SOPHOS

Guía de Sophos sobre ciberseguros

Cómo unos cibercontroles robustos pueden mejorar la asegurabilidad y reducir las primas

El mercado de los ciberseguros continúa cambiando y las condiciones siguen siendo difíciles, ya que en los últimos años ha aumentado el número de reclamaciones y su coste. Aunque la mayoría de las organizaciones ya cuentan con algún ciberseguro, muchas se encuentran con que el nivel de ciberseguridad necesario para optar a la cobertura es más alto, las pólizas son más complejas y las primas siguen subiendo.

Conseguir un ciberseguro que nos cubra es posible, pero los proveedores son sumamente selectivos en cuanto a quién aseguran y suelen evitar a los solicitantes de mayor riesgo. Al invertir en unas defensas sólidas, las organizaciones pueden reducir su ciberriesgo, lo que a su vez mejora su posición frente a las aseguradoras. Contar con unas ciberdefensas robustas tiene numerosas ventajas; entre otras, facilita el acceso a la cobertura, reduce las primas y permite conseguir unos límites más altos.

En esta guía se ofrece una presentación del estado del mercado de los ciberseguros y se explican las distintas formas en que la ciberseguridad puede afectar positivamente a su ciberpóliza. También se detallan las tecnologías y los servicios de Sophos que pueden ayudarle a reducir su ciberriesgo y optimizar su posición en el mercado asegurador.

Monográficos de Sophos. Diciembre de 2023

Aspectos básicos

Por qué tener un ciberseguro

Un ciberseguro, también conocido como seguro contra ciberriesgos o de ciberresponsabilidad, le protege frente al impacto de la ciberdelincuencia, pero no del delito en sí. En términos generales, contar con un ciberseguro ofrece cuatro ventajas principales:

1. **Económica.** El seguro cubre los costes derivados de un incidente de ciberseguridad.
2. **Comercial.** Cada vez más, tener un ciberseguro es un requisito previo para hacer negocios con muchas organizaciones.
3. **Operativa.** El equipo asegurador ofrece acceso inmediato a expertos en el caso de producirse un incidente, entre ellos, especialistas forenses de TI, abogados dedicados a la privacidad y profesionales de RR. PP.
4. **Tranquilidad.** Contar con un ciberseguro da confianza a sus clientes, partners, proveedores y empleados de que está preparado y cubierto ante un posible ataque cibernético.

Causas de las reclamaciones de ciberseguros

Aunque existe una amplia gama de incidentes que pueden desencadenar reclamaciones a los ciberseguros, según el informe Cyber Claims Study de NetDiligence de 2023, las causas más frecuentes son:

1. Ransomware
2. Estafas por correo electrónico corporativo comprometido
3. Hackers
4. Robo de dinero
5. Errores cometidos por el personal[1]

1 Informe Cyber Claims Study de NetDiligence de 2023

Qué cubre un ciberseguro

Un ciberseguro cubre los costes en los que se incurre como consecuencia de un ciberataque. Aunque las pólizas individuales varían, suelen cubrir:

- Costes de interrupción de la actividad
- Análisis forenses para identificar el origen del ataque
- Demandas de rescate y especialistas para gestionar las negociaciones de los rescates
- Costes de recuperar el acceso o restaurar sus datos a partir de copias de seguridad u otras fuentes
- Costes legales
- Servicios de relaciones públicas
- Notificación a los clientes y/o entidades reguladoras
- Servicios de control de crédito para individuos afectados

Al buscar seguros y comparar costes, hay que tener en cuenta que los costes de la interrupción del negocio, como la pérdida de ingresos o los gastos adicionales del trabajo consecuencia del ciberataque, están incluidos en algunas pólizas pero no en otras.

En el caso de que se produzca un ciberincidente, la compañía aseguradora intervendrá y pondrá a su disposición a expertos para ayudarle con la situación. En un ataque de ransomware, normalmente:

- Designará a un consultor para que le asesore sobre cómo gestionar y negociar una demanda de rescate
- Identificará la forma más económica de restaurar los datos (pago del rescate, copias de seguridad, etc.)
- Recurrirá a los expertos necesarios para tratar el problema

Cobertura de primera parte o de terceros

Muchas pólizas incluyen cobertura tanto de primera parte como de terceros. La cobertura de primera parte incluye los costes directos asociados a la respuesta al ataque, como gastos legales, forenses, de notificaciones a clientes, de relaciones públicas y otros. La cobertura de terceros incluye principalmente los costes asociados a demandas judiciales.

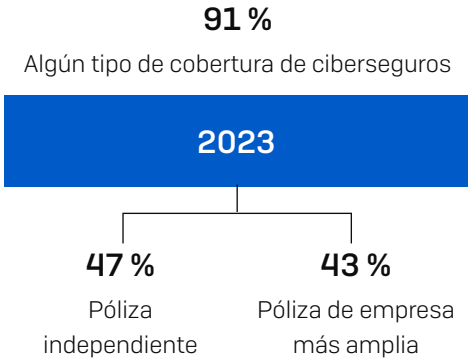
Dentro de una póliza, puede haber sublímites concretos para la cobertura de primera parte, e incluso para elementos específicos de la cobertura de primera parte. Por ejemplo, es posible que la cobertura de primera parte esté limitada a 500 000 USD, con un límite de 50 000 USD para costes de RR. PP.

Las realidades de los ciberseguros

El predominio de los ciberseguros

Tener un ciberseguro es sin duda la norma: el 91 %[2] de las organizaciones tenían algún tipo de ciberseguro en 2023, según una encuesta independiente encargada por Sophos, lo que supone un notable incremento con respecto al 84 % registrado en 2020[3] y se acerca al 92 % de las organizaciones que afirmaron que tenían cobertura en 2022. De las organizaciones que afirmaron que tenían cobertura en 2023, algunas tenían ciberpólizas independientes (47 %), mientras que otras optaron por cierta cobertura en materia de ciberseguridad que se incluía en un seguro empresarial más amplio (43 %).

Sin embargo, estas cifras no lo explican todo. Las pólizas varían y no todas ellas cubren el ransomware, la primera causa de las reclamaciones de los ciberseguros. Casi una de cada diez organizaciones que tenían cobertura en materia de ciberseguridad en 2022 no estaban aseguradas contra el ransomware, lo que las dejaba totalmente expuestas a los altos costes y grandes desafíos que conlleva recuperarse de estos tipos de ataque.



2 La vital importancia de las ciberdefensas de primera línea para la contratación de seguros, Sophos.
3 El estado del ransomware 2021, Sophos

Contratación de ciberseguros por sector

En el plano industrial, la encuesta reveló que el sector de la educación (tanto primaria y secundaria como superior) registró el nivel general más alto de cibercobertura (96 %), aunque estas organizaciones tienden a contratar esta cobertura como parte de una póliza de ciberseguridad más amplia en lugar de adquirir una póliza independiente.

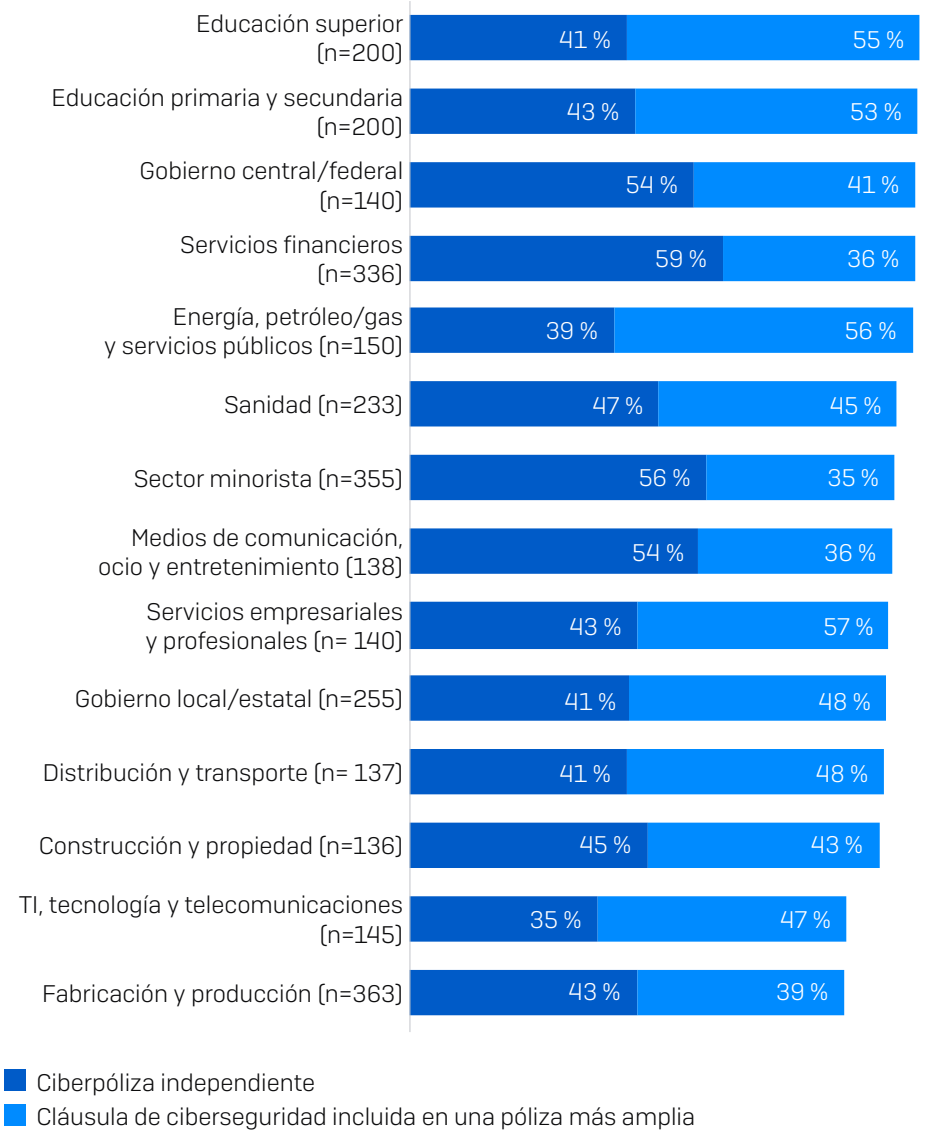
Este alto nivel de cobertura es comprensible dado que este sector notificó el índice más alto de ataques de ransomware en nuestro estudio El estado del ransomware 2023, en que el 80 % de las instituciones de educación superior y el 79 % de las de educación primaria y secundaria afirmaron que se habían visto afectadas por el ransomware en el año anterior. El sector de servicios financieros fue el más propenso a contratar una ciberpóliza independiente (59 %), seguido de cerca por el sector minorista (56 %).

Contratación de ciberseguros por ingresos

No es de extrañar que la contratación de ciberseguros aumente con los ingresos. El 96 % de las organizaciones con una facturación anual de más de 5000 millones USD cuentan con algún tipo de cibercobertura, frente al 79 % de aquellas que informan de unos ingresos de menos de 50 millones USD.

Las organizaciones con más ingresos también son más propensas a contratar una ciberpóliza independiente que aquellas con unos ingresos inferiores: el 58 % de las organizaciones que declaran unos ingresos anuales de más de 5000 millones USD tienen una póliza independiente, frente al 34 % de aquellas con unos ingresos anuales de menos de 10 millones USD. En términos generales, nuestro estudio revela un incremento progresivo de la contratación de pólizas independientes ligado a los ingresos[4].

Contratación de ciberseguros por sector, 2023



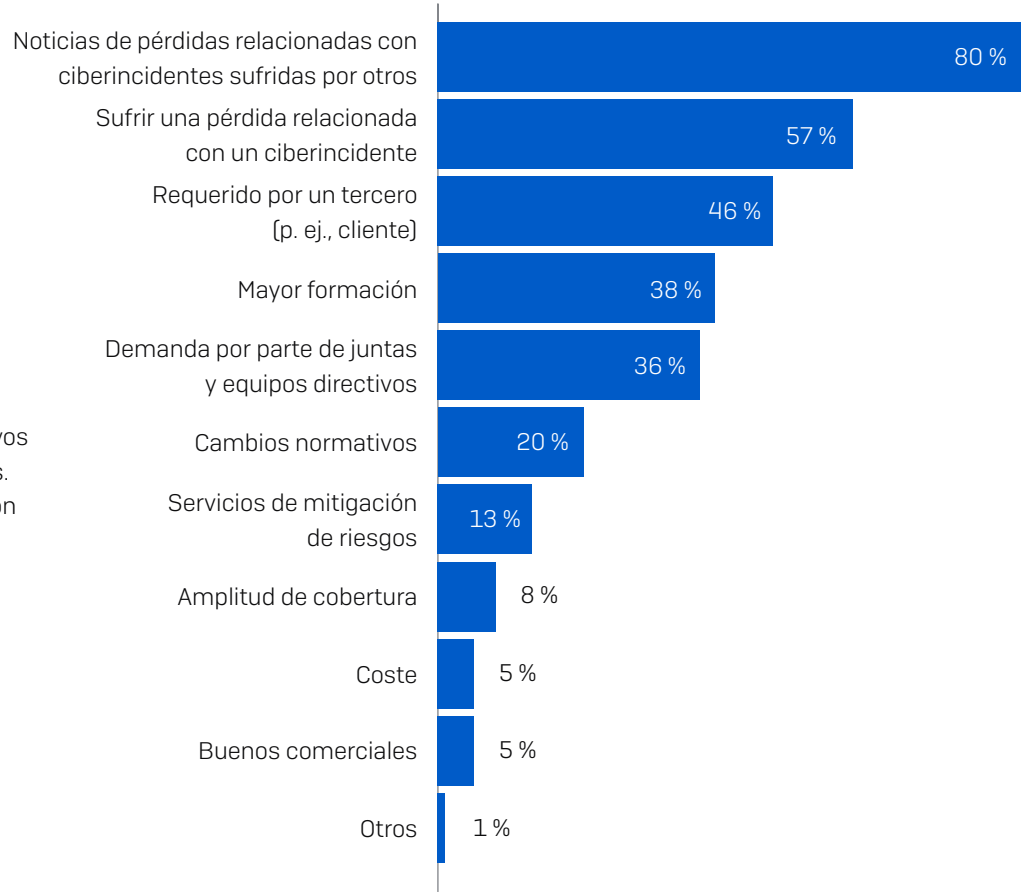
¿Tiene algún ciberseguro su organización? Sí, tenemos una ciberpóliza independiente; Sí, tenemos un ciberseguro como parte de una póliza de empresa más amplia (p. ej., una póliza de responsabilidad general). Números base en la tabla

4 La vital importancia de las ciberdefensas de primera línea para la contratación de seguros, Sophos.

Los ciberataques impulsan los ciberseguros

Gracias a una encuesta realizada por Advisen y PartnerRe a agentes de ciberseguros y empresas ciberaseguradoras de todo el mundo, tenemos conocimiento de los principales motores del incremento de las ventas de ciberseguros. Tal vez no sorprenda que los dos principales factores tras la contratación de un ciberseguro sean las noticias de pérdidas relacionadas con ciberincidentes sufridas por otros y sufrir una pérdida relacionada con un ciberincidente. Sin embargo, en tercer lugar está el hecho de que sea un requisito de un tercero. Ante el aumento de los ataques a la cadena de suministro, cada vez se exige más a las organizaciones que cuenten con un ciberseguro como condición para entablar una relación comercial que cubra al cliente si sufre un ciberincidente como resultado de la colaboración.

Más de un tercio (36 %[5]) cita la demanda por parte de juntas y equipos directivos como uno de los principales factores que impulsan la compra de ciberseguros. Esta elevada demanda por parte de los equipos directivos refleja la devastación que puede provocar un importante ciberincidente en toda una organización. Defenderse de las implicaciones de un ciberataque es ahora un problema empresarial generalizado, y no solo un reto de TI.



Cyber Insurance: The Market's View – Advisen, PartnerRe

5 Cyber Insurance: The Market's View, PartnerRe and Advisen

El coste de los ciberseguros

Como con todos los tipos de seguros, el coste depende de múltiples factores, entre ellos:

- **Demografía:** tamaño, industria, sector, ubicación, ingresos, etc.
- **Exposición potencial:** tipo y volumen de datos sensibles almacenados, recopilados y procesados.
- **Nivel de ciberseguridad:** las defensas de seguridad que utiliza una organización.
- **Historial:** las reclamaciones previas resultan siempre en primas más altas.
- **Condiciones de la póliza:** cobertura, límite de responsabilidad, etc.

Es importante conocer la diferencia entre las pólizas con deducible y con retención. En el caso de una póliza con deducible, el deducible (conocido como «franquicia» en algunos países) está incluido en el límite total de la póliza. En cambio, en el caso de una póliza con retención, el importe de la retención es adicional al límite de la póliza.

DEDUCIBLE	RETENCIÓN
Límite de póliza 100 000 USD; deducible (franquicia) 10 000 USD	Límite de póliza 100 000 USD; retención 10 000 USD
Usted paga los primeros 10 000 USD de la reclamación; la aseguradora paga 90 000 USD	Usted paga los primeros 10 000 USD de la reclamación; la aseguradora paga 100 000 USD
Cobertura total 100 000 USD	**Cobertura total 100 000 USD**

Agrupaciones de seguros

En el mercado de las pymes, no es extraño que haya una única entidad ciberaseguradora. Sin embargo, en el mercado de las grandes compañías, son habituales las agrupaciones de ciberseguros, ya que una única aseguradora no puede proporcionar toda la transferencia de riesgo necesaria. Los corredores de seguros crean agrupaciones para clientes individuales, reuniendo dos, tres, cuatro o más proveedores. El primer proveedor cubre la principal transferencia de riesgo, mientras que el resto cubre el exceso de transferencia de riesgo.

Panel de aseguradoras

Las ciberaseguradoras suelen tener proveedores preaprobados, a los que se conoce como «panel», con los que trabajan en caso de incidente. Si la empresa que sufre el incidente no tiene ninguna relación existente con proveedores, la ciberaseguradora le instará o incluso le exigirá que trabaje con una de estas organizaciones que integran el panel.

Dicho esto, la mayoría de las aseguradoras también están dispuestas a trabajar con otros proveedores de confianza, sobre todo si existe una relación previa o condiciones contractuales. Es lo que se denomina una aprobación fuera del panel. Como es lógico, trabajar con un proveedor que ya conoce la organización que sufre el incidente y su estructura informática y empresarial tiene muchas ventajas financieras y operativas.

Si su proveedor preferente no forma parte del panel de su compañía de seguros, puede solicitarlo. Es primordial contactar con antelación con su aseguradora para que el equipo de ciberseguros de su proveedor preferente pueda ponerse en contacto con la compañía de seguros para obtener las aprobaciones oportunas.

Necesidades de cobertura

Al seleccionar una póliza de ciberseguridad, es importante elegir el nivel correcto de cobertura para su organización. Necesita poder recuperarse adecuadamente y mantener su negocio a flote si sufre un ciberataque, al tiempo que mantiene sus primas a un nivel asequible.

Los costes de recuperación de un ciberataque son considerables y van en aumento. En 2023, el coste medio para que una organización subsanara el impacto de un ataque de ransomware fue de 1,82 millones USD[6], lo que supone un aumento con respecto a los 0,76 millones USD de 2020. Curiosamente, se trata de un descenso pequeño pero positivo con respecto a los 1,85 millones USD de 2021, lo que probablemente refleja que, a medida que el ransomware se ha hecho más frecuente, ha disminuido el daño a la reputación que causa un ataque. Paralelamente, las aseguradoras están mejor capacitadas para guiar a las víctimas de forma rápida y efectiva a través del proceso de respuesta al incidente, lo que reduce los costes de remediación de los ataques.

6 El estado del ransomware 2023, Sophos

El mercado de los ciberseguros

Las condiciones de los ciberseguros se han endurecido

Los ciberseguros han sido durante muchos años un mercado «blando», caracterizado por una gran capacidad y primas bajas. Sin embargo, por primera vez en sus más de 15 años de historia con pólizas independientes, el mercado se endureció en 2021, ya que las indemnizaciones que concedían las aseguradoras crecían más rápido que los ingresos que obtenían de las primas: el índice de siniestralidad de la industria aumentó de forma constante desde 2018, hasta llegar al 72,8 % en 2020[7]. (El índice de siniestralidad son los costes de los seguros divididos por el total de primas devengadas. Por ejemplo, si una empresa paga 80 USD en reclamaciones por cada 160 USD devengados en primas, el índice de siniestralidad sería del 50 %).

Los factores que provocaron este endurecimiento del mercado fueron varios:

- Aumentó el volumen y la complejidad de los ciberataques:
  - El 57 % de los responsables de TI afirmaron haber experimentado un aumento del volumen de ciberataques[8]
  - El 59 % observaron un aumento en la complejidad de los ataques[9]
- Los costes para recuperarse de un ciberataque aumentaron: como ya se ha mencionado, el coste medio para remediar un ataque ascendió a la demoledora cifra de 1,82 millones USD en 2023.

El resultado de este endurecimiento del mercado fue que se volvió mucho más difícil conseguir la cobertura de un ciberseguro. Esta situación fue confirmada por la encuesta a 5600 profesionales de TI que realizamos a principios de 2022, que reveló que el 94 % de las organizaciones con un ciberseguro contratado afirmaron que el proceso de obtención de la cobertura había cambiado en el último año:

- Según el 54 %, el nivel de ciberseguridad necesario para optar a un seguro era más alto.
- Según el 47 %, las pólizas eran más complejas.
- Según el 40 %, menos compañías ofrecían ciberseguros.
- Según el 37 %, el proceso era más largo.
- Según el 34 %, era más caro[10].

7 S&P Global, 1 de junio de 2021
8 El estado del ransomware 2022, Sophos
9 El estado del ransomware 2023, Sophos
10 Ciberseguros 2022: La realidad desde la primera línea de la seguridad de la información, Sophos

«Nuestro ciberseguro sube de precio y tenemos que superar más obstáculos que nunca».
Empresa de viajes corporativos

Este endurecimiento del mercado supuso un reto particularmente complejo para las entidades públicas, que suelen considerarse blancos fáciles para los ciberdelincuentes debido a que sus defensas son más débiles. En consecuencia, aquellas organizaciones públicas que deseaban obtener o renovar su cobertura disponían de menos proveedores y se enfrentaban a unas condiciones más duras, con precios que a veces se duplicaban de un año a otro.

«Los casos en que [las aseguradoras] solían ofrecer 10 millones USD, ahora ofrecen 5 millones».
Jack Kudale, director ejecutivo, Cowbell Cyber Inc.

En la segunda mitad de 2023 se ha producido una suavización selectiva del mercado de los ciberseguros. Con la entrada de nuevos operadores en el mercado, la capacidad se ha visto incrementada, aunque los proveedores son sumamente selectivos en cuanto a quién cubren: las empresas de bajo riesgo consiguen mejores ofertas de seguros, mientras que las de alto riesgo siguen teniendo dificultades para conseguir cobertura.

Los ciberseguros pagan

La buena noticia es que los ciberseguros responden siempre si ocurre lo peor y el tomador acaba siendo víctima de un ciberataque. En la encuesta El estado del ransomware 2022 de Sophos, el 98 % de los encuestados asegurados y atacados por el ransomware afirmaron que la aseguradora cubrió los costes derivados del ataque. En casi tres cuartas partes (73 %) de los incidentes, la empresa aseguradora cubrió los costes de limpieza para que la organización pudiera volver a ponerse en marcha. En el 36 % de los incidentes, el seguro pagó el rescate y, en el 33 % de los casos, pagó otros costes como los resultantes del tiempo de inactividad y las oportunidades perdidas.

Los ciberseguros propician la mejora de las defensas

Ante el endurecimiento del mercado, casi todas las organizaciones (97 %) con un ciberseguro han introducido cambios en sus ciberdefensas para mejorar su posición frente a las aseguradoras:

- El 64 % ha implementado nuevos servicios/tecnologías.
- El 56 % ha aumentado las actividades de formación/educación del personal.
- El 52 % ha cambiado procesos/conductas[11]

Pero, ¿cuáles son los cambios que debe hacer?
¿Qué le ayudará a mejorar su posición frente a las aseguradoras?

11 Ciberseguros 2022: La realidad desde la primera línea de la seguridad de la información, Sophos

Una ciberseguridad sólida ayuda a optimizar su posición frente a las ciberaseguradoras

Hay una relación directa entre la ciberseguridad y los ciberseguros; de hecho, el 95 % de las organizaciones que contrataron un seguro en 2023 afirmaron que la calidad de sus defensas repercutió directamente en su posición en el mercado asegurador[12]. Invertir en unas defensas robustas tiene numerosas ventajas en relación con los seguros:

1. Facilita el acceso a la cobertura

El 60 % de las organizaciones con un ciberseguro afirmaron que la calidad de sus defensas repercutió en su capacidad para obtener cobertura[13]. Las aseguradoras se centran cada vez más en gestionar y reducir el riesgo. Una ciberseguridad robusta le permite reducir su ciberriesgo, lo que, a su vez, le convierte en un candidato más atractivo para obtener cobertura con un ciberseguro. Aunque los requisitos específicos de cada aseguradora varían, en el mercado se suelen exigir varios cibercontroles:

Autenticación multifactor

La autenticación multifactor es un requisito esencial para obtener cobertura: las aseguradoras quieren cerciorarse de que esta carencia de seguridad común esté resuelta antes de asumir el riesgo.

«La renovación de nuestro ciberseguro depende de que habilitemos la MFA para el acceso remoto».

Proveedor de servicios y soporte de TI, EE. UU.

«Nos dijeron que si no implementábamos la MFA en el plazo de un año, perderíamos nuestro ciberseguro».

Proveedor del sector sanitario, EE. UU.

12 La vital importancia de las ciberdefensas de primera línea para la contratación de seguros, Sophos.
13 La vital importancia de las ciberdefensas de primera línea para la contratación de seguros, Sophos.

Endpoint Detection and Response (EDR) o Extended Detection and Response (XDR)

Una protección para endpoints de alta calidad que bloquee automáticamente las amenazas es una capa fundamental de unas ciberdefensas sólidas. Sin embargo, a medida que los adversarios mejoran sus ataques explotando herramientas de TI legítimas, credenciales comprometidas y vulnerabilidades sin parchear, una protección de endpoints por sí sola ya no resulta suficiente. Para detener filtraciones y ataques de ransomware avanzados (y las reclamaciones resultantes), es fundamental que también se supervisen, se investiguen y se responda proactivamente a las actividades sospechosas antes de que los ciberdelincuentes puedan desplegar sus ataques.

EDR y XDR son herramientas que permiten a los especialistas en seguridad detectar e investigar posibles ataques y neutralizar un ciberataque avanzado antes de que se produzcan daños. Como su nombre indica, la EDR trabaja solamente con puntos de datos procedentes de tecnologías de protección de endpoints, mientras que la XDR utiliza fuentes de datos de soluciones de protección de endpoints y de toda la pila de seguridad (incluidas las soluciones de seguridad de firewalls, correo electrónico, la nube y dispositivos móviles) para ofrecer una mayor visibilidad y acelerar la detección y respuesta. La EDR en particular es a menudo un requisito previo para obtener cobertura con la mayoría de las ciberaseguradoras, y las organizaciones sin esta funcionalidad suelen tener dificultades para contratar una póliza.

Detección y respuesta gestionadas (MDR)

MDR es un servicio 24/7 totalmente gestionado prestado por expertos especializados en detectar y responder a los ciberataques que las soluciones tecnológicas por sí solas no pueden detener. Ofrece el máximo nivel de protección frente a las ciberamenazas, lo que minimiza el riesgo y la probabilidad de que se presenten reclamaciones. Aunque rara vez es un requisito indispensable para obtener cobertura, las organizaciones que utilizan los servicios MDR suelen ser considerados clientes «de primer nivel» por las aseguradoras, ya que representan un nivel de riesgo inferior.

«El departamento jurídico quiere contratar un seguro contra el ransomware y [MDR] es el paso que necesitamos para conseguirlo».

Proveedor de soluciones y tecnología de TI, alcance global

Plan de respuesta a incidentes

La mejor manera de evitar que un ciberataque acabe en una infracción de seguridad es prepararse con antelación. A menudo, después de que una organización sufra una infracción, se dará cuenta de que podría haber evitado muchos costes, molestias e interrupciones si hubiera contado con un plan de respuesta a incidentes. Contar con un plan detallado que le permita minimizar el impacto de un incidente reducirá su ciberriesgo, lo que le convertirá en un candidato más atractivo para las aseguradoras.

2. Reduce las primas

El 62 % de las organizaciones con un ciberseguro afirmaron que la calidad de sus defensas repercutió en el coste de su cobertura[14]. Igual que tener una alarma y cerraduras en las ventanas reduce las primas de los seguros del hogar, disponer de unas ciberdefensas avanzadas ayuda a reducir los costes de los ciberseguros. Aunque los algoritmos específicos que utilizan las aseguradoras para calcular las primas son un secreto muy bien guardado, los clientes afirman sistemáticamente que la calidad de su protección tiene un efecto sobre sus primas.

«Como no teníamos la EDR implementada en el 100 % de nuestros dispositivos, [el coste de] nuestro seguro se duplicó».

Empresa de alojamiento web, EE. UU.

«Con Measured, los clientes que han implementado los productos Sophos MDR o Sophos Endpoint pueden reducir la prima de su ciberseguro en hasta un 25 %».

Measured Insurance, EE. UU.

3. Reduce la probabilidad de abrir una reclamación

Al igual que ocurre con otros seguros, si presenta una reclamación, es posible que tenga dificultades para renovar su póliza. Las organizaciones que han presentado reclamaciones también acusan un aumento significativo de sus primas en los años siguientes. Al minimizar su riesgo de sufrir un ciberataque gracias a unas ciberdefensas robustas, reducirá sus probabilidades de tener que recurrir a su póliza, lo que le ayudará a mantener sus primas a raya.

4. Reduce el riesgo de impago

Una higiene de seguridad TI deficiente puede impedirle recibir ayuda financiera en caso de producirse un incidente. Si la compañía de seguros cree que «dejó la puerta abierta» debido a prácticas inadecuadas, podría tener motivos para no pagarle una indemnización. Solventar estas carencias le ayudará a garantizar que la empresa aseguradora intervenga en el caso de que ocurra lo peor.

«No pagamos por ninguna reclamación, pérdida, filtración, investigación de privacidad o amenaza que se deba al uso de software o sistemas no actualizados o no compatibles».

Texto de la póliza de Hiscox Cyberclear™, Reino Unido, junio de 2021

5. Minimiza el impacto y el coste en caso de incidente

Responder de forma rápida y adecuada a un ciberataque puede reducir notablemente el impacto y el coste del incidente. Tener implementado un plan de respuesta a incidentes de malware y poder recurrir a expertos en respuesta a incidentes le ayudará a minimizar las consecuencias del ataque.

14 La vital importancia de las ciberdefensas de primera línea para la contratación de seguros, Sophos.

Cómo puede ayudar Sophos

Optimice sus ciberdefensas

Sophos permite a las organizaciones implantar muchos de los cibercontroles que son cada vez más necesarios tanto para optar a la cobertura como para acceder a las mejores primas y condiciones en las pólizas, todo ello con el respaldo de la información sobre amenazas y los conocimientos de ciberseguridad de Sophos X-Ops.

Sophos Endpoint Detection and Response (EDR)

Sophos EDR combina la robusta estrategia centrada en la prevención de Sophos Endpoint con unas potentes funciones de detección y respuesta que permiten a los analistas de seguridad y administradores de TI buscar, investigar y responder a la actividad sospechosa en todos los endpoints y servidores. Las detecciones se priorizan con análisis basados en IA, lo que le ayuda a identificar en qué debe invertir más tiempo y energía. Los operadores pueden acceder a los dispositivos de manera remota para investigar problemas, instalar y desinstalar software, finalizar procesos activos, ejecutar scripts o programas y editar archivos de configuración, entre otras acciones.

Sophos Extended Detection and Response (XDR)

Cuanto más vea, más rápido podrá actuar. Sophos XDR utiliza telemetría de sus actuales inversiones en seguridad, sean o no de Sophos, para que pueda detectar, investigar y responder a la actividad sospechosa en todo su entorno de seguridad.

- **Detección:** las detecciones basadas en IA proporcionan una visibilidad instantánea de la actividad sospechosa en todas las superficies de ataque claves, y nuestra sencilla búsqueda sin SQL le permite buscar amenazas a toda velocidad.
- **Investigación:** los casos creados y las detecciones priorizadas automáticamente permiten centrarse en lo importante, mientras que nuestra experiencia de usuario diseñada por analistas le brinda la información y las herramientas que necesita para llevar a cabo investigaciones fácilmente.
- **Respuesta:** las numerosas herramientas de gestión de casos y acciones de respuesta le permiten colaborar con miembros del equipo y neutralizar rápidamente los ataques.

Sophos Managed Detection and Response (MDR)

Sophos MDR es el servicio MDR en el que más confía el mundo, ya que protege a más organizaciones que cualquier otro proveedor. Ofrece lo último en protección a través de un servicio totalmente gestionado prestado por un equipo de expertos que se encarga de la detección, investigación y respuesta a amenazas 24/7. Con una media de tiempo de cierre de incidentes de 38 minutos, Sophos MDR minimiza enormemente el riesgo de un ciberincidente grave y optimiza su posición frente a las aseguradoras.

Reduzca la probabilidad de realizar una reclamación

Sophos le ofrece una protección líder a escala mundial contra el ransomware, el hacking malicioso y otras amenazas avanzadas. Nuestras soluciones le ayudan a minimizar el riesgo de sufrir un ciberincidente importante, lo que reduce la probabilidad de que necesite presentar una reclamación y ayuda a mantener el precio de las primas en el futuro.

«No podemos detener todo lo que llega. Por eso, confiamos en Sophos».

Vancouver Canucks, Canadá

Validación de Sophos por clientes y analistas

Las soluciones de Sophos gozan de un amplio reconocimiento entre los clientes, la comunidad de analistas y los evaluadores independientes:

Sophos Managed Detection and Response (MDR)

- Recibió la distinción Gartner® Customers' Choice™ para Managed Detection and Response (MDR) en 2023 con una puntuación de los clientes de 4,8/5 en Gartner Peer Insights
- Nombrado líder para Managed Detection and Response (MDR) en los informes G2 Grid® de otoño de 2023
- Resultados excepcionales en la evaluación de MITRE Engenuity ATT&CK de 2022 para servicios administrados

Sophos Extended Detection and Response (XDR)

- Nombrado líder para XDR en los informes G2 Grid® de otoño de 2023
- Resultados excepcionales en las evaluaciones MITRE Engenuity ATT&CK 2023 (Turla)
- Reconocido como el líder global n.º 1 en el informe Seleccionar una solución de detección y respuesta ampliadas (XDR) integral de Omdia Universe

Sophos Endpoint Detection and Response (EDR)

- Nombrado líder en el Magic Quadrant™ de Gartner® 2022 de plataformas de protección de endpoints por 13.ª vez consecutiva
- Recibió la distinción Gartner® Customers' Choice™ para plataformas de protección de endpoints en 2023 y por segundo año consecutivo con una puntuación de los clientes de 4,8/5 en Gartner Peer Insights
- Nombrado líder en suites de protección para endpoints y EDR en los informes G2 Grid® de otoño de 2023 Resultados excepcionales en las evaluaciones MITRE Engenuity ATT&CK 2023 (Turla)
- Calificaciones AAA y puntuaciones de protección del 100 % en el informe de pruebas de protección para endpoints de SE Labs del T3 2023 en las categorías de grandes empresas y de pymes.

Para obtener más información sobre las soluciones de Sophos haga clic aquí

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

2024-01-12 (WP-PC)

SOPHOS