforma nativa en la nube y basada en IA más grande y escalable del sector. Se utiliza para gestionar todas las soluciones de ciberseguridad next-gen de Sophos, entre las que se incluyen Sophos Endpoint, Sophos Firewall, Sophos XDR, Sophos MDR, Sophos Email y Sophos ZTNA. Las integraciones con una amplia gama de tecnologías de terceros, como Microsoft y Google, garantizan que los clientes puedan sacar el máximo partido de sus inversiones en seguridad.

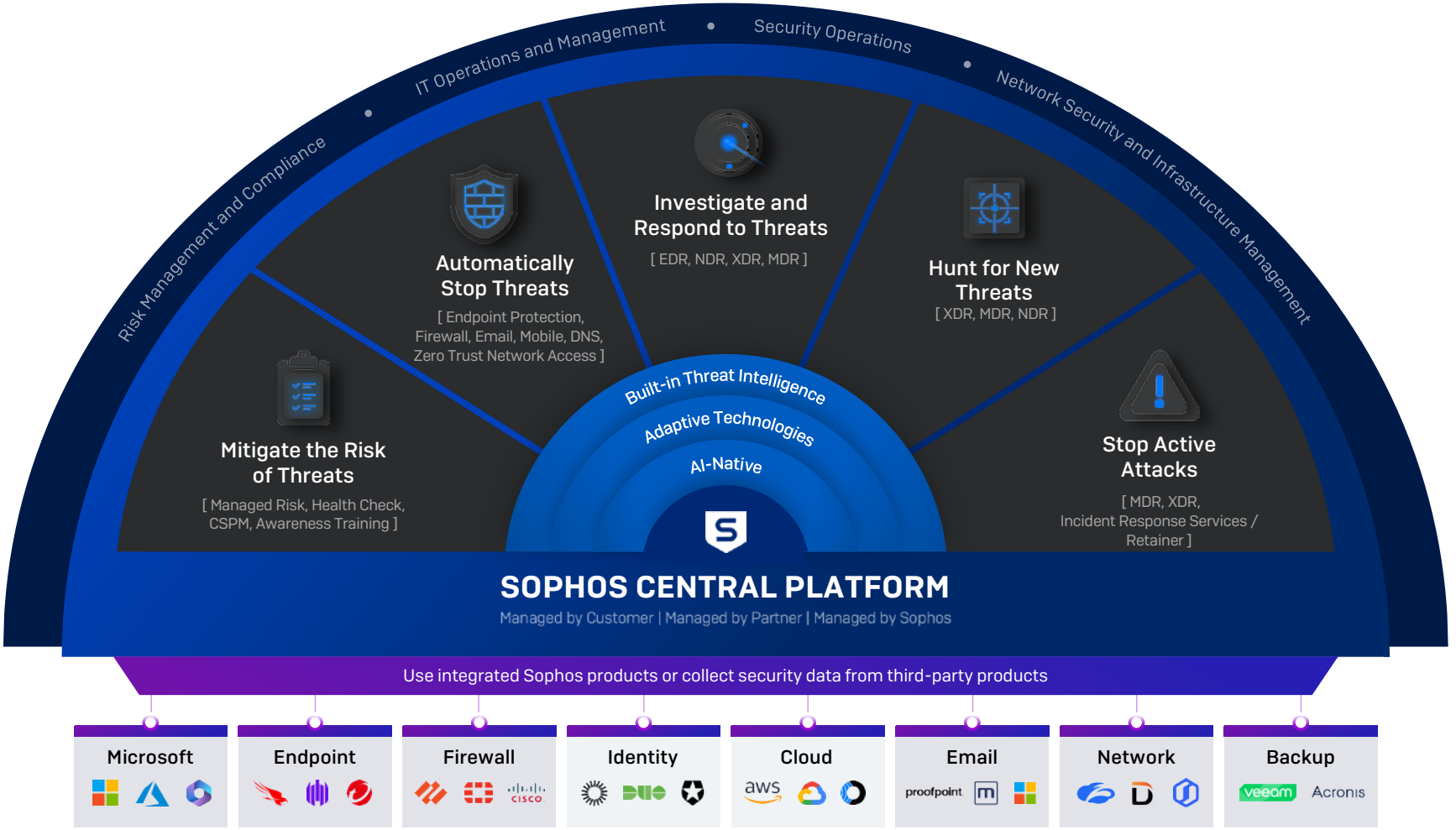
Funciones de los productos

Las soluciones de Sophos son altamente sofisticadas y cuentan con décadas de experiencia en la detención de ciberamenazas. También están diseñadas para ser fáciles de usar, de modo que organizaciones de todos los tamaños y niveles de recursos se beneficien de las funcionalidades de protección líderes en el mercado.

Ejemplos:

- **Sophos Endpoint** se despliega automáticamente con la configuración recomendada, incluida nuestra protección antiransomware y funciones antiexploits líderes en el sector, sin necesidad de realizar ajustes manuales.
- La administración centralizada y generación de informes de **Sophos Firewall** le permiten gestionar varios firewalls en un solo lugar, lo que resulta especialmente útil para organizaciones con ubicaciones dispersas.
- **Sophos Endpoint** incluye defensas adaptativas que detectan la presencia de adversarios en el entorno y responden automáticamente, lo que aumenta sus defensas y le da tiempo para responder.
- La función integrada Verificar estado de cuenta de **Sophos Endpoint** ofrece visibilidad en tiempo real de la postura de seguridad, y el botón Corregir automáticamente le permite volver a la configuración recomendada con un solo clic.
- La integración de **Sophos Firewall** con la plataforma más amplia de Sophos le permite bloquear automáticamente las amenazas activas y coordinar una respuesta en los endpoints; también se integra con ZTNA, switches y puntos de acceso inalámbricos para evitar el movimiento lateral.

La plataforma de ciberseguridad de Sophos



Conclusión

La encuesta pone de manifiesto que la escasez de competencias en ciberseguridad pesa mucho sobre las pymes. La consiguiente falta de conocimientos y habilidades tiene un impacto material en la capacidad de las empresas para defenderse de los ataques. Sin que se vislumbre el final de la falta de recursos, las organizaciones pequeñas harían bien en tomar medidas para mitigar sus efectos contratando a especialistas externos y eligiendo soluciones diseñadas específicamente para su negocio.

Para obtener más información sobre las soluciones de Sophos para pymes, hable con su representante o Partner de Sophos o visite es.sophos.com.

2024-10-08 ES-WP [PC]

SOPHOS