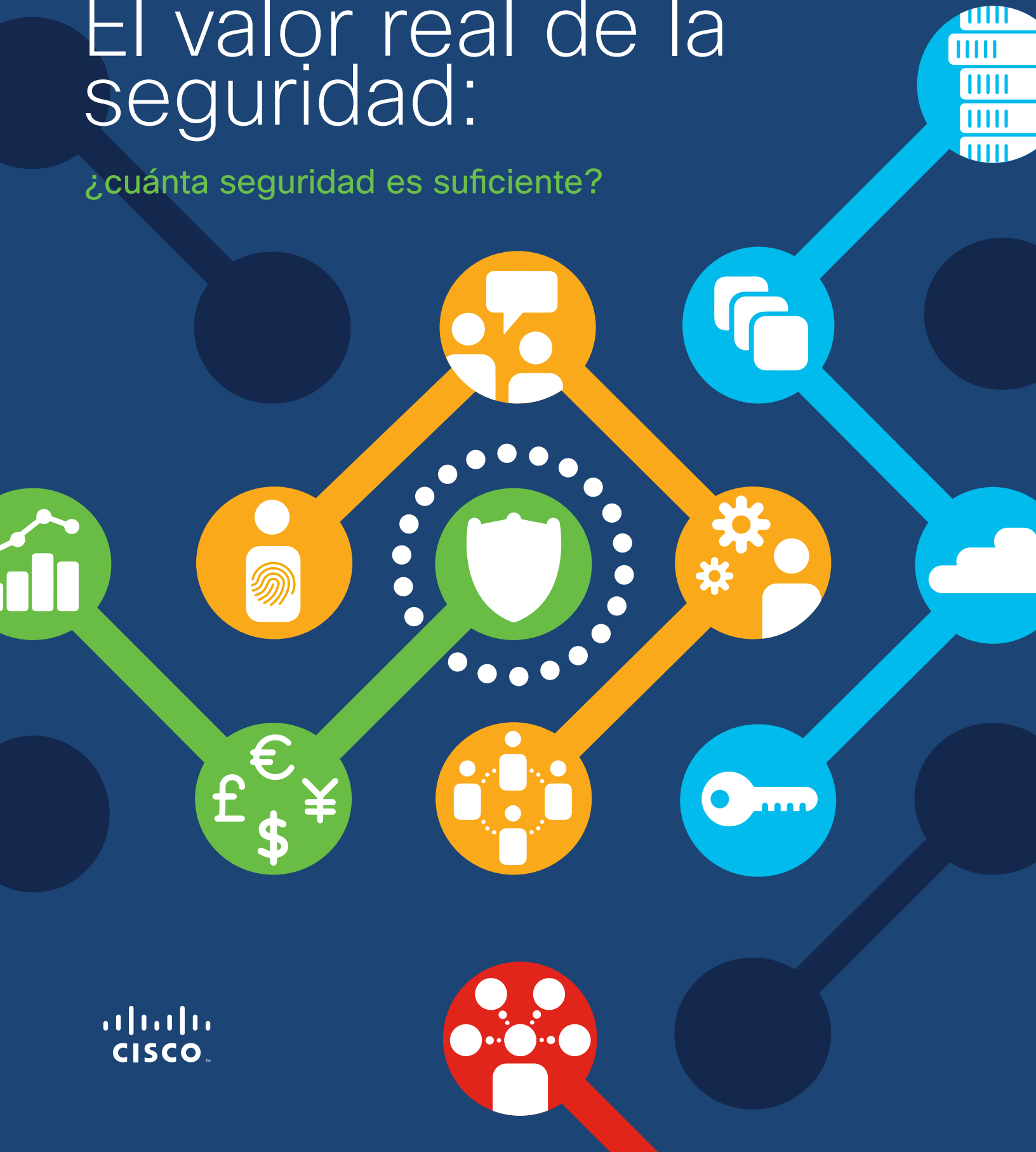
El valor real de la seguridad:

¿cuánta seguridad es suficiente?



CISCO

Contenido

Introducción: El valor real de la seguridad

Cuando las organizaciones tienen docenas de productos de seguridad instalados, pero aún son vulnerables, se plantean las siguientes preguntas: *¿cuánta seguridad es suficiente?* ¿Cuántos productos necesita una organización? ¿Cuáles? ¿Cuánto se debe invertir en seguridad? En otras palabras, *¿cuál es el valor real de la seguridad?*

Las organizaciones pueden invertir en seguridad infinitamente a fin de mantener a los atacantes a raya. Pero, ¿cuánto ***deben*** gastar y qué ***deben*** hacer para estar protegidas?

Va más allá del dinero. Quizás una organización tiene un presupuesto sustancial para la seguridad, pero no ha contratado a los expertos adecuados para ejecutar su visión. O tal vez una organización tiene un presupuesto de seguridad reducido, pero ha invertido sabiamente en tecnología y personal adecuados para sus recursos más vulnerables o críticos. A veces, gran parte de la seguridad de una organización se administra mediante un tercero que no tiene la fuerza para influir en las actualizaciones o los cambios necesarios.

Sí, el presupuesto es importante cuando se trata de seguridad. Pero no lo es todo. ¿Dónde se encuentra su organización cuando se trata de la seguridad? ¿Cuenta con el personal, los procesos y la tecnología adecuados para defender proactivamente su entorno? ¿Está por encima o por debajo del valor real de la seguridad?

En este informe, esbozaremos los factores clave para el éxito de la seguridad según lo determinan nuestros expertos del sector y un grupo de aproximadamente 80 participantes en una encuesta anónima reciente de profesionales de seguridad realizada por Cisco. Por supuesto, sería injusto no proporcionar al menos un poco de orientación respecto de cómo llevar su seguridad al siguiente nivel.

"Hay muchas dinámicas en los desafíos de seguridad más allá del dinero".

Wendy Nather, jefa de asesoría de los CISO, Cisco

Los números no mienten

Fue llamativo descubrir en nuestra encuesta reciente que el 56 % de los encuestados (más de la mitad) experimentó un importante evento de seguridad (infracción, intrusión, infección de malware, etc.) en el último año. El 94 % de los encuestados afirmó saber que aún tiene que implementar una seguridad eficaz. Y el 43 % admite que, a veces, tiene que tomar atajos para lidiar con problemas de seguridad, como eliminar completamente un terminal infectado en lugar de eliminar quirúrgicamente el malware. (Consulte la Figura 1).

Figura 1 ¿Cómo están abordando las organizaciones actuales el tema de la seguridad?
Porcentaje de encuestados: N = 79

Fuente: Encuesta sobre el valor real de la seguridad de CISCO

Pero no todas son malas noticias. El 95 % de los encuestados dijo que puede identificar eficazmente qué datos y sistemas de su organización requieren los niveles más altos de protección. ¡Un buen comienzo! Entonces, ¿por qué siguen luchando? ¿Se trata de dinero? ¿O hay otros factores en juego?

Wendy Nather, jefa de asesoría de los CISO de Cisco, presenta los siguientes cuatro factores que pueden afectar el éxito de la seguridad:

- Presupuesto
- Experiencia
- Capacidad
- Influencia

Hace varios años, Nather acuñó el famoso término "línea de pobreza de la seguridad" para iniciar este debate. También fue la autora de dos informes sobre el tema mientras se desempeñaba como directora de investigación en **451 Research**: "Vivir por debajo de la línea de pobreza de la seguridad" en 2011 y "Costo real de la seguridad" en 2013.

"Basándome en mi experiencia anterior como CISO en los sectores público y privado, sé que hay muchas organizaciones que tienen problemas de seguridad", afirma Nather. "Hay muchas dinámicas en los desafíos de seguridad más allá del dinero, por ejemplo, una organización que gasta millones aún puede ser deficiente en materia de seguridad, mientras que una organización con un presupuesto más pequeño puede tener las defensas suficientes en función de sus necesidades específicas".

Factores para determinar el éxito de la seguridad

Aparte del dinero, hay otros factores que pueden afectar el valor de la seguridad. Junto con el presupuesto, están la experiencia, la capacidad y la influencia.

Presupuesto

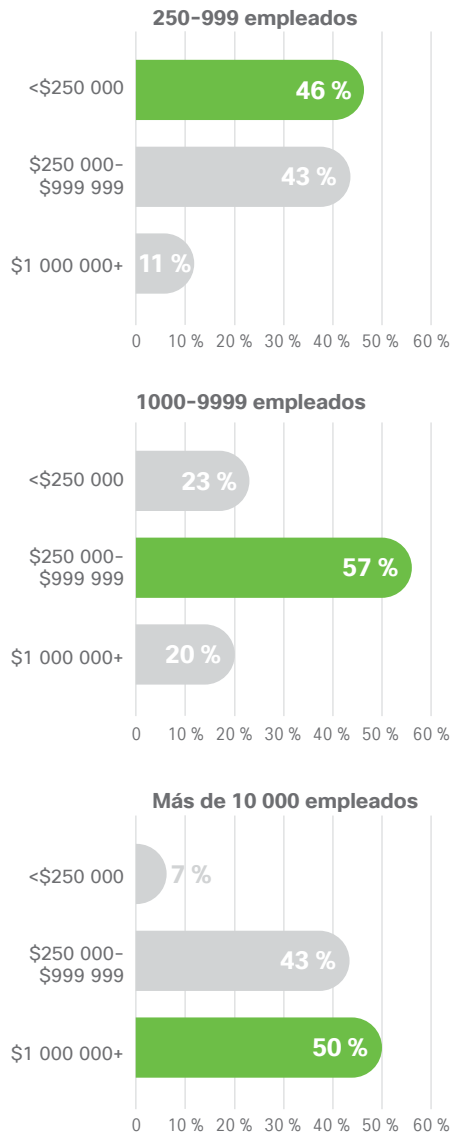
¿Cuánto invierten las organizaciones en seguridad?

No hay un número mágico cuando se trata de invertir en seguridad. La cantidad que una organización debe invertir en seguridad depende de varios factores, entre ellos: tamaño, industria, tolerancia al riesgo, postura, etc. Sin embargo, hemos dividido el gasto anual en seguridad de nuestros encuestados (según el tamaño de su organización) como punto de referencia aproximado para otras organizaciones. Como se ilustra en la figura 2:

- Entre las **organizaciones de mercado intermedio (250 a 999 empleados)**, el 46 % gasta menos de USD 250 000 anuales en seguridad y el 43 % gasta de USD 250 000 a USD 999 999 anualmente. (Solo el 11 % gasta USD 1 millón o más anualmente).
- La mayoría (57 %) de las **organizaciones empresariales (1000 a 9999 empleados)** gasta entre USD 250 000 y USD 999 999 anuales en seguridad. (Solo el 20 % gasta USD 1 millón o más anualmente, mientras que el 23 % gasta menos de USD 250 000 anualmente).
- El 50 % de las **grandes empresas (con más de 10 000 empleados)** gasta USD 1 millón o más anualmente en seguridad, el 43 % gasta entre USD 250 000 y USD 999 999 y solo el 7 % gasta menos de USD 250 000.

Si bien estos números proporcionan cierta información básica sobre proporción del tamaño de la organización con respecto a la inversión en seguridad, es importante tener en cuenta que el tamaño de una organización no lo es todo cuando se trata de invertir en seguridad. La cantidad de empleados por sí sola no se correlaciona necesariamente con la cantidad de ingresos o fondos disponibles ni incluso con la cantidad de riesgos que afronta la organización. Por ejemplo, un fondo de cobertura puede administrar miles de millones de dólares con un pequeño equipo y una gran agencia del gobierno estatal con muchos empleados puede tener un presupuesto pequeño y fluctuante.

Figura 2 ¿Cuánto gasta su organización anualmente en seguridad?



Fuente: Encuesta sobre el valor real de la seguridad de CISCO

Otro criterio popular para medir el gasto en seguridad es tomar un porcentaje del presupuesto de TI. Sin embargo, los porcentajes no ayudan cuando los números involucrados son muy grandes o muy pequeños. Si un banco puede permitirse gastar el 10 % del presupuesto de TI de mil millones de dólares en seguridad, puede adquirir mucho más que una empresa en crecimiento que obtiene el 10 % de un presupuesto de TI de USD 50 000 para gastar en seguridad. Cuando las empresas establecen niveles de gasto para la seguridad, mejoran el precio de las capacidades de seguridad específicas que necesitan en lugar de simplemente elegir un porcentaje del presupuesto de TI al azar.

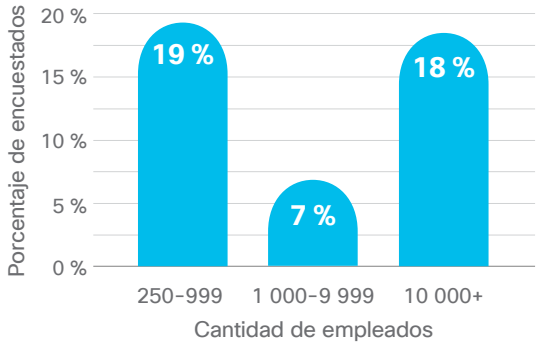
¿Las organizaciones pueden costearse la seguridad que necesitan?

Un asombroso 84 % de los encuestados dijo que pudo pagar una parte, pero no la cantidad *mínima* total de seguridad que necesitaba para proteger su infraestructura. Curiosamente, descubrimos que eran organizaciones con 1000 a 9999 empleados las que parecían estar teniendo más problemas para afrontar lo necesario; solo el 7 % de estas organizaciones dijo que era capaz de pagar la seguridad mínima total que necesitaba. (Consulte la Figura 3).

En comparación, el 19 % de las organizaciones más pequeñas (250 a 999 empleados) y el 18 % de las organizaciones más grandes (más de 10 000 empleados) dijo que podía pagar la seguridad *mínima* total que necesitaba. Al parecer, a medida que las organizaciones crecen, los presupuestos de seguridad no siempre crecen proporcionalmente (hasta que se alcanza una gran cantidad de empleados).

"La pregunta más interesante es por qué no son las organizaciones más pequeñas las que a menudo se consideran incapaces de pagar la seguridad mínima que necesitan", afirma Nather. "¿Es porque sienten que son inferiores al objetivo y, por lo tanto, no necesitan tanta seguridad? ¿Crece el riesgo de seguridad percibido en relación con otros factores de crecimiento en una organización? ¿O una empresa entra en el radar de los atacantes después de que logra un determinado perfil, solo para enfrentarse a un imperativo de seguridad que no ha cumplido?"

Figura 3 Mi organización es capaz de pagar toda la seguridad mínima que necesita.
Porcentaje de encuestados que están de acuerdo



Fuente: Encuesta sobre el valor real de la seguridad de CISCO

¿Un presupuesto más grande aumenta la confianza y la capacidad de la seguridad?

El 27 % de las organizaciones que gastan USD 1 millón o más anuales en seguridad afirmó que pudo pagar la seguridad mínima total que necesitaba en comparación con tan solo el 9 % de las organizaciones que gastan entre USD 250 000 y USD 999 999. Por lo tanto, parece lógico que sí; el aumento del gasto marca una diferencia en la capacidad de la seguridad.

Sin embargo, en cuanto a todos los presupuestos de seguridad, las organizaciones aún sienten que deben seguir avanzando en la implementación de una seguridad eficaz. El 94 % de los que gastan USD 1 millón o más anuales afirmó que aún debe seguir avanzando; el 95 % de los que gastan entre USD 250 000 y USD 999 999 y el 92 % de los que gastan menos de USD 250 000 indicaron lo mismo.

Entre las organizaciones con 1000 a 9999 empleados, solo el 23 % afirmó que confía más en el personal interno cuando se trata de conocimientos en seguridad. Esto, una vez más, habla sobre el hallazgo de que las organizaciones de este tamaño en particular tienen más inconvenientes a la hora de afrontar las capacidades de seguridad que necesitan.

Así que, si bien el presupuesto definitivamente ayuda, no lo es todo en lo que respecta a la seguridad. ¿Qué otros factores entran en juego?

Experiencia

¿Las organizaciones tienen las destrezas y el personal apropiados para proteger eficazmente sus entornos?

Cuando se preguntó en quién confían *más* respecto de la experiencia en seguridad, solo el 37 % dijo que en el personal interno. Casi la misma cantidad de encuestados (28 %) afirmó que depende más de las redes profesionales. Esto habla de la escasez de destrezas generalizadas en ciberseguridad. Según una investigación de (ISC)², hoy en día tenemos una escasez de casi 3 millones de profesionales en ciberseguridad en todo el mundo.

Aunque es bueno que las organizaciones sientan que pueden recurrir a recursos externos para obtener experiencia en materia de seguridad, también hay conocimientos comerciales críticos que deben tener en su personal de seguridad interno. Esto incluye el conocimiento en torno a la experiencia del usuario y el diseño de procesos, el análisis de riesgos y la respuesta ante incidentes.

"Hay muchas llamadas de riesgo de seguridad que deben tenerse en cuenta y una gran cantidad de trabajo de respuesta ante incidentes que solo se puede llevar a cabo si se tiene el conocimiento institucional de la organización", afirma Nather. "Por lo tanto, incluso cuando se cuenta con personal de respuesta ante incidentes externo, aún se debe contar con profesionales internos que sepan lo que está sucediendo dentro de la red".

También descubrimos que el 34 % de los encuestados está aprendiendo sobre las vulnerabilidades de seguridad y los incidentes que afectan a su organización desde los medios de comunicación. Esto destaca la necesidad continua de periodistas confiables y blogueros expertos para llenar la brecha de conciencia situacional de la ciberseguridad para muchas empresas.

Capacidad

¿Qué factores adicionales impiden que las organizaciones logren una seguridad sólida?

Incluso si una organización tiene la experiencia necesaria para saber qué debe hacer en su programa de seguridad, eso no significa necesariamente que tenga la capacidad de ejecutarlo. Por ejemplo, la sabiduría convencional sostiene que la segmentación de la red es un control crítico de seguridad cibernética, pero una red heredada compleja administrada por múltiples proveedores puede ser demasiado difícil y costosa de separar con los recursos disponibles.

Además, los equipos de seguridad no siempre pueden dictar sus requisitos a grupos u organizaciones externos. Por ejemplo, cuando un fabricante debe cumplir con docenas de normas y regulaciones operacionales específicas de cada país, puede llevar años aprobar y distribuir una actualización de software para sus sistemas de control.

La capacidad es un factor importante en la estrategia de seguridad. A veces también conocida como "madurez de la seguridad", la capacidad se basa en la funcionalidad básica que las organizaciones necesitan antes de que puedan avanzar con proyectos más sofisticados. Esto incluye (consulte la figura 4):

Figura 4 Pirámide de madurez de la seguridad

1. **Saber qué se tiene y qué hace.** Mantener un inventario de activos actualizado no es tan fácil como suena en el entorno dinámico actual. Muchos ecosistemas de aplicaciones son tan complejos que nadie puede saber qué datos se comparten, con qué fines y a través de qué interfaces. Las auditorías de usuarios generalmente descubren cuentas que son críticas, pero que no están documentadas.
2. **Poder iniciar (y prevenir) cambios en los recursos.** Si no controla un recurso, debe poder hacer que el propietario lo cambie de manera oportuna para solucionar una vulnerabilidad. Asimismo, debe asegurarse de que los cambios solo se produzcan cuando se aprueban y de que también se tengan en cuenta las dependencias de la tecnología.
3. **Comprender los riesgos de seguridad.** ¿Cuáles son sus recursos más importantes y cuánto valen para los delincuentes? Debe saber qué tipos de amenazas son más propensas a dirigirse a sus recursos, cómo reconocerlas y cómo bloquearlas. De lo contrario, puede gastar tiempo y dinero en recursos que no importan, al tiempo que ignora los que sí lo hacen.
4. **Poder instalar y operar la tecnología de seguridad.** Una vez que haya dominado las tres primeras capacidades, podrá hacer un uso eficaz de los productos y servicios.

¿Qué tecnologías se utilizan más comúnmente en los programas de seguridad?

Estas son las 15 principales tecnologías de seguridad que utilizan nuestros encuestados:

1. **Firewalls/administración de políticas de seguridad**
2. **Seguridad del correo electrónico**
3. **Protección contra malware de la red**
4. **Detección/protección de amenazas y cargas de la nube**
5. **Prevención de pérdida de datos**
6. **Cifrado**
7. **VPN**
8. **Gateway web y de Internet seguro**
9. **Administración de eventos e información de seguridad (SIEM)**
10. **Control de acceso a la red**
11. **Agente de seguridad de acceso a la nube**
12. **Seguridad de terminales/EDR**
13. **Firewall de aplicación web**
14. **Detección de amenazas de red/análisis de tráfico de red**
15. **Plataformas de inteligencia de amenazas**

"Cuantos más productos tenga, más trabajo tendrá para conectar toda esa información. Cuando piense en la seguridad, adopte un enfoque holístico, no solo una estrategia de pilares... Con la automatización incorporada, puede comenzar a tomar medidas sin tener que hacer que su equipo crezca significativamente".

Marisa Canciller, directora sénior, Seguridad informática, Cisco

En sí mismas, las 15 tecnologías principales indicadas anteriormente conforman un portafolio sustancial, que requiere una gran cantidad de personas con experiencia sólida para configurar, mantener y monitorear todo. La implicación es que el costo del personal de seguridad es mucho mayor de lo que muchas organizaciones consideran cuando intentan planificar lo que necesitan.

"En mi rol anterior como analista industrial, encuestaba a profesionales de seguridad sobre qué tecnologías pensaban que los CISO necesitaban adquirir para proteger adecuadamente sus organizaciones", afirma Nather. "Las respuestas que recibí fueron generalizadas, lo que indica que no hay un plan estándar. Algunos mencionaron tan solo cuatro tecnologías, mientras que otros destacaron más de 31 herramientas diferentes".

"Muchos de los encuestados en este sondeo simplemente dijeron que lo que una organización necesita depende de varios factores, entre ellos, qué tipo de datos se tienen, en qué sector se encuentran, si están dispersos geográficamente", continúa Nather. "Si no podemos crear una respuesta única para todos los CISO, y lo más cercano que tenemos es un estándar de cumplimiento para un caso de riesgo bien comprendido y de amplio alcance, como PCI-DSS, no podemos esperar que cada organización sepa con confianza lo que realmente necesita. Y si no sabe lo que necesita, tampoco sabrá si puede incluso costearse la seguridad".

Si bien hay algunas tecnologías que la mayoría de las organizaciones elige tener, como firewalls y seguridad de terminales, el resto depende realmente de la situación específica de cada organización. Y puede requerir una investigación sustancial y una auditoría de ciberseguridad antes de que una organización pueda determinar qué es exactamente lo que necesita o puede permitirse.

Kelley Misata, PhD, es la fundadora y CEO de Sightline Security. Sightline es una nueva empresa de ciberseguridad y 501(c)(3) organización sin fines de lucro que se asocia con otras organizaciones de este tipo para evaluar, priorizar y mejorar la seguridad.

Ciberseguridad para organizaciones sin fines de lucro

¿Por qué se necesita una organización como Sightline hoy en día?

Misata: Por varias razones, pero estas son las tres principales. Primero, las organizaciones sin fines de lucro aún no saben lo que necesitan. Están navegando por la ciberseguridad sin un mapa. Con todas las complejidades de la seguridad actual, eso es realmente difícil; especialmente cuando tienen tiempo, personal y dinero limitados. Y, con buenos motivos, cuando uno da el 200 % de si mismo en su misión de ayudar a los demás.

Segundo, las soluciones de seguridad comerciales no están diseñadas teniendo en cuenta organizaciones sin fines de lucro. Sí, las organizaciones sin fines de lucro tienen funciones comerciales similares, pero también tienen matices que las diferencian en la forma en que administran la seguridad.

En tercer lugar, las organizaciones sin fines de lucro no están bien versadas en el lenguaje de la seguridad, y, francamente, a veces, los profesionales de seguridad pueden hacer que sea difícil para las personas que no son del entorno de seguridad comprender de qué hablamos. Las organizaciones sin fines de lucro asisten a conferencias de seguridad y descubren que no comprenden muy bien lo que se dice o no logran alinear las soluciones que se ofrecen con sus empresas. La misión de Sightline es ser puente, traductor y defensor de estas organizaciones. Estamos desarrollando herramientas de evaluación y una comunidad de seguridad únicamente para organizaciones sin fines de lucro.

Influencia

¿Pueden las organizaciones influir eficazmente en los proveedores, los partners y demás terceros para proporcionar la seguridad que necesitan?

La seguridad de la cadena de abastecimiento de terceros es una preocupación importante para los CISO hoy en día. Con los servicios, el hardware y el software que provienen de docenas o cientos de fuentes diferentes, las organizaciones no tienen ninguna oportunidad cuando se trata de ejercer el control total de la seguridad.

Y no es de extrañar que cuantos más empleados y organizaciones de presupuesto tengan, más probabilidades tendrán de influir en los proveedores y los partners para ayudarlos con la seguridad. Por ejemplo, el 86 % de las organizaciones con más de 10 000 empleados está aprendiendo sobre las vulnerabilidades de seguridad y los incidentes que afectan a su organización provenientes de los proveedores/partners afectados antes de que sea público, en comparación con tan solo el 60 % de las organizaciones con menos de 1000 empleados.

Y el 38 % de las organizaciones que gasta USD 1 millón o más anuales en seguridad afirmó que siempre pudo agregar términos y condiciones relacionados con la seguridad a un contrato de un proveedor/partner, en comparación con tan solo el 17 % de las organizaciones que gastan menos de USD 250 000 anuales en seguridad. Esto indica que las organizaciones más grandes con más potencia de gasto están mejor posicionadas para negociar con terceros.

¿Dónde deja esto a las organizaciones más pequeñas, que pueden ser aún más dependientes de los partners externos? "Su mejor opción puede ser la de agruparse con pares para ejercer mayor influencia sobre los proveedores y distribuidores compartidos", afirma Nather. "Por ejemplo, las asociaciones industriales, los foros regionales de ciberseguridad o los centros de intercambio y análisis de información (ISAC) permiten que los miembros organicen solicitudes y respuestas a los problemas de seguridad. Encontrar o crear esta influencia es parte del trabajo del CISO en la actualidad, lo que hace que las redes sean aún más importantes".

(Ciberseguridad para organizaciones sin fines de lucro, cont.)

¿Cuáles son algunos de los desafíos de seguridad específicos que enfrentan las organizaciones sin fines de lucro?

Misata: En primer lugar, las empresas sin fines de lucro tienen muy poco personal, lo que significa que no tienen tiempo ni dinero para desperdiciar en nada que no respalde directamente su misión. Para muchas organizaciones sin fines de lucro, la ciberseguridad se considera costosa, abrumadora y no es necesaria hasta que ocurre algo malo.

En segundo lugar, muchas organizaciones sin fines de lucro no han identificado cuáles de sus recursos podrían ser atractivos para los atacantes. Entonces, ¿cómo pueden saber qué proteger? Muchas organizaciones sin fines de lucro de la actualidad son llevadas a gastar dinero en soluciones antes de comprender lo que necesitan.

En tercer lugar, uno de los mayores desafíos para las organizaciones sin fines de lucro es que ninguna persona en la organización está centrada directamente en la seguridad. A pesar de que están muy entusiasmados y saben que la seguridad (en particular la ciberseguridad) es importante, su atención se dispersa en muchas direcciones.

La buena noticia es que, a pesar de ello, las organizaciones sin fines de lucro se están intensificando y ya no se ven a sí mismas como inmunes a un ataque; reconocen que tienen recursos y datos de valor. Pero a menudo tienen una influencia mínima sobre los proveedores y distribuidores de servicios: están muy relegadas. A través de nuestro trabajo con los miembros de Sightline, ahora podemos recopilar datos y conocimientos sobre el estado de la seguridad en las organizaciones sin fines de lucro, de modo que podamos comenzar a incorporarlas.

Conclusiones principales

En general, las organizaciones no creen que puedan pagar la seguridad que necesitan, independientemente del tamaño que tienen o la cantidad que gastan actualmente.

Es a las organizaciones intermedias, con 1000 a 9999 empleados, a las que más les cuesta proteger adecuadamente sus entornos.

No hay una respuesta única cuando se trata de los productos de seguridad que una organización debe utilizar o de cuánto debe gastar en seguridad. Depende en gran medida del tamaño y el tipo de organización, la criticidad de sus recursos y lo que realmente puede permitir. Esto hace que a las empresas les sea más difícil averiguar qué deben incluir sus programas de seguridad.

El aumento del gasto no siempre se traduce en una mayor capacidad de seguridad y confianza. Se deben tener en cuenta otros factores, como la experiencia y la influencia.

Las organizaciones deben asegurarse de que su personal interno siga desarrollando experiencia en seguridad general y en entornos específicos y perfiles de riesgo. Hay algunos aspectos de la seguridad que solo el personal interno está equipado para manejar.

La capacidad juega un papel importante en la utilidad de la seguridad. Factores tales como si un equipo de seguridad tiene el control sobre ciertos recursos pueden afectar enormemente la capacidad de ejecutar una estrategia de defensa, incluso con el presupuesto y la experiencia requeridos a su disposición.

Cuanto más grande es la organización, más fácil es que influyan en terceros que afecten su postura de seguridad. Las organizaciones más pequeñas pueden necesitar aprovechar el poder de las asociaciones para obtener la misma influencia y economías de escala.

Recomendaciones para elevar la seguridad

Independientemente de dónde se encuentra su organización en relación con de la seguridad, a continuación le presentamos algunas recomendaciones para resolver los principales desafíos que se plantean en este informe.

1. Descubra qué es lo correcto para su organización

Las organizaciones deben analizar de cerca dónde se encuentran sus gastos de seguridad. En este sector, hay mucha presión para mantenerse al ritmo de los pares. *"¿Qué compran todos los demás? ¿Necesito esa nueva tecnología?"* Por supuesto, siempre es bueno estar atento al sector y evaluar lo que hacen otros para aumentar sus defensas. Sin embargo, como hemos confirmado en este informe, la seguridad nunca es un modelo único para todos.

Antes de ir a comprar más tecnología, observe su experiencia en relación con la pirámide de madurez de la seguridad en nuestra sección Capacidad. Como dice el viejo refrán: "No se puede proteger lo que se desconoce". Y un analizador de vulnerabilidades no lo ayudará si no puede solucionar lo que encuentra.

Saber qué amenazas no solo son posibles, sino *probables*, le permitirá centrarse en las prioridades correctas cuando no pueda cubrirlo todo. Considere realizar una **evaluación de riesgo cibernético**, ya sea internamente o a través de terceros, para comenzar por el camino correcto.

2. Obtenga más de sus inversiones

Una tendencia desafortunada a lo largo de los años ha sido buscar siempre los mejores y más recientes productos de seguridad. Esto es bueno, en teoría, para asegurarse de estar protegido contra amenazas en constante evolución. Sin embargo, para muchas organizaciones, ha generado un complejo desorden de productos puntuales desarticulados que son difíciles, si no imposibles, de administrar. Si recibe demasiadas alertas de tecnologías dispares y debe pasar todo el día yendo y viniendo entre diferentes aplicaciones para averiguar qué sucede en su entorno, su seguridad sufrirá.

En cambio, es hora de invertir en tecnologías de seguridad que funcionen para usted, en lugar de hacerlo de la otra manera. Cisco adopta un **enfoque de plataforma para la seguridad**, lo que significa que no solo vendemos firewalls o seguridad del correo electrónico o tecnología anti-malware. También proporcionamos un portafolio abierto y amplio de tecnologías de seguridad que trabajan en conjunto para defender su red. Si encuentra una amenaza en un área, le damos la capacidad de bloquearla automáticamente en cualquier otro lugar. La automatización y la integración pueden recorrer un largo camino para minimizar la complejidad y garantizar el máximo provecho de sus tecnologías de seguridad y personal.

"Considero la seguridad como un ecosistema. Cuantas más cosas funcionen en conjunto, mejor. Si tengo que dedicar tiempo y energía a la integración de tecnologías por mi cuenta, es menos tiempo que puedo dedicar realmente a la seguridad."

Steve Martino, SVP/CISO, Cisco

Cuando se trate de sus proveedores, asegúrese de aprovechar todo lo que ofrecen; que puede ser mucho a poco o ningún costo. Asista a los webinars gratuitos. Comuníquese con el soporte técnico. Asista a los eventos del proveedor. Únase a los grupos de asesores de clientes. Participe en capacitaciones de proveedores. Por supuesto, si ha invertido en tecnología, el personal de seguridad debe saber cómo usarla de manera eficaz.

3. Adopte un enfoque de Zero Trust para la seguridad

Las amenazas actuales llegan a su organización desde todos los ángulos. Se dirigen a los usuarios, las aplicaciones, la red, la nube, los dispositivos de IoT y la lista continúa. Esta superficie de ataque expandida hace que sea fundamental que las organizaciones adopten un **enfoque de Zero Trust** para la seguridad.

Zero Trust requiere que las organizaciones:

- Obtengan visibilidad de todas las áreas de la red
- Adopten controles para garantizar que solo las personas, los dispositivos y las aplicaciones adecuados puedan operar en el entorno de la organización.
- Cuenten con un método eficaz para bloquear comportamientos sospechosos para evitar la propagación de ataques

Con estos pasos, las organizaciones pueden proteger más eficazmente su fuerza laboral, su carga y su lugar de trabajo.

Al traspasar las medidas de seguridad básicas y adoptar un enfoque holístico y más estratificado de la seguridad, se puede lograr que para los atacantes sea más difícil y costoso comprometer los recursos, lo que ciertamente ayuda a la utilidad de la seguridad.

4. Aumente su capacitación

Dado que muchos de nuestros encuestados confían en fuentes externas para la experiencia en seguridad, deberían contar con más capacitaciones en regla. Asegúrese de continuar invirtiendo en la comprensión de su entorno y sus destrezas una vez que contrate sus talentos.

Permita que asistan a conferencias y talleres. Realice sesiones de capacitación interna. Pídales que accedan a recursos gratuitos, como **Cisco Security Blog** y la **página de inteligencia de amenazas de Cisco Talos**, para mantenerse actualizado sobre las amenazas más recientes. Permita que persigan más certificaciones. En resumen, asegúrese de que no solo hagan su trabajo, sino que también se conviertan en verdaderos expertos en el proceso, no solo expertos en seguridad, sino también expertos en su negocio. Un tercero nunca comprenderá sus necesidades y restricciones de seguridad particulares tan bien como su propia gente.

5. Considere la subcontratación

Si ejecuta una serie de sistemas antiguos, lo más probable es que su equipo de TI dedique mucho tiempo a administrarlos y actualizarlos, pero obtenga una seguridad ineficaz a cambio. La migración de sistemas heredados complejos a aplicaciones de SaaS subcontratadas para funciones comerciales bien conocidas y no esenciales, como correo electrónico, aplicaciones de oficina, nóminas y otras, puede ayudar enormemente a la seguridad en dichas áreas a fin de que pueda concentrarse en proteger sus principales recursos y procesos.

Para los productos de seguridad que requieren un personal más dedicado que el que tiene disponible (debido al costo), la subcontratación de la administración de dichas tecnologías a través de un proveedor de respuestas ante incidentes (MSSP) también es una opción. Tenga en cuenta que, a veces, es mejor y más rentable obtener ayuda con la seguridad que intentar hacer todo por su cuenta.

6. Una fuerzas

Como se indica en nuestra sección Influencia, ciertamente los números tienen poder cuando se trata de la seguridad. Si su organización es demasiado pequeña para hacer valer la influencia sobre los proveedores, considere la posibilidad de agruparse con otras organizaciones a través de redes profesionales o grupos industriales para generar más influencia. Ser capaces de obtener correcciones de errores y actualizaciones oportunas de los proveedores y partners es fundamental para una seguridad eficaz. Es más difícil para ellos decir que no a 50 empresas pequeñas en comparación con una sola.

Visite cisco.com/go/security para descubrir cómo podemos ayudarlo a proteger SU entorno.

Metodología

Nuestros datos para este informe se basan en una encuesta doble ciego en línea entre aproximadamente 80 responsables de la toma de decisiones de TI en los Estados Unidos, quienes respondieron preguntas sobre planificación y presupuesto de seguridad. Los encuestados son empleados a tiempo completo en el mercado intermedio (de 250 a 999 empleados), empresas (de 1000 a 9999 empleados) y organizaciones de grandes empresas (+10 000 empleados) que trabajan para una organización con fines de lucro, el gobierno o una institución de educación superior con un departamento de TI formal. Están bien informados sobre los procedimientos y las políticas de seguridad, implicados en la configuración de estrategias de seguridad e invierten al menos el 40 % de su tiempo en la seguridad.

Acerca de la serie de ciberseguridad de Cisco

Durante la última década, Cisco ha publicado una gran cantidad de información crucial de seguridad e inteligencia de amenazas para profesionales de seguridad interesados en el estado de la ciberseguridad global. Estos informes exhaustivos proporcionaron explicaciones detalladas de los panoramas de amenazas y las consecuencias para las organizaciones, así como los procedimientos recomendados para defenderse frente a los efectos adversos de vulneraciones de datos.

En nuestro nuevo enfoque de liderazgo intelectual, el departamento de seguridad de Cisco está realizando una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner: Serie de ciberseguridad de Cisco. Hemos ampliado el número de títulos para incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas innovadores en el sector de seguridad, la recopilación previa de informes de la serie 2019 incluye el Reporte de referencia de privacidad de datos, el Reporte de amenazas, el Reporte de referencia de CISO, y el Reporte de seguridad del correo electrónico, el Reporte de Caza de Amenazas, y otros reportes que vendrán a lo largo del año.

Para más información y para acceder a todos los informes y las copias archivadas, visite www.cisco.com/mx/securityreports.

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 y los números de teléfono y fax están disponibles en el sitio web de Cisco en **www.cisco.com/go/offices**.

Publicado en octubre de 2019 BTTM_01_1019