INFORME ESPECIAL DE CIBERSEGURIDAD

MERCADO DE EMPRESAS MEDIANAS Y PEQUEÑAS

Pequeño y poderoso

Cómo fortifica el mercado de empresas medianas y pequeñas sus defensas contra las amenazas actuales

CISCO

El 53% del mercado de empresas medianas ha experimentado una brecha

Hasta

5000

alertas de seguridad en promedio

El mercado de empresas medianas investiga el **55,6%** de las alertas de seguridad

El 29% del mercado de empresas medianas afirma que las brechas cuestan menos de USD 100 000. El 20% afirma que cuestan entre USD 1 000 000 y USD 2 499 999

El mercado de empresas medianas y pequeñas aspira a prácticas de ciberseguridad más eficaces, como las de las grandes empresas. Las pequeñas y medianas empresas son dinámicas; son la red troncal de la innovación y el ejemplo modelo del trabajo arduo. Funcionan mucho más rápido y trabajan mucho más duro que sus pares empresariales. Y están expuestas a las mismas amenazas cibernéticas.

En el actual panorama de amenazas cibernéticas, cada organización, grande o pequeña, corre el riesgo de un ataque. Pero progresivamente, el mercado de empresas medianas y pequeñas es el centro de los ataques[1] y, a menudo, sirve como plataforma de lanzamiento o conducto para iniciativas más grandes. Los atacantes ven al mercado de empresas medianas y pequeñas como un blanco fácil con prácticas e infraestructuras de seguridad menos sofisticadas y una cantidad inadecuada de personal capacitado para administrar y responder ante una amenaza.[1]

El mercado de empresas medianas y pequeñas recién está comenzando a darse cuenta de cuán atractivo es para los ciberdelincuentes. Muchas veces, se da cuenta demasiado tarde: después de un ataque. Recuperarse de un ataque cibernético puede ser difícil y costoso, aunque no imposible, para estas empresas, según la naturaleza y el alcance de la iniciativa. Este informe brindará una idea de los riesgos que enfrentan las organizaciones más pequeñas y compartirá conocimientos sobre cómo se posicionan respecto de sus pares en relación con la seguridad y pautas para tener en cuenta en el año 2018 y el futuro.

Considere los resultados del Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco: más de la mitad (54%) de todos los ataques cibernéticos causa daños financieros por más de USD 500 000, entre otros, pérdida de ingresos, clientes, oportunidades y gastos de bolsillo. Esa cantidad es suficiente para dejar fuera de servicio a una empresa mediana o pequeña de forma permanente.

Un estudio reciente de Better Business Bureau (BBB)[2] destaca cómo el mercado de empresas medianas y pequeñas puede luchar financieramente para sobrevivir después de un ataque cibernético grave. BBB preguntó a propietarios de pequeñas empresas en América del Norte: ¿Durante cuánto tiempo su empresa podría seguir siendo rentable si pierde permanentemente el acceso a los datos críticos? Solo alrededor de un tercio (35%) respondió que podría seguir siendo rentable durante más de tres meses. Más de la mitad informó que quedaría improductivo en menos de un mes.

Por cierto, consideramos como pequeñas y medianas empresas a las compañías con menos de 250 empleados y las definimos como empresas con entre 250 y 499 empleados. Ambos segmentos se incluyen en este informe.

Analizamos las respuestas de los encuestados de las pequeñas y medianas empresas en nuestro Estudio comparativo sobre capacidades de seguridad de 2018, que denominaremos simplemente estudio comparativo. Ofrece perspectivas sobre las prácticas de seguridad actualmente en uso y compara los resultados completos de los últimos tres años.

Nuestros datos del mercado de empresas medianas y pequeñas y medianas empresas incluyen a 1816 encuestados de 26 países.

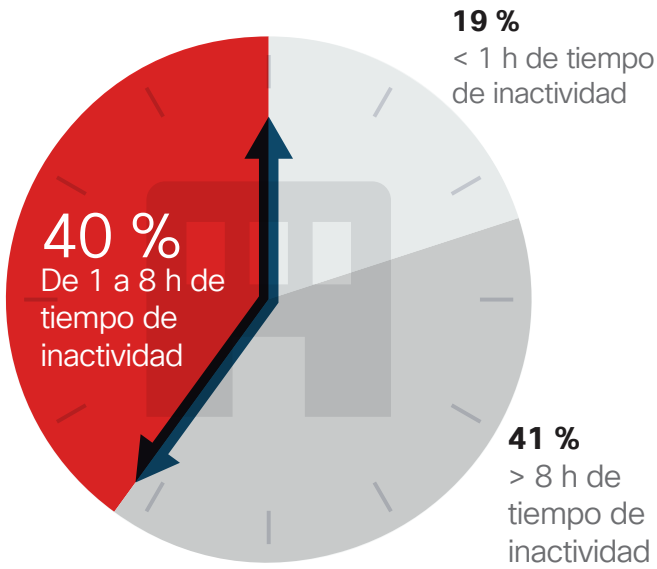
1 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Desarrollado en colaboración con Cisco y el Centro Nacional para el Mercado Intermedio. Disponible en: https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.
2 2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

¿Qué es un día de negocios perdido entre colegas?

Dijo nunca ningún administrador de TI. El tiempo de inactividad del sistema, que socava la productividad y la rentabilidad, es un problema importante para las empresas después de un ataque cibernético. La investigación del estudio comparativo arrojó que el 40% de los encuestados (250 a 499 empleados) experimentó ocho horas o más de tiempo de inactividad del sistema debido a una brecha de seguridad grave en el último año (Figura 1). Cisco vio resultados similares para las organizaciones más grandes en el ejemplo del estudio (aquellas con 500 empleados o más). La diferencia, sin embargo, es que las organizaciones más grandes tienden a ser más resistentes que las pequeñas y medianas empresas después de un ataque, dado que cuentan con más recursos para responder y recuperarse.

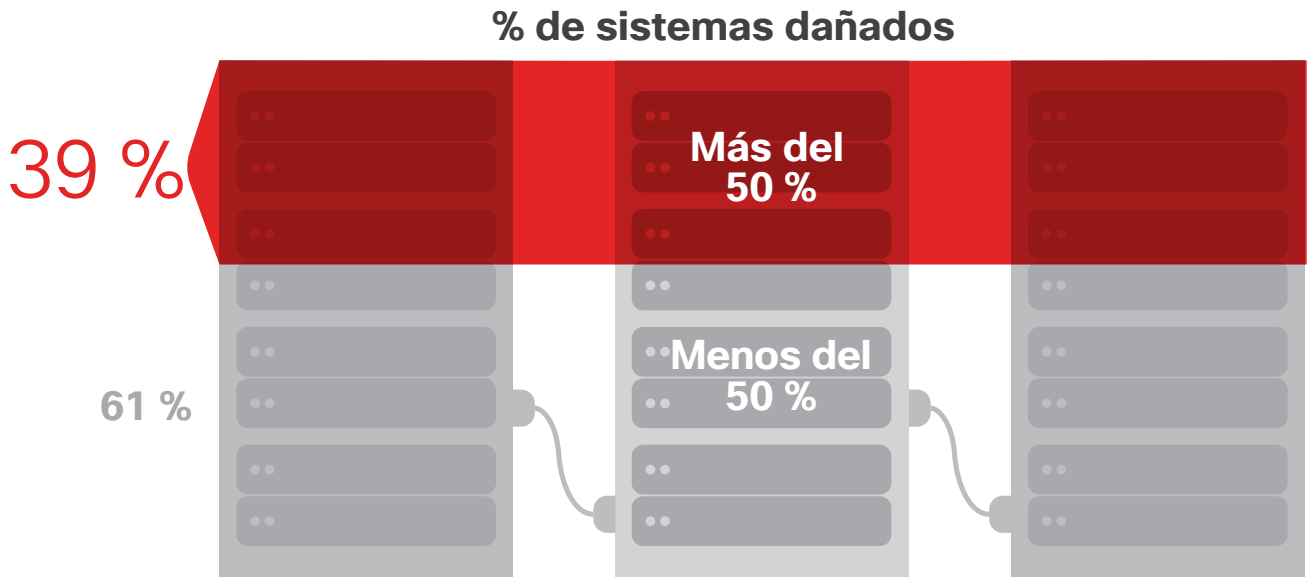
Además, el 39% de los encuestados informó que al menos la mitad de sus sistemas se vio afectada por una brecha severa (Figura 2). Las empresas más pequeñas son menos propensas a tener múltiples ubicaciones o segmentos de negocio y sus sistemas centrales generalmente están más interconectados. Cuando estas organizaciones experimentan un ataque, la amenaza puede propagarse con rapidez y facilidad de la red a otros sistemas.

Figura 1 Tiempo de inactividad del sistema tras una brecha grave



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Figura 2 Porcentaje de sistemas afectados por una brecha grave



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

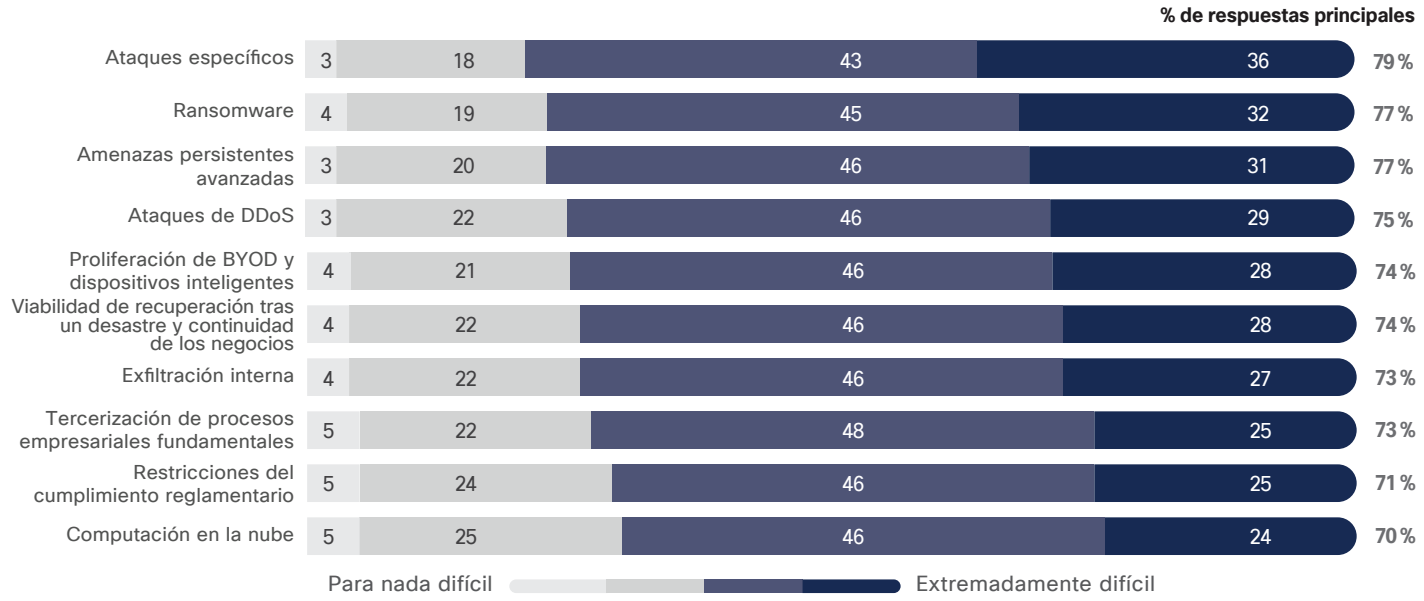
Noches de seguridad en blanco

Cuando se les preguntó sobre los mayores desafíos de seguridad enfrentados, los encuestados mostraron mayor preocupación por tres cosas:

- Los ataques dirigidos contra los empleados (suplantación de identidad bien elaborada)
- Las amenazas persistentes avanzadas (malware avanzado desconocido)
- El ransomware

El ransomware (curiosamente no citado como una de las tres preocupaciones principales de las grandes empresas), que es, como bien sabe, malware que cifra los datos generalmente hasta que los usuarios afectados pagan la exigencia de rescate, también puede generar interrupciones graves y tiempo de inactividad en el sistema para el mercado de empresas medianas y pequeñas. El ransomware además es costoso de diferente manera para estas organizaciones: los expertos en seguridad de Cisco explican que el mercado de empresas medianas y pequeñas está más dispuesto a pagar los rescates a los atacantes para reanudar rápidamente las operaciones normales. Simplemente no pueden permitirse el tiempo de inactividad y la falta de acceso a los datos críticos, incluidos los datos del cliente. (Consulte la Figura 3).

Figura 3 Principales inquietudes de seguridad para el mercado de empresas medianas[5]



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Otras amenazas que las pequeñas y medianas empresas no pueden ignorar

A pesar de las preocupaciones acerca del ransomware, los expertos en seguridad de Cisco sugieren que se trata de una amenaza menguante, dado que los atacantes cambian su enfoque hacia la extracción ilícita de criptomonedas ("criptoexplotación"). Esta actividad tiene un triple atractivo: puede ser muy lucrativa, pueden seguirse los pagos y los atacantes tienen menos preocupaciones respecto del potencial de responsabilidad delictiva de sus acciones. (Por ejemplo, no hay ningún riesgo de que los pacientes queden privados de la atención crítica debido al bloqueo de los sistemas y los datos esenciales del hospital por parte del ransomware). Los atacantes también pueden proporcionar software de explotación ("minadores") a través de diversos métodos, como las campañas de correo electrónico no deseado y los kits de explotación.[3]

3 Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions, blog de Cisco Talos, 31 de enero de 2018: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Los investigadores de amenazas de Cisco explican que los actores maliciosos que usan el nuevo modelo comercial de criptoexplotación ilícita "ya no penalizan a las víctimas por abrir un archivo adjunto o ejecutar una secuencia de comandos maliciosa que secuestra al sistema y exige un rescate. Ahora, aprovechan activamente los recursos de los sistemas infectados".[4] Para el mercado de empresas medianas y pequeñas que inadvertidamente ayuda en las operaciones ilícitas de criptoexplotación, un rendimiento más lento del sistema puede ser la única señal de alerta de peligro; a menos que se cuente con la tecnología adecuada para detectar la presencia de una actividad de criptoexplotación.

Un 0,5% de amenazas internas: ¿100% es demasiado?

A medida que las empresas de los encuestados mueven más datos y procesos a la nube, deben adoptar medidas para administrar otra posible amenaza: los infiltrados fraudulentos. Sin herramientas para detectar la actividad sospechosa (como la descarga de información confidencial del cliente), corren el riesgo de perder la propiedad intelectual, los datos financieros confidenciales y los datos de los clientes por los sistemas corporativos en la nube.

Una investigación reciente de los investigadores de amenazas de Cisco resalta este riesgo: de enero a junio de 2017 analizaron las tendencias de exfiltración de datos mediante el aprendizaje mecanizado para trazar el perfil de 150 000 usuarios en 34 países que utilizaban la nube. En 1,5 meses, los investigadores descubrieron que el 0,5% de los usuarios realizó descargas sospechosas. ¿El 50% parece mucho? En otras palabras, esto significa que dos empleados en una firma de 400 personas son amenazas infiltradas. Un 100% muy alto. Específicamente, estos usuarios descargaron, en total, más de 3,9 millones de documentos de sistemas corporativos en la nube. Un promedio de 5200 documentos por usuario durante un período de 1,5 meses.[5]

Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Este informe especial destaca las conclusiones de datos seleccionados del Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco. La investigación involucró a más de 3600 encuestados de 26 países. Para obtener más información sobre las prácticas de seguridad actualmente en uso de las organizaciones de todos los tamaños y una comparación de los resultados de los estudios anteriores de Cisco, descargue el *Informe anual de ciberseguridad de Cisco de 2018* disponible en: https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Ibid.
5 Para obtener más detalles, consulte "Amenazas infiltradas: aprovechamiento de la nube" en el Informe anual sobre ciberseguridad de Cisco de 2018 disponible en: https://www.cisco.com/c/en/us/products/security/security-reports.html.

Desafíos

La mejor defensa contra las amenazas descritas anteriormente requiere la coordinación y orquestación de los recursos de TI. Esos recursos más comúnmente son las personas, los procesos y la tecnología que las empresas acumulan para disuadir los ataques.

Sin embargo, las pequeñas empresas, incluso más que sus homólogas de mayor tamaño, tienen el desafío de coordinar estos recursos de manera que produzcan conocimientos de las amenazas y detengan o mitiguen los ataques antes de que provoquen daños. La falta perpetua de talentos de seguridad que afecta a las empresas impacta aún más en las contrapartes más pequeñas.

Tendencias de tecnologías de seguridad para las pequeñas y medianas empresas

Ahora las organizaciones más pequeñas efectivamente buscan abordar los desafíos de ciberseguridad que amenazan a sus organizaciones con nuevas herramientas para detenerlas.

Los encuestados del estudio comparativo afirman que, si contaran con recursos de personal disponibles, podrían:

- Actualizar la seguridad de los terminales con una protección contra malware avanzada/EDR más sofisticada (la respuesta más común con un 19%).
- Considerar una mejor seguridad de aplicaciones web contra ataques web (18%).
- Implementar la prevención de intrusiones, aún vista como tecnología vital para detener los ataques a la red y los intentos de explotación (17%). (Consulte la Figura 5).

A medida que las organizaciones consideran las nuevas tecnologías, el desafío está en determinar qué tan bien sus productos interoperarán para mantener protegida a la empresa. No deben subestimarse las cargas de gestión de análisis de varias consolas para responder a las amenazas o los incidentes de seguridad.

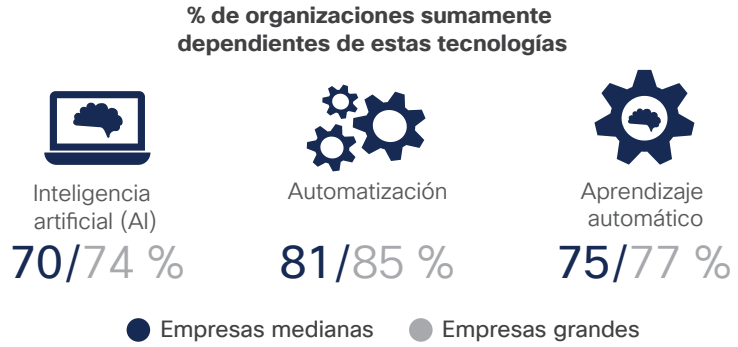
“Muchas personas piensan que si siguen el mejor enfoque del multiproveedor, estarán mejor protegidas”, dice Ben M. Johnson, CEO de Liberty Technology, un partner de Cisco, en Griffin, Georgia. “Pero lo que podemos ver es que es más difícil de administrar, cuesta más y disminuye la eficacia general de la seguridad”.

Aprendizaje mecanizado: ¿ayuda para la seguridad o moda?

Todos hemos escuchado acerca del aprendizaje mecanizado debido a su reciente publicidad. Resulta que el mercado de empresas medianas depende de casi la misma cantidad de soluciones de análisis de comportamiento que las empresas más grandes para detectar con eficacia los ataques. Y confía en menor medida en las soluciones que usan el aprendizaje mecanizado y la automatización en comparación con las organizaciones que tienen más de 1000 empleados (Figura 4).

El aprendizaje mecanizado es más eficaz cuando es una capa de detección adicional en un producto ya implementado en contraste con la adquisición de un producto independiente de “aprendizaje mecanizado”. De esta forma, los equipos obtienen el beneficio del aprendizaje mecanizado para detectar anomalías y amenazas a la velocidad de la máquina sin cargar el equipo.

Figura 4 El mercado de empresas medianas depende menos de la automatización y las herramientas de inteligencia artificial



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Mercado de empresas medianas móviles

Las empresas también reconocen que sus enfoques de seguridad deben cumplir con las demandas del entorno laboral moderno, particularmente el cambio hacia la movilidad y la adopción de los dispositivos móviles. El 56% de los encuestados dijo que proteger los dispositivos móviles de los ataques cibernéticos es muy difícil o sumamente complejo.

El mercado de empresas medianas y la nube

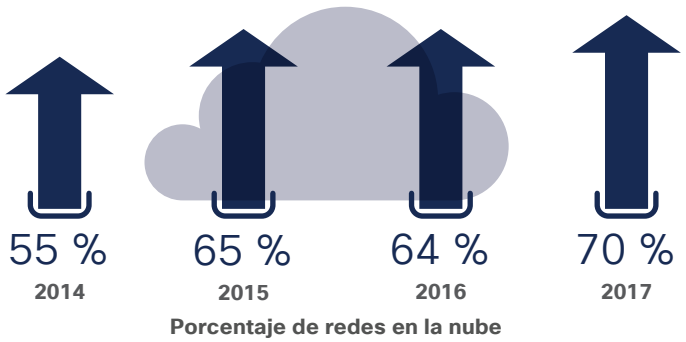
En reconocimiento de los desafíos de seguridad, muchos de los encuestados recurren a la nube para reforzar las defensas sin añadir personal ni salirse de los recursos existentes. La pregunta es si mover la seguridad a la nube es una estrategia suficiente para frenar los ataques. Además, las empresas no pueden simplemente delegar la responsabilidad de la seguridad migrando los datos a la nube; deben conocer los controles de seguridad impuestos por los proveedores de la nube y cómo las posibles brechas en la nube pueden afectar los recursos en las instalaciones.

La adopción de los servicios en la nube en el mercado de empresas medianas está claramente en alza, según la investigación de Cisco. En 2014, el 55% de estas empresas dijo que alojaron algunas de sus redes a través de una forma de la nube; en 2017, dicho número aumentó al 70% (Figura 5).

Muchos de los encuestados creen que la nube puede ayudar a cerrar esas brechas en las defensas y resolver algunas deficiencias en la infraestructura y las capacidades del personal. De hecho, según la investigación de Cisco, la razón principal del mercado de empresas medianas para alojar redes en la nube es la creencia de que ofrecen una mejor seguridad de los datos (68%); el segundo motivo más popular es que las empresas carecen de la cantidad suficiente de trabajadores internos de TI (49%). (Consulte la Figura 6).

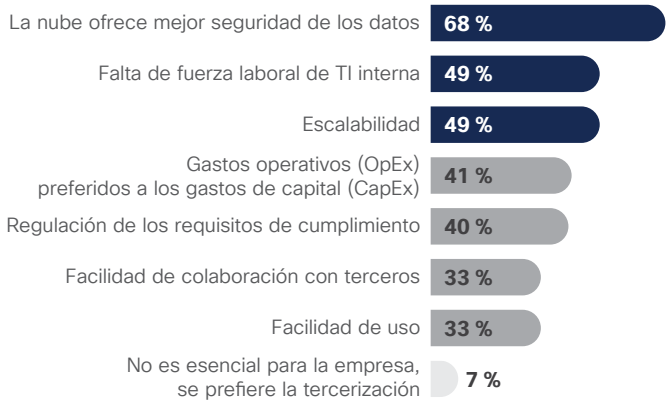
El mercado de empresas medianas también prefiere la nube por su escalabilidad (es decir, reduce la dependencia de la empresa de los recursos internos) y por el cambio flexible a los gastos operativos en lugar de los gastos de capital (Figura 6).

Figura 5 El mercado de empresas medianas muestra un aumento constante en la adopción de la nube



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Figura 6 El mercado de empresas medianas opta por la nube para la seguridad y la eficiencia



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Personas: búsqueda de personal para fortalecer la seguridad

La buena noticia es que el estudio comparativo muestra que el 92% del mercado de empresas medianas cuenta con un directivo responsable de la seguridad. (Consulte la Figura 7).

Respecto de los amplios recursos de personal, el mercado de empresas medianas está dispuesto a agregar más herramientas de seguridad, como firewalls de aplicación web o protecciones avanzadas de terminales.

Lo que el mercado de empresas medianas tiene en común con las empresas grandes es la escasez de personal de TI, que obstaculiza la capacidad para reforzar las defensas. Simplemente no hay personal interno suficiente para administrar las herramientas que podrían mejorar la seguridad, según la investigación de Cisco.

Por este motivo, muchas empresas medianas y pequeñas recurren a la subcontratación de colaboradores para reunir el talento necesario a fin de incrementar su conocimiento sobre las amenazas, ahorrar dinero y responder a las brechas más rápidamente. El deseo de conocimientos objetivos fue el motivo más frecuente del mercado de empresas medianas para la subcontratación de tareas de seguridad (Figura 8), seguido de la rentabilidad y la necesidad de responder rápidamente a los incidentes de seguridad.

La subcontratación de colaboradores es una buena manera para que las empresas aprovechen al máximo los recursos limitados. Pero estas compañías pueden verse en problemas si suponen que un proveedor subcontratado o un partner de la nube proporcionará todas las capacidades de las que carecen internamente.

Chad Paalman, CEO de NuWave Technology Partners en Kalamazoo, Michigan, un partner de Cisco, señala que muchas empresas medianas y pequeñas desconocen exactamente cuánto análisis y supervisión ofrecen los proveedores de servicios de seguridad tercerizados.

Figura 7 Directivos responsables de la seguridad en el mercado de empresas medianas

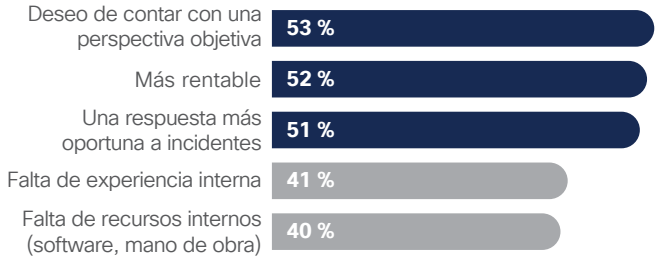
92 % tiene un directivo responsable de la seguridad

Cargo del ejecutivo responsable de la seguridad

42 %	Director general de seguridad de la información (CISO)
24 %	Director general de seguridad (CSO)
10 %	Director general (CEO)
8 %	Director general de información (CIO)
3 %	Director de operaciones (COO)
5 %	Director general de tecnología (CTO)
6 %	Vicepresidente sénior o vicepresidente de TI (SVP o VP)
2 %	Director de riesgos o director de cumplimiento (CRO o CCO)

Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Figura 8 El mercado de empresas medianas utiliza la subcontratación de colaboradores para superar la falta de recursos internos



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

“Muchos líderes empresariales no conocen sus redes. Suponen que si tienen un firewall, es como tener un candado en la puerta para que nadie ingrese. También asumen que si tercerizan la seguridad con un proveedor de servicios administrados (MSP), se supervisan los registros o el servicio incluye la detección de intrusiones”.

Chad Paalman, CEO de NuWave Technology Partners

Sin embargo, la conclusión es que las empresas medianas y pequeñas cuentan con los partners subcontratados para proporcionar:

- Servicios de asesoría y consultoría subcontratados (57%)
- Respuesta ante los incidentes (54%)
- Monitoreo de seguridad (51%)

No obstante, son menos propensas a subcontratar tareas tales como inteligencia de amenazas (39%). (Consulte la Figura 9).

La buena noticia es que el mercado de empresas medianas parece estar dejando de lado algunos de sus recursos limitados de comprensión y respuesta ante las amenazas a fin de reforzar la inteligencia de amenazas y la respuesta ante los incidentes.

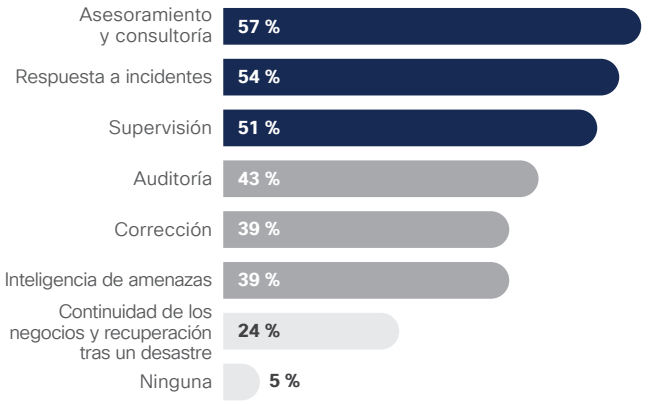
Procesos: verificaciones periódicas para administrar la seguridad

Los procesos de seguridad integrales y periódicos, como los controles de activos de gran valor y las revisiones de prácticas de seguridad, ayudan a las organizaciones a identificar sus debilidades en las defensas. Dichos procesos no son tan predominantes como debieran en el mercado de empresas medianas, quizás debido a la falta de personal.

Por ejemplo, según el Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco, el mercado de empresas medianas es menos propenso que las organizaciones más grandes a revisar las prácticas de seguridad periódicamente, contar con herramientas implementadas para revisar las capacidades de seguridad e investigar rutinariamente los incidentes de seguridad (Figura 10).

Un aspecto positivo es que el 91% del mercado de empresas medianas dijo que realizó simulacros para probar los planes de respuesta ante los incidentes al menos anualmente. Sin embargo, al igual que la dependencia de la nube y los partners subcontratados, la pregunta es si dichos planes de respuesta ante los incidentes son adecuados para rechazar a los atacantes cada vez más sofisticados.

Figura 9 El mercado de empresas medianas subcontrata servicios de consultoría y asesoramiento además de respuesta ante los incidentes



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Figura 10 El mercado de empresas medianas es menos propenso a estar totalmente de acuerdo con el uso de procesos operativos

Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

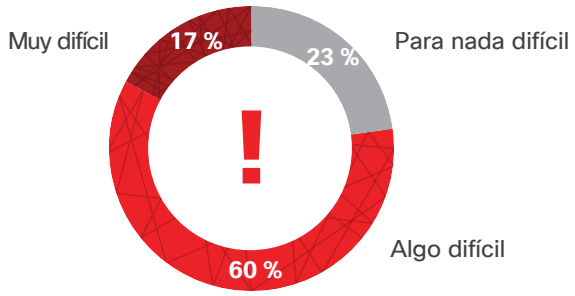
Conexión entre personas, procesos y tecnologías: el desafío de la organización

Si el mercado de empresas medianas y pequeñas agrega más proveedores y productos de seguridad a sus defensas, y cambia los recursos de TI para administrar estos productos, ¿sus organizaciones administrarán mejor la seguridad? Lo opuesto puede ser verdad; al menos en términos de comprensión y coordinación de las alertas de seguridad.

La mayoría de las empresas pequeñas y medianas hoy en día reconoce que, a medida que generan un entorno de proveedores y productos más complejo, aumentan sus responsabilidades. Por ejemplo, al 77% del mercado de empresas medianas le resulta difícil o muy complejo coordinar las alertas de las diferentes soluciones (Figura 11).

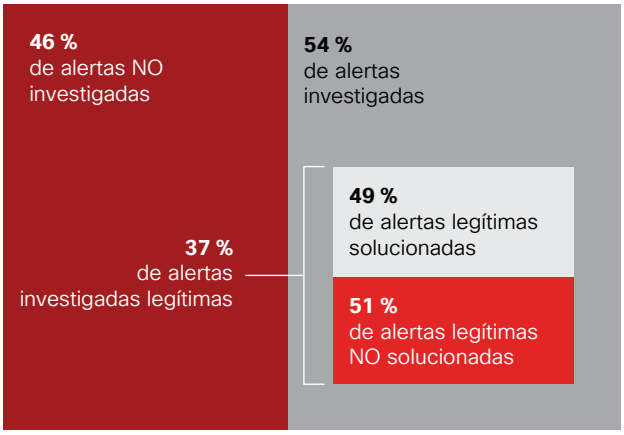
Cuando las empresas intentan analizar estas alertas, los desafíos combinados de personas, procesos y tecnologías pueden generar muchas alertas que quedan sin investigar, como muestra el estudio comparativo (Figura 12):

Figura 11 El mercado de empresas medianas es menos propenso a estar totalmente de acuerdo con el uso de procesos operativos



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Figura 12 Porcentajes de alertas de seguridad sin investigar o solucionar



Fuente: Estudio comparativo sobre capacidades de seguridad de 2018 de Cisco

Recomendaciones para el futuro

Tecnología

A medida que las organizaciones consideran herramientas nuevas, lo ideal sería que eviten agregarlas a la flota de proveedores y generar más alertas.

Teniendo esto en cuenta, ¿se diseñan los productos con una mente abierta? ¿Cómo se integran con otros en términos de uso compartido de datos e inteligencia de amenazas? ¿Existe la integración de la consola de administración?

Si un proveedor afirma que los productos se diseñaron para adaptarse al trabajo conjunto, ¿esto sucede directamente o el comprador debe realizar un gran trabajo de API?

El aprendizaje mecanizado, si bien se ha puesto de moda, tiene su lugar en la seguridad. Sin embargo, use el aprendizaje mecanizado como una capa de detección dentro de los productos implementados en lugar de los productos autónomos de otros proveedores que añaden un nuevo producto para administrar.

Personas y procesos

En llanas palabras, desarrolle una estrategia para mejorar la ciberseguridad. Solo el 38% de las empresas medianas y pequeñas tiene una estrategia de riesgos cibernéticos activa vigente conforme a Vistage Research Center, un centro de recursos para líderes empresariales.[6]

¿Su estrategia incluye usuarios finales que reciben capacitación adecuada? ¿Sus políticas de seguridad cubren la pérdida de negocios ante un ataque cibernético? ¿Qué le parece generar una continuidad de negocios y planes de comunicación en situaciones críticas para habilitar la recuperación más rápida y ayudar a prevenir daños reputacionales?

Los líderes de TI además deben explicar en términos claros qué deben saber los gerentes empresariales respecto de las brechas:

- ¿Cuál es el impacto en la organización?
- ¿Qué medidas adopta el equipo de seguridad para contener e investigar las amenazas? ¿Cuánto tiempo demorará reanudar las operaciones normales?[7]

“Al adoptar un conjunto de herramientas y plataformas de seguridad que trabajan en conjunto, a diferencia de piezas dispares que pueden entrar en conflicto entre sí, amplía la eficacia de la seguridad y simplifica su administración”.

Ben M. Johnson, CEO de Liberty Technology

“El mercado de empresas medianas y pequeñas debe evaluar estos riesgos y desarrollar planes de respuesta antes de una brecha, no después”.

Chad Paalman, NuWave Technology Partners

6 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Desarrollado en colaboración con Cisco y el Centro Nacional para el Mercado Intermedio. Disponible en: https://www. vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Informe semestral de ciberseguridad de Cisco de 2017: https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ibid.

Conclusión

Una recomendación final para el mercado de empresas medianas y pequeñas a fin de impulsar mejoras en la ciberseguridad es reconocer que el cambio gradual es mejor que ningún cambio. En resumen, no se debe dejar que el deseo de ser "perfecto" en el enfoque de seguridad se interponga en el camino para ser "mejor". La perfección, como en todas las cosas, no existe.

El mercado de empresas medianas y pequeñas además debe comprender que no existe ninguna solución de tecnología "milagrosa" para resolver todos los desafíos de ciberseguridad. El panorama de amenazas es demasiado complejo y dinámico. La superficie de ataque siempre se amplía y cambia. Y, como respuesta, las estrategias y tecnologías de seguridad deben evolucionar constantemente.

Para obtener más información sobre el enfoque centrado en las amenazas de Cisco, visite www.cisco.com/go/security.

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Ámsterdam,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

Publicado en julio de 2018