SOPHOS

EL ESTADO DEL RANSOMWARE 2020

Resultado del studio independiente realizado a 5000 directores de TI en 26 países

Monográfico Sophos Mayo de 2020

Introducción

Las historias de organizaciones paralizadas por el ransomware suelen dominar los titulares de las noticias TI, y los relatos de demandas de rescate de seis y siete cifras son habituales. Pero ¿las noticias cuentan la historia completa?

Para comprender la realidad que se esconde detrás de los titulares, Sophos encargó una encuesta independiente a 5000 responsables de TI de 26 países. Los hallazgos proporcionan una nueva visión de lo que realmente sucede una vez que el rescate llega. Revela el porcentaje de ataques que consiguen cifrar los datos; cuántas víctimas pagan el rescate; cómo el pago del rescate repercute en los costes generales de limpieza; y la función del seguro de ciberseguridad. Preparado para sorprenderse.

Acerca de la encuesta

Sophos encargó a la empresa de investigación especializada Vanson Bourne que encuestara a 5000 directores de TI sobre sus experiencias con el ransomware. Sophos no desempeñó ningún papel en la selección de los encuestados y todas las respuestas se proporcionaron de forma anónima. El estudio se realizó durante enero y febrero de 2020.

Los encuestados procedían de 26 países de los seis continentes:

PAÍS	# ENCUESTADOS
Australia	200
Bélgica	100
Brasil	200
Canadá	200
China	200
Colombia	200
República Checa	100
Francia	300
Alemania	300
India	300
Italia	200
Japón	200
Malasia	100

PAÍS	# ENCUESTADOS
México	200
Países Bajos	200
Nigeria	100
Filipinas	100
Polonia	100
Singapur	200
Sudáfrica	200
España	200
Suecia	100
Turquía	100
EAU	100
Reino Unido	300
Estados Unidos	500

Dentro de cada país, el 50 % de los encuestados pertenecían a organizaciones de entre 100 y 1000 empleados, mientras que el 50 % pertenecía a organizaciones de entre 1001 y 5000 empleados. Los encuestados procedían de diversos sectores, tanto públicos como privados.

SECTOR	# ENCUESTADOS	% RESPUESTAS
TI, tecnología y telecomunicaciones	979	20 %
Venta al por menor, distribución y transporte	666	13 %
Fabricación y producción	648	13 %
Servicios financieros	547	11 %
Sector público	498	10 %
Servicios empresariales y profesionales	480	10 %
Construcción y propiedad	272	5 %
Energía, petróleo/gas y servicios públicos	204	4 %
Medios de comunicación, ocio y entretenimiento	164	3 %
Otros	542	11 %

Resumen ejecutivo

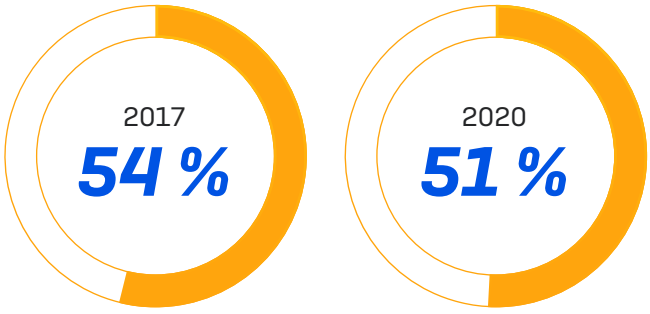
La encuesta ofrece una nueva visión de la experiencia de las organizaciones afectadas por el ransomware, entre ellas:

- **Casi las tres cuartas partes de los ataques de ransomware terminan en el cifrado de los datos.** El 51 % de las empresas se vieron afectadas por el ransomware en el último año. Los criminales lograron cifrar los datos en el 73 % de estos ataques.
- **El 26 % de las víctimas de ransomware cuyos datos fueron cifrados recuperaron sus datos pagando el rescate.** Otro 1 % pagó el rescate pero no recuperó sus datos.
- **El 94 % de las organizaciones cuyos datos fueron cifrados, los recuperaron.** Más del doble, los recuperaron por medio de copias de seguridad (56 %) que pagando el rescate (26 %).
- **Pagar el rescate duplica el coste de lidiar con un ataque de ransomware.** El coste medio para rectificar los efectos del ataque más reciente de ransomware (teniendo en cuenta el tiempo de inactividad, el tiempo de las personas, el coste de los dispositivos, de la red, la oportunidad perdida, el rescate pagado, etc.) es de 732 520 USD para las organizaciones que no pagan el rescate, y aumenta a 1 448 458 USD para las organizaciones que sí lo pagan.
- **A pesar de los titulares, el sector público se ve menos afectado por el ransomware que el sector privado.** El 45 % de las organizaciones del sector público se vieron afectadas por el ransomware el año pasado, en comparación con la media mundial del 51 %, y un máximo del 60 % en sectores de comunicación, ocio y entretenimiento.
- **Una de cada cinco organizaciones tiene un gran agujero en su ciberseguro.** El 84 % de los encuestados tiene un seguro de seguridad cibernética, pero sólo el 64 % tiene un seguro que cubre el ransomware.
- **El seguro de ciberseguridad paga el rescate.** Para las organizaciones que tienen un seguro antiransomware, el 94 % de las veces que se paga el rescate para recuperar los datos, es la compañía de seguros la que paga.
- **La mayoría de los ataques de ransomware exitosos incluyen datos en la nube pública.** El 59 % de los ataques en los que los datos fueron cifrados, implicaron datos en la nube pública. Si bien es probable que los encuestados hayan hecho una interpretación amplia de la nube pública, incluyendo los servicios basados en nube como Google Drive y Dropbox y las copias de seguridad en la nube como Veeam, es evidente que los ciberdelincuentes están apuntando a los datos dondequiera que se almacenen.

Parte 1: La prevalencia del ransomware

La mitad de las organizaciones fueron víctimas del ransomware el año pasado

El 51 % de los encuestados dijeron que habían sido víctimas del ransomware en el último año. Las organizaciones informaron de un ligero descenso de los ataques en comparación con años anteriores. Una encuesta anterior encargada por Sophos y publicada en 2017 (tamaño de la muestra: 1700 organizaciones) reveló que el 54 % de los encuestados habían sido víctimas del ransomware en el año anterior.



En el último año, ¿se ha visto afectada por el ransomware su empresa? Base: 5000 encuestados (2020), 1700 encuestados (2017).

Este descenso, aunque bienvenido, probablemente se deba a un cambio de táctica de los atacantes, más que a un menor foco en realizar este tipo de ataque. En el mercado masivo de 2017 el ransomware de escritorio 'spray and pray' fue muy común basado en los conocimientos de SophosLabs. Esos ataques se difundieron amplia e indiscriminadamente, lo que dio lugar a que un gran número de organizaciones fueran atacadas.

Ahora, en el año 2020, la tendencia son los ataques basados en servidores. Se trata de ataques muy específicos y sofisticados que requieren un mayor esfuerzo de despliegue, de ahí la reducción del número de ataques. Sin embargo, suelen ser mucho más dañinos debido al mayor valor de los activos cifrados y pueden paralizar a las organizaciones con solicitudes de rescate multimillonarias.

Para las preguntas posteriores de la encuesta, si la organización informó de múltiples ataques de ransomware en el último año, les pedimos que respondieran por *el ataque más significativo en el último año solamente.*

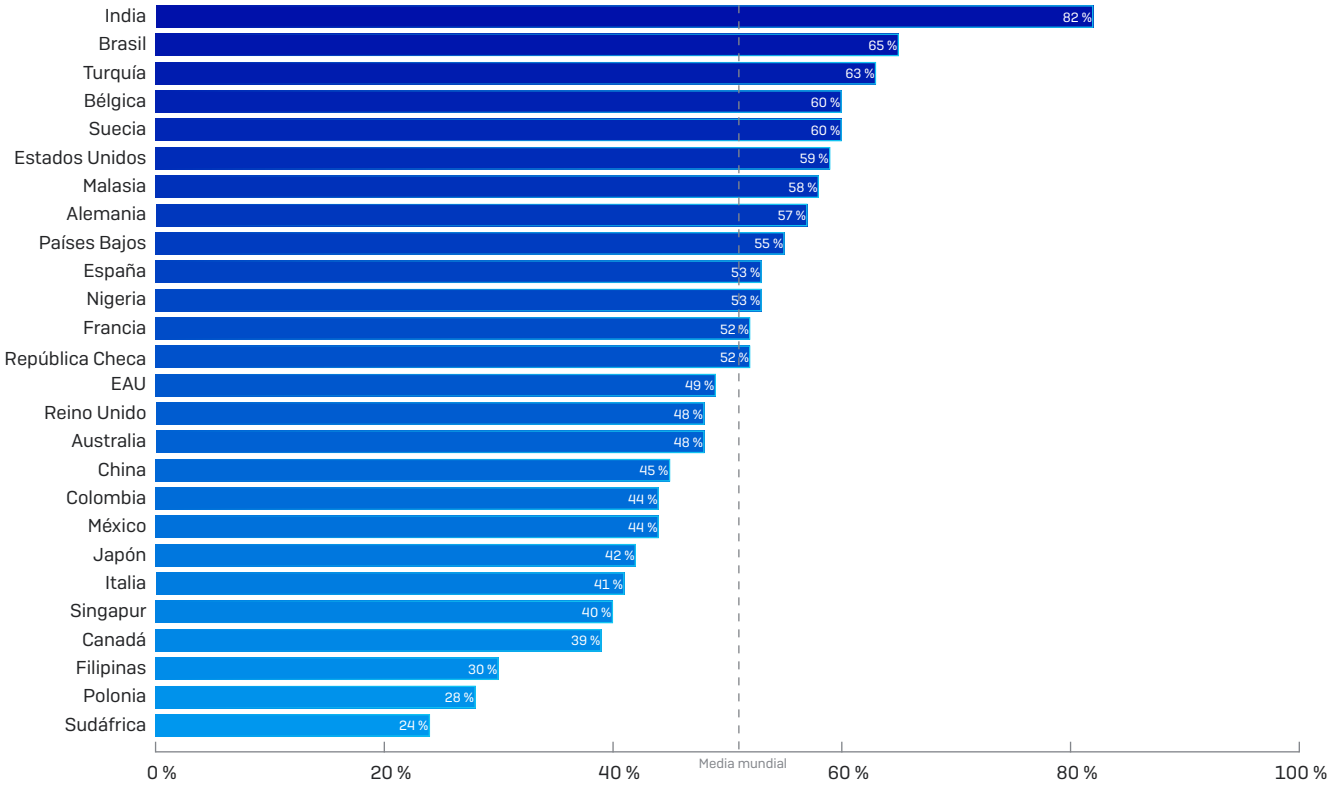
El tamañao no importa

Había una pequeña diferencia en los índices de ataques de ransomware según el tamaño de la organización. Mientras que poco menos de la mitad de las organizaciones más pequeñas (100-1000 empleados) fueron atacadas (47 %), poco más de la mitad (54 %) de las organizaciones más grandes (1001-5000 empleados) fueron asi mismo, atacadas.

Los niveles de ataque varían en todo el mundo

Viendo el nivel de los ataques de ransomware en todo el mundo observamos interesantes variaciones. Esto se debe probablemente a que los delincuentes centran sus esfuerzos donde ven mayores oportunidades de retorno, y también a que los países cuentan con diferentes niveles de defensa contra los rescates.

Porcentaje de empresas afectadas por el ransomware en el último año



En el último año, ¿se ha visto afectada por el ransomware su empresa? Base: 5000 encuestados.

- **India** (300 encuestados) encabeza la lista con el 82 % de las organizaciones que informaron haber sido víctimas de un ransomware en el último año. No es una gran sorpresa. La higiene cibernética es, en general, deficiente en la India, y la tecnología pirateada abunda, lo que crea debilidades en las defensas cibernéticas y hace que las organizaciones sean más vulnerables a los ataques.

- **Filipinas, Polonia y Sudáfrica** reportan los niveles más bajos de ciberataques. Como hemos comentado anteriormente, los ciberdelincuentes han pasado de los ataques de ransomware de "spray and pray" a ataques más selectivos basados en servidores que afectan a menos organizaciones, pero con mayores exigencias de rescate. Ellos geo-dirigen sus ataques para perseguir las oportunidades más lucrativas. Los tres países que se encuentran en la parte inferior de la escala de ataques, también tienen un PIB inferior al de muchos de los otros países que se encuentran en la parte superior de la lista, lo que puede ser la razón por la que reciben menos atención de los ciberdelincuentes.

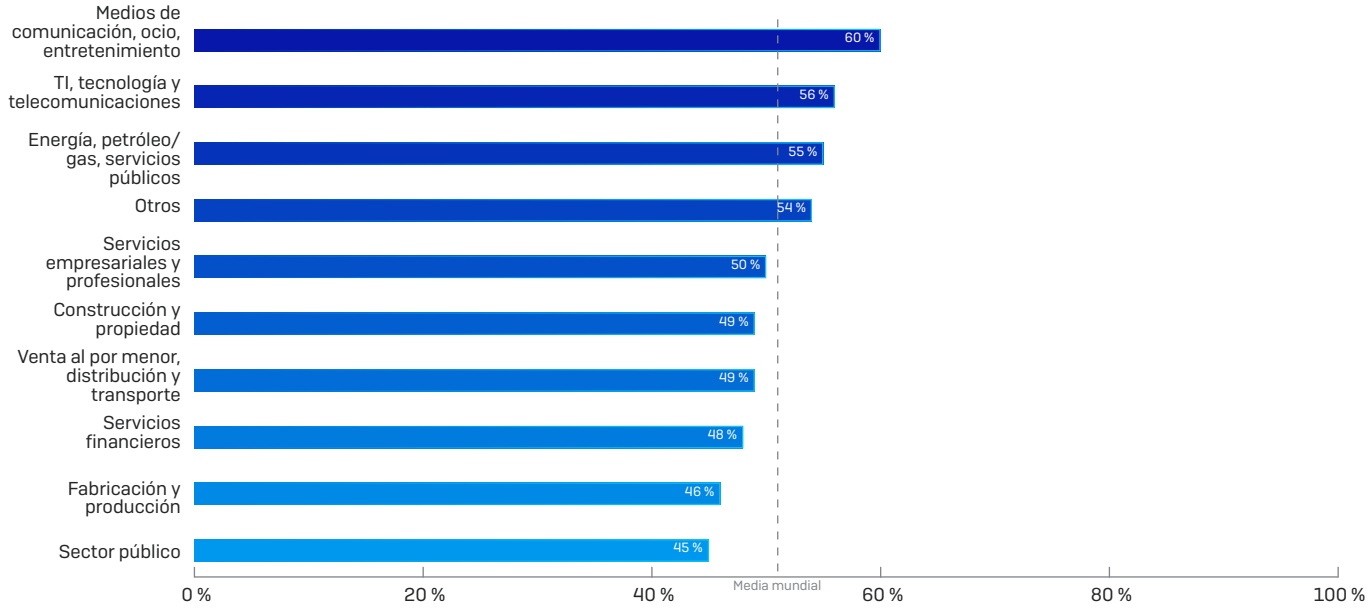
- Pasar de los ataques "spray and pray" a ataques dirigidos a objetivos más lucrativos probablemente contribuyó a la notable reducción del ransomware en **Sudáfrica**. En nuestra encuesta anterior (2017) el 54 % de los encuestados informaron haber sido víctimas del ransomware en el último año, pero ahora ha bajado al 24 %, una caída de más del 50 %.

- **Canadá** (200 encuestados) reporta sorprendentemente pocos ataques de ransomware. Como país avanzado, occidental, se consideraría un objetivo lucrativo, sin embargo, sólo el 39 % de los encuestados informan de que han sido víctimas de un ransomware. Esto es un total de 20 puntos porcentuales más bajo que el vecino EE.UU., donde el 59 % informó de ransomware. Al mismo tiempo, los encuestados canadienses estaban muy atentos a la cuestión y esperaban que se les presentara; el 68 % de las organizaciones no afectadas por el ransomware prevén estarlo en el futuro.

El sector público es el que menos ataques de ransomware sufre

Sí, lo ha leído correctamente - el sector público informó de menos ataques que todos los demás sectores. Los sectores de medios de comunicación, ocio y entretenimiento reportan los niveles más altos de ataque (60 %), seguidos de cerca por TI, tecnología y telecomunicaciones (56 %).

Porcentaje de empresas afectadas por el ransomware en el último año



En el último año, ¿se ha visto afectada por el ransomware su empresa? Base: 5000 encuestados.

A primera vista esto es sorprendente: las noticias están llenas de historias de hospitales y organizaciones gubernamentales que han sufrido un ataque de ransomware. Sin embargo, la encuesta revela que esos titulares están creando una imagen sesgada de la realidad.

En muchos países, el sector público está obligado a informar de los ataques de ransomware. Sin embargo, el sector privado a menudo no tiene esos requisitos, por lo que puede optar por mantener el ataque en silencio, tal vez para evitar crear preocupación entre los clientes, dañar la reputación o ser percibido como un blanco fácil por otros atacantes.

Estos hallazgos están respaldados por la propia investigación de Sophos sobre el ransomware SamSam. Trabajando con la organización de vigilancia de la criptografía Neutrino, Sophos hizo un seguimiento del dinero e identificó muchos pagos de ransomware y víctimas que anteriormente eran desconocidos. Sobre la base del número mucho mayor de víctimas que se conoce en la actualidad, parece que el sector privado ha sido el más afectado por SamSam.

Parte 2: El impacto del ransomware

Las tres cuartas partes de los ataques de ransomware resultan en el cifrado de los datos

Tradicionalmente, hay tres elementos principales para un ataque exitoso de ransomware: cifrar los datos, obtener el pago, descifrar los datos. En casi tres cuartas partes de los ataques de ransomware (73 %), los ciberdelincuentes lograron cifrar los datos.

Sin embargo, es alentador que en poco menos de una cuarta parte de los casos (24 %) el ataque se detuvo antes de que los datos pudieran ser cifrados. Parece que la tecnología anti-ransomware está teniendo un impacto en la tasa de éxito estos ataques.

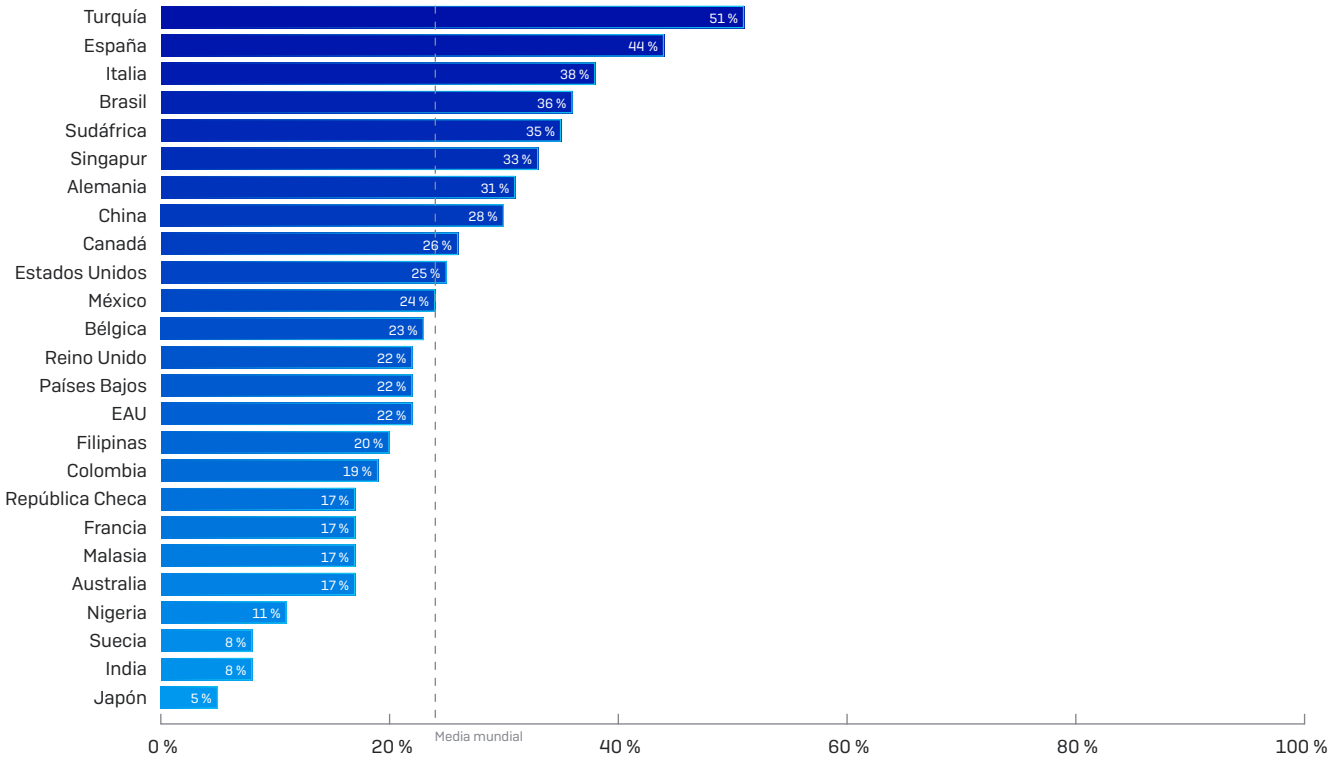
Un hallazgo interesante de la encuesta es que el 3 % de las organizaciones dijeron que sus datos no estaban cifrados pero que aún así se les pedía un rescate. Este tipo de ataque fue particularmente dominante en Nigeria, así como en Colombia, Sudáfrica, China, Polonia, Bélgica y Filipinas.

Se podría argumentar que se trata de una extorsión más que de un rescate. Dejando de lado la semántica, lo más importante es que se trata de un vector de ataque del que hay que estar atentos mientras los delincuentes buscan formas de hacer dinero sin el esfuerzo de cifrar y descifrar archivos.

Los ataques con más probabilidades de éxito sucedieron en Japón

Como país, Japón es el que menos éxito tiene en detener los ataques, ya que el 95 % de ellos resultan en el cifrado de los datos. Por el contrario, en Turquía, la mitad de los ataques (51 %) se detuvieron antes de que los datos pudieran ser cifrados. Entre las razones de esta variación mundial podrían figurar los diferentes niveles de conciencia tanto de la prevalencia de los programas de ransomware como de la probabilidad de que sean atacados, lo que a su vez podría dar lugar a diferentes niveles de defensas específicas contra el ransomware.

Porcentaje de ataques detenidos antes de que los datos fueran cifrados

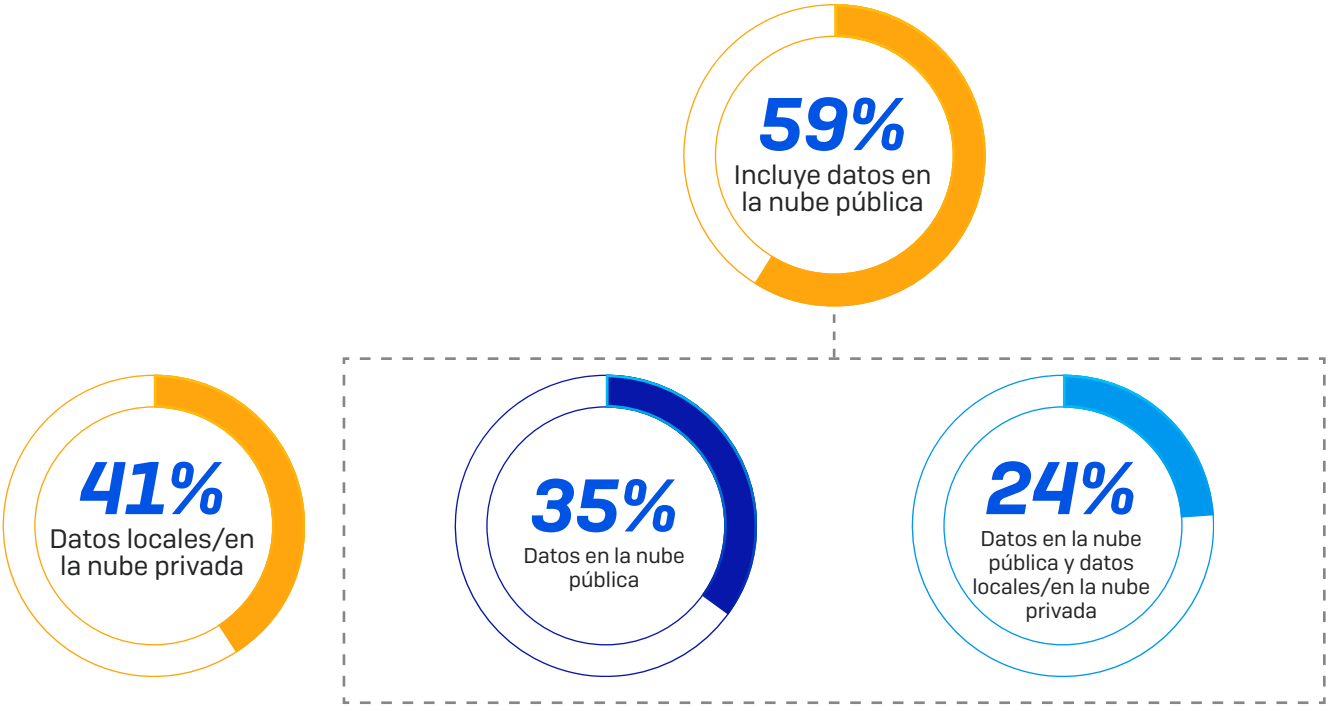


Porcentaje de encuestados que respondió 'No, el ataque fue detenido antes de que los datos pudieran ser cifrados' a: ¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? Pregunta visible solo para los encuestados cuya empresa se vio afectada por el ransomware en el último año. Base: 2538 encuestados.

Polonia ha sido eliminada de este gráfico ya que tiene una base de menos de 30 encuestados, y Filipinas tiene una base de solo 30.

Los datos en la nube pública son un objetivo principal

Preguntamos al 73 % de los encuestados que dijeron que sus datos habían sido cifrados en el último ataque de ransomware y qué datos estaban cifrados. El 41 % dijo solo datos on-premise y/o datos en la nube privada, mientras que el 35 % dijo solo datos en la nube pública. El 24 % dijo que una combinación de ambos. Sumando esto, casi seis de cada 10 ataques exitosos (59 %) incluyen datos en la nube pública.



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? Respuestas de los encuestados cuyos datos de la organización habían sido cifrados en el más reciente ataque de ransomware. Base: 1849 encuestados.

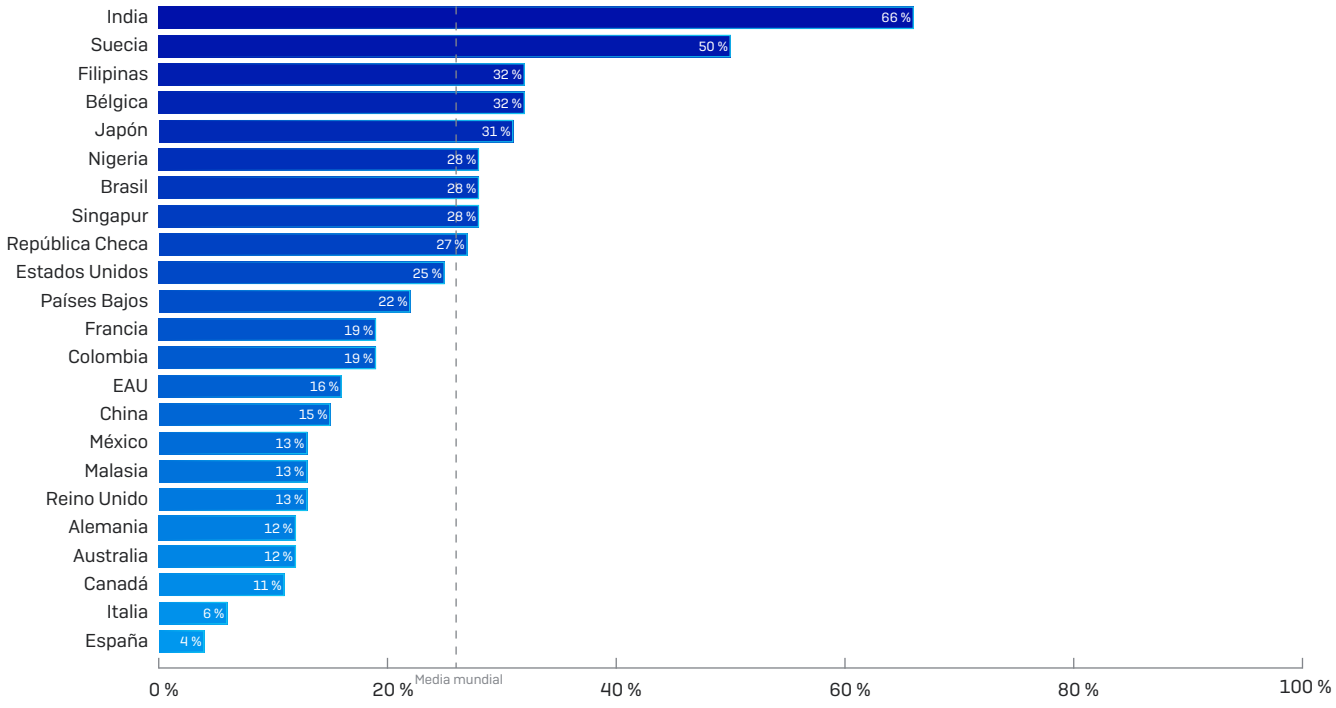
Un poco de precaución aquí: es probable que los encuestados adoptaran una interpretación amplia de la nube pública, incluyendo los servicios basados en la nube como Google Drive y Dropbox y backup de la nube como Veem, en lugar de centrarse únicamente en los servicios de tipo nube de AWS, Azure y Alibaba. Sin embargo, hay una clara ventaja: ningún dato está seguro, y debe asegurarse de que los datos almacenados en la nube están tan protegidos y respaldados como los datos almacenados en las instalaciones.

El 26 % de las víctimas de ransomware recuperaron sus datos pagando el rescate

El 26 % de las organizaciones cuyos datos fueron cifrados los recuperaron pagando el rescate. Otro 1 % de las organizaciones cuyos datos estaban cifrados pagaron el rescate pero no recuperaron sus datos, de modo que en general, el 95 % de las organizaciones que pagaron el rescate recuperaron sus datos (473 de las 496 organizaciones que lo pagaron).

Cuando se trata de pagar el rescate, vemos algunas variaciones por región dignas de mención. En la India, dos de cada tres (66 %) pagaron el rescate para recuperar los datos, mientras que el 29 % utilizó copias de seguridad. Por el contrario, en España sólo el 4 % pagó el rescate mientras que el 72 % restauró los datos de las copias de seguridad.

Porcentaje de empresas que pagaron el rescate



Porcentaje de encuestados que respondieron "Sí, pagamos el rescate" a: ¿Su empresa recuperó los datos en el ataque de ransomware más importante? Pregunta visible solo para los encuestados cuya empresa sufrió un ataque de ransomware en que se cifraron datos. Base: 1849 encuestados.

Nota: hemos eliminado Filipinas, Sudáfrica, Polonia y Turquía de este gráfico porque todos ellos tuvieron una base de 30 o menos para esta pregunta.

El 94 % de las empresas recuperaron sus datos

Si bien el 73 % de los ataques de ransomware lograron cifrar datos, la buena noticia es que el 94 % de las empresas afectadas consiguieron recuperar sus datos.

Como hemos visto, el 26 % recuperaron sus datos pagando el rescate. Sin embargo, más del doble (56 %) restauraron sus datos mediante copias de seguridad. El 12 % restante afirmaron que recuperaron sus datos por otros medios.

El tamaño de la empresa influye en el coste de remediación

Como era de esperar, la encuesta ha confirmado que el coste de remediar un ataque de ransomware es superior para las empresas de mayor tamaño.

Coste medio para remediar un ataque de ransomware

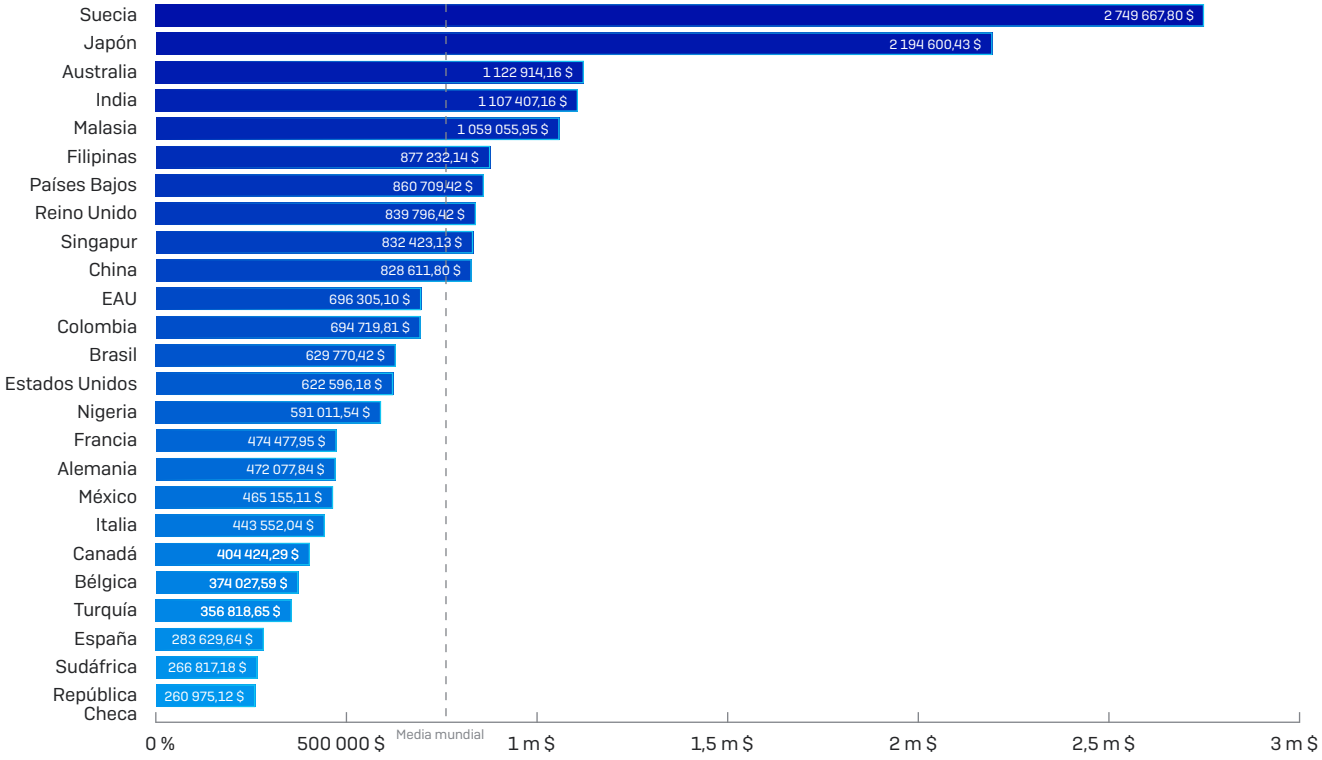
¿Cuál fue el coste aproximado para su empresa de rectificar los perjuicios del ataque de ransomware más reciente (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, el rescate pagado, etc.)? Pregunta visible solo para los encuestados cuya empresa se vio afectada por el ransomware en el último año. Base: 2538 encuestados.

El coste medio para la empresa de rectificar los perjuicios del ataque de ransomware más reciente (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, el rescate pagado, etc.) fue de 761 106 USD. En el caso de las empresas más pequeñas de 100-1001 empleados, el coste medio fue de 505 827 USD y, en el de las empresas de 1001-5000 empleados, de 981 140 USD.

Los costes del ransomware según el país

Sin embargo, lo que sí sorprende es la variación del coste de remediación en los distintos países encuestados. En particular, Suecia y Japón informan de unos costes considerablemente superiores a los de los demás países. En el otro extremo, Sudáfrica y la República Checa tienen los costes de remediación más bajos. Hemos excluido Polonia de este gráfico porque tuvo una base de menos de 30 encuestados.

Coste medio de remediación del ransomware por país



¿Cuál fue el coste aproximado para su empresa de rectificar los perjuicios del ataque de ransomware más reciente (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, el rescate pagado, etc.)? Pregunta visible solo para los encuestados cuya empresa se vio afectada por el ransomware en el último año. Base: 2538 encuestados.

Un posible motivo de esta variación en el coste son los costes de la mano de obra en los distintos países. Suecia y Japón suelen ser países con salarios más altos, de modo que el coste de las horas de trabajo requeridas para remediar el ataque de ransomware también es alto. Por el contrario, Sudáfrica y la República Checa son países en que el coste de la mano de obra suele ser inferior.

Ya hemos visto que Suecia tiene el índice más alto de pagos de rescates de todos los países encuestados, en segundo lugar después de la India. Sin embargo, a diferencia de la India, también tiene unos costes de mano de obra superiores, combinación que tiene como resultado un doble golpe financiero a la hora de resolver los problemas ocasionados por el ransomware.

Pagar el rescate duplica el coste

Una de las conclusiones más interesantes que se deriva de la encuesta es que pagar el rescate prácticamente duplica el coste de remediación total en comparación con no pagar o recuperar los datos mediante copias de seguridad o por otros medios. No pagar un rescate generalmente no solo nos hace sentir mejor por el hecho de no haber entregado nuestro dinero a los delincuentes, sino que además supondrá un ahorro a largo plazo.

Coste medio para remediar un ataque de ransomware

¿Su empresa recuperó los datos en el ataque de ransomware más importante? Los datos solo representan a los encuestados cuyos datos de empresa habían sido cifrados en el ataque de ransomware más reciente. Base: 1849 encuestados. **Pagaron el rescate** combina las respuestas "Sí, pagamos el rescate" y "No, aunque pagamos el rescate". **No pagaron el rescate** combina las respuestas "Sí, utilizamos copias de seguridad para restaurar los datos", "Sí, utilizamos otros medios para recuperar nuestros datos" y "No, no pagamos el rescate".

Esto puede sonar contradictorio: si ha pagado el rescate, ¿por qué cuesta más? Porque, aunque pague el rescate, necesitará hacer mucho trabajo para restaurar los datos igualmente. De hecho, es probable que los costes de recuperar los datos y restaurar la normalidad sean los mismos tanto si recupera los datos de los delincuentes como si lo hace con sus copias de seguridad. Pero si paga el rescate, tendrá otro coste adicional.

Parte 3: El rol de los seguros

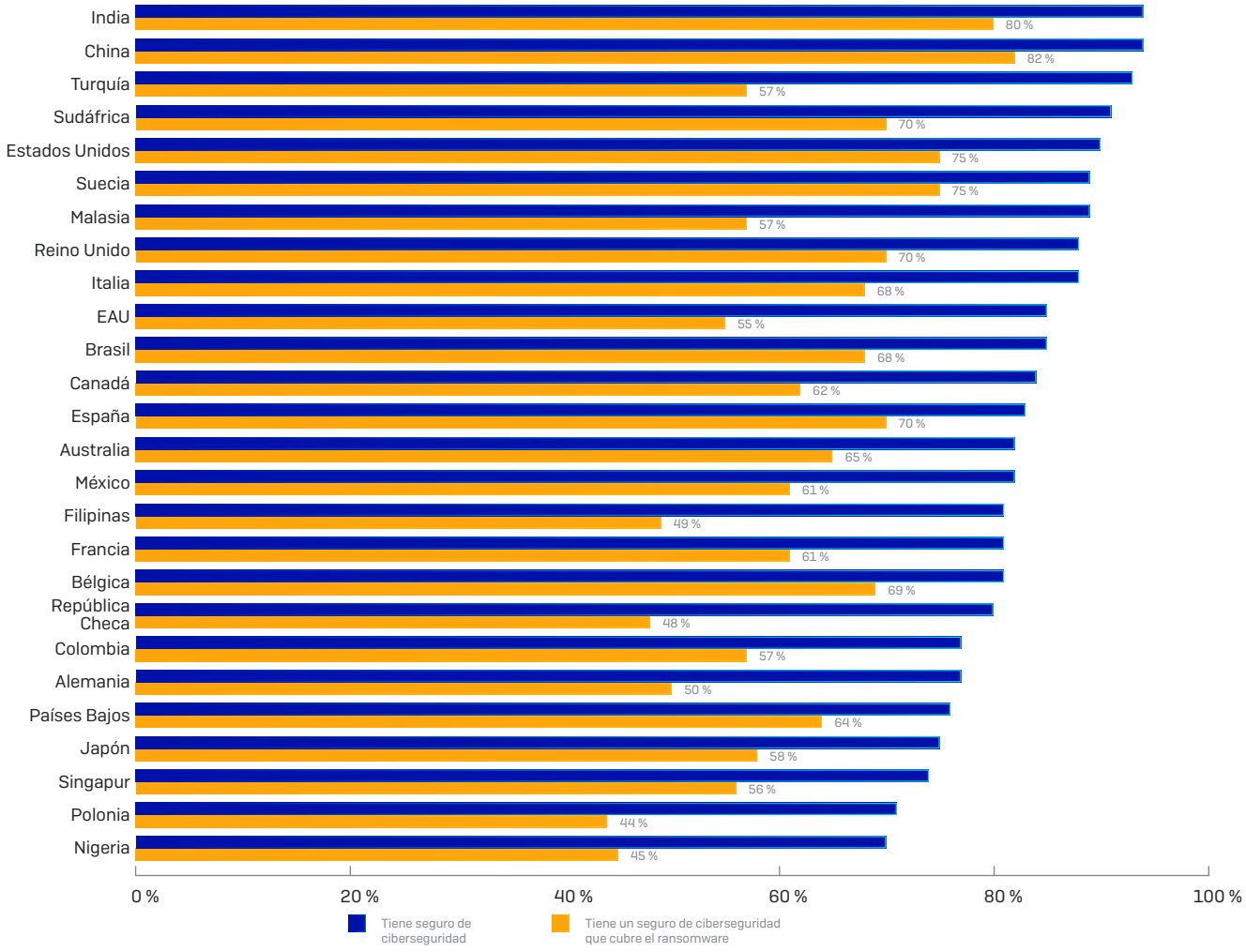
Una de cada cinco empresas tiene carencias en su seguro de ciberseguridad

Actualmente los seguros de ciberseguridad son la norma, puesto que el 84 % de las empresas afirman que disponen de uno. Sin embargo, solo el 64 % cuenta con un seguro de ciberseguridad que cubra el ransomware. Esto significa que una de cada cinco empresas (20 %) paga por un seguro de ciberseguridad que no cubre el ransomware.

¿Tiene su empresa un seguro de ciberseguridad que lo cubra si recibe un ataque de ransomware? Base: 5000 encuestados.

Dado que, como hemos visto, el 51 % de las empresas se han visto afectadas por el ransomware en el último año, y que el coste medio de remediación es de 761 106 USD, las empresas deberían cuestionarse el valor de los seguros que excluyen el ransomware.

Seguro de ciberseguridad por país



¿Tiene su empresa un seguro de ciberseguridad que lo cubra si recibe un ataque de ransomware? Base: 5000 encuestados.

Esta tabla muestra estos puntos de datos por país. El azul representa el porcentaje de empresas con seguro de ciberseguridad y el naranja representa el porcentaje con un seguro que cubre el ransomware. En lo que debemos fijarnos aquí es tanto en los números absolutos de cada columna como en la diferencia entre las dos barras para cada país.

La India encabeza la lista de empresas con seguro de ciberseguridad y tiene el segundo índice más alto (80 %) de empresas con seguro que cubre el ransomware. Puesto que la India también demostró ser el país más propenso a sufrir un ataque de ransomware, la correlación es lógica.

Turquía se situó en tercer lugar en la lista de países con más ataques de ransomware. Sin embargo, aunque es el tercer país con más empresas con seguros de ciberseguridad (el 93 % están cubiertas), también muestra una de las mayores diferencias entre barras, con solo un 57 % de empresas con cobertura para el ransomware.

A pesar de que China tiene un índice de ataques de ransomware por debajo de la media (el 45 % de las empresas se vieron afectadas en el último año), ocupa la primera posición compartida en número de seguros de ciberseguridad (94 %), así como la primera posición en seguros de ciberseguridad con cobertura para el ransomware (82 %). Efectivamente, muestra la diferencia más pequeña entre columnas de los 26 países encuestados.

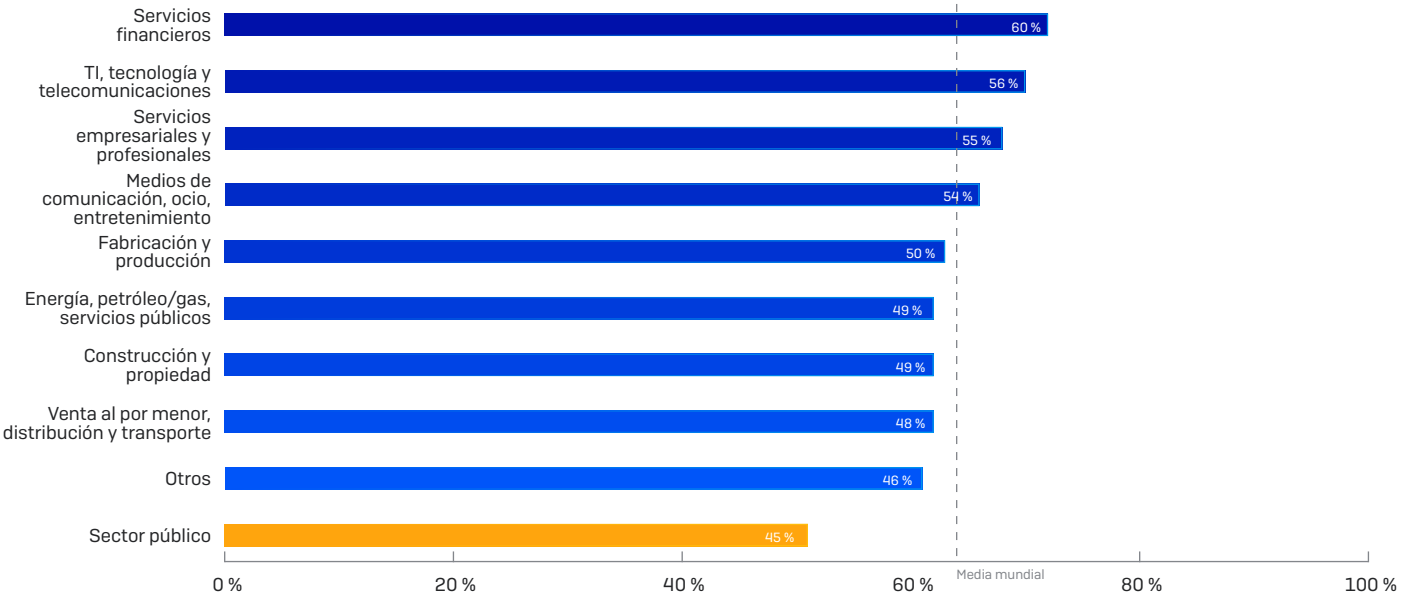
Un caso que destaca en este contexto es Alemania. Es sorprendente ver una economía desarrollada con un índice de seguros tan bajo (77 %), así como uno de los índices de seguros de ciberseguridad más bajos con cobertura para el ransomware (50 %). Alemania presentó niveles de ransomware por encima de la media (el 57 % de las empresas se vieron afectadas en el último año), lo que hace que estos datos sobre seguros sean aún más sorprendentes.

El sector público está más expuesto a los costes del ransomware

Aunque hemos visto que el sector público está menos expuesto al ransomware, lo cierto es que está más expuesto al coste total de un ataque.

De media, el 64 % de las empresas tienen seguros que cubren el ransomware. El sector de servicios financieros tiene el índice más alto de cobertura (72 %), lo que probablemente se debe a la propia naturaleza del sector, ya que los convierte en un objetivo lucrativo para los delincuentes. Las TI, las telecomunicaciones y la tecnología le siguen de cerca con un 70 %.

Seguros de ciberseguridad con cobertura para el ransomware



¿Tiene su empresa un seguro de ciberseguridad que lo cubra si recibe un ataque de ransomware? Base: 5000.

Las empresas del sector público, sin embargo, se quedan considerablemente atrás con respecto a sus equivalentes del sector privado. Solo el 51 % tiene un seguro que les cubra los costes del ransomware, diez puntos porcentuales por detrás del siguiente sector. Este índice de protección tan bajo podría deberse a los costes. El sector público suele contar con una financiación ajustada en todo el mundo, y puede ser que los presupuestos no alcancen a cubrir los seguros. Sea como sea, esto es tan solo un ahorro a corto plazo si un ataque logra penetrar en sus defensas.

Seguros de ciberseguridad y pagos de rescates

Ahora veamos qué papel juega la ciberseguridad en el pago de los rescates. Como hemos visto, el 73 % de los ataques de ransomware resultan en el cifrado de los datos. De las empresas cuyos datos fueron cifrados, el 26 % afirmaron haber pagado el rescate para recuperar los datos.

Sin embargo, al analizarlo más a fondo, descubrimos que, en prácticamente todos los incidentes en que se paga el rescate (94 %), es el seguro de ciberseguridad el que lo hace. Y, como hemos visto también, pagar el rescate duplica los costes generales de limpieza.

Parte 4: Técnicas de ataque del ransomware

Preguntamos a las empresas que afirmaron haber sido víctimas del ransomware en el último año cómo penetró el ataque en su empresa. La descarga de archivos y el correo electrónico con archivos adjuntos maliciosos encabezaron la lista, sumando un 29 % de los ataques. El segundo lugar lo ocuparon los ataques remotos a los servidores, que representaron el 21 % de los ataques.

CÓMO ENTRÓ EL RANSOMWARE EN LA EMPRESA	N.º DE INCIDENTES	% DE INCIDENTES
A través de una descarga de archivos/correo electrónico con un enlace malicioso	741	29 %
A través de un ataque remoto al servidor	543	21 %
A través de correo electrónico con un adjunto malicioso	401	16 %
Instancias en la nube pública mal configuradas	233	9 %
A través de nuestro protocolo de escritorio remoto (RDP)	221	9 %
A través de un proveedor que trabaja en nuestra empresa	218	9 %
A través de un dispositivo USB/de medios extraíbles	172	7 %
Otros	0	0 %
No lo saben	9	0 %
Total	2538	100 %

¿Cómo entró en su empresa el ataque de ransomware? Pregunta realizada a los encuestados cuya empresa se ha visto afectada por el ransomware en el último año. Base: 2538 encuestados.

Lo que realmente llama la atención al analizar estos datos es que no existe un único vector de ataque. En lugar de ello, los atacantes utilizan múltiples técnicas y cualquier defensa con carencias para introducirse. Cuando una técnica falla, pasan a la siguiente, y así hasta que encuentran un punto débil.

Estos datos demuestran la necesidad de una defensa por capas efectiva que cubra sus endpoints, servidores, instancias en la nube pública, correo electrónico, puerta de enlace de red y cadena de suministro. Centrarse en una única tecnología es una infección segura.

Recomendaciones

La encuesta ha confirmado que el ransomware sigue siendo una amenaza muy real para las empresas de hoy día. También ha arrojado luz sobre cómo minimizar su riesgo de convertirse en víctima:

1. **Empiece por asumir que *se verá* afectado**. El ransomware no hace distinciones: todas las empresas son posibles objetivos, independientemente del tamaño, el sector o la geografía. Planifique su estrategia de seguridad basándose en el supuesto de que recibirá un ataque.
2. **Invierta en tecnología antiransomware para detener el cifrado no autorizado.** El 24 % de los encuestados que se vieron afectados por el ransomware pudieron detener el ataque antes de que se cifraran sus datos.
3. **Proteja los datos allá donde se encuentren.** Prácticamente 6 de cada 10 ataques de ransomware que consiguieron cifrar datos afectaron a datos en la nube pública. Su estrategia debe incluir la protección de los datos en la nube pública, en la nube privada y aquellos almacenados localmente.
4. **Realice copias de seguridad periódicamente y guárdelas fuera de la red y en ubicaciones externas.** El 56 % de las empresas cuyos datos se cifraron restauraron sus datos mediante copias de seguridad en el último año. Utilizar copias de seguridad para restaurar sus datos reduce considerablemente los costes de remediar el ataque si lo comparamos con pagar del rescate.
5. **Asegúrese de que su seguro de ciberseguridad cubra el ransomware.** Compruebe que cuenta con una cobertura completa si sucede lo peor.
6. **Despliegue una defensa por capas.** Los responsables del ransomware utilizan una amplia gama de técnicas para esquivar sus defensas; cuando una está bloqueada, pasan a la siguiente, y así hasta que encuentran una grieta en la armadura. Es necesario que se proteja contra todos los vectores de ataque.

Presentación de Sophos Intercept X Endpoint

Los responsables del ransomware combinan técnicas de ataque sofisticadas con el hacking manual. Sophos Intercept X Endpoint le ofrece las tecnologías de protección avanzada que necesita para desestabilizar toda la cadena de ataque, como:

- **Reversión de cifrado**: CryptoGuard bloquea el cifrado no autorizado de archivos y los revierte a su estado seguro en segundos.
- **Protección contra exploits**: detecta y bloquea casi 40 técnicas de explotación utilizadas para descargar e instalar malware, lo que evita que los atacantes penetren en su red.
- **Protección contras amenazas con IA**: el motor de Deep Learning propio de Sophos impide de forma predictiva más ataques y tiene menos falsos positivos que cualquier otro software de seguridad.
- **Robo de credenciales**: impide que los hackers se hagan con sus credenciales, bloqueando los accesos no autorizados al sistema y el aumento de privilegios de administrador.

Obtenga más información e inicie una demostración online instantánea en

es.sophos.com/intercept-x

Acerca de Vanson Bourne

Vanson Bourne es una consultora independiente especializada en estudios de mercado para el sector tecnológico. Su reputación de análisis sólidos y creíbles basados en la investigación se asienta en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en todos los principales mercados. Visítelos en www.vansonbourne.com

Ventas en España:
Tel.: (+34) 913 756 756
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

200629 WPEN (NP)

SOPHOS