SOPHOS
Cybersecurity evolved.

El estado del ransomware en el sector de los servicios financieros 2021

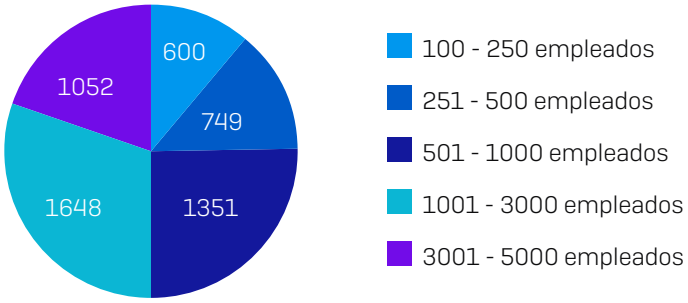
Basado en una encuesta independiente a 550 responsables de TI, este monográfico incluye nueva información detallada sobre la situación actual del ransomware en el sector de los servicios financieros. Ofrece un análisis en profundidad sobre la incidencia del ransomware en los servicios financieros, el impacto de estos ataques sobre las víctimas, el coste de la remediación del ransomware y la situación en que se encuentra este sector en términos de futuras expectativas y preparación frente a estos ataques.

Monográficos de Sophos. Septiembre 2021

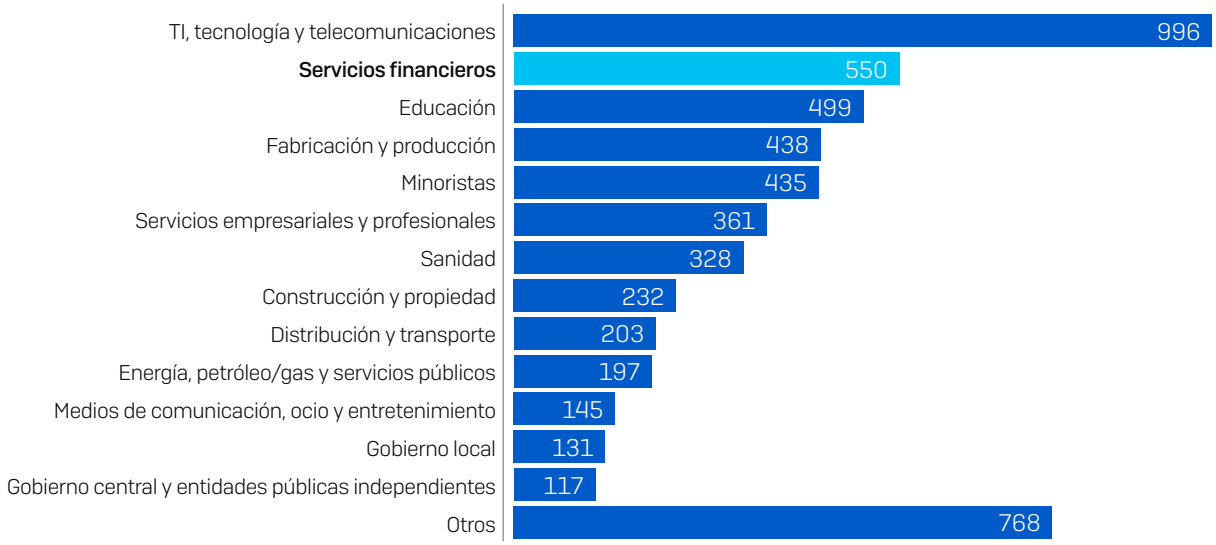
Acerca de la encuesta

Sophos encargó una encuesta global a 5400 responsables de TI de 30 países por parte de la consultora independiente Vanson Bourne. Los encuestados procedían de una amplia variedad de sectores, incluidos 550 responsables del sector de los servicios financieros. La encuesta se llevó a cabo en enero y febrero de 2021.

¿Cuántos empleados tiene su organización en todo el mundo? [5400]



¿A qué sector pertenece su organización? [5400]



El 50 % de los encuestados de cada país procedían de organizaciones con entre 100 y 1000 empleados y el otro 50 %, de organizaciones con entre 1001 y 5000 empleados. Los 550 responsables de TI del sector de los servicios financieros procedían de todas las regiones geográficas incluidas en la encuesta: América, Europa, Oriente Medio, África y Asia-Pacífico.

Región	N.º de encuestados
América	146
Europa	197
Oriente Medio y África	78
Asia-Pacífico	129

550 responsables de TI del sector de los servicios financieros

Principales conclusiones en los servicios financieros

- El **34 %** de las organizaciones de servicios financieros se **vieron afectadas por el ransomware en el último año**.
- El **51 %** de las organizaciones afectadas por el ransomware afirmaron que los **ciberdelincuentes consiguieron cifrar sus datos** en el ataque más importante.
- El **25 %** de las organizaciones cuyos datos fueron cifrados **pagaron el rescate para recuperar sus datos** en el ataque de ransomware más importante.
- El **62 %** de las organizaciones cuyos datos se cifraron **utilizaron copias de seguridad para recuperar los datos**.
- El **63 % de los datos fueron restaurados**, de media, después de pagar el rescate, con lo que más de un tercio de los datos quedaron inaccesibles.
- El **91 %** de las organizaciones de servicios financieros **tienen un plan de recuperación de incidentes de malware**.
- **La factura media de rectificar un ataque de ransomware** en el sector de los servicios financieros, teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado y demás, fue de **2,10 millones USD**.

El ransomware es un problema muy real para la industria de los servicios financieros. Aproximadamente un tercio (34 %) de las organizaciones se vieron afectadas por el ransomware en el último año y, aunque es una cifra inferior a la media global del 37 %, sigue siendo un gran motivo de preocupación.

Un cuarto (25 %) de las organizaciones de servicios financieros cuyos datos fueron cifrados pagaron el rescate para recuperar sus datos. De nuevo, se trata de un porcentaje inferior a la media de todos los sectores del 32 %, y probablemente se deba a la capacidad superior a la media de este sector de restaurar datos a partir de copias de seguridad. Parece que los servicios financieros están cosechando los beneficios de tener planes de continuidad empresarial y de recuperación de desastres (BC-DR), que sirven para prepararse para situaciones como un ataque de ransomware. Puesto que las organizaciones que pagaron el rescate recuperaron solo el 63 % de sus datos de media, las instituciones financieras hacen bien en apostar por las copias de seguridad como su método de recuperación principal.

En términos generales, el sector de los servicios financieros destaca por ser el único en el que todas las organizaciones cuyos datos fueron cifrados lograron recuperar al menos parte de ellos. De nuevo, es probable que el trabajo de recuperación de desastres de las organizaciones financieras les haya preparado adecuadamente para los ataques de ransomware.

Los servicios financieros también se sitúan por debajo de la media en cuanto a los rescates pagados, puesto que efectuaron un pago medio de 69 369 USD frente a la media de todos los sectores de 170 404 USD (Nota: el número base de encuestados de servicios financieros no es suficientemente elevado como para sacar conclusiones sólidas).

Sin embargo, aquí se terminan las buenas noticias. El coste general de recuperación del ransomware para los servicios financieros es de alrededor de un cuarto de millón de dólares más que la media global (2,10 millones frente a 1,85 millones USD). Probablemente esto se debe a los elevados gastos de las medidas de remediación para mantener el funcionamiento de las operaciones a cualquier precio, y a los altos costes de la notificación de filtraciones de datos, los perjuicios para la reputación y las sanciones por incumplimiento normativo que afectan a este sector.

Además, dos tercios (68 %) de los equipos de TI de los servicios financieros afirmaron que su carga de trabajo de ciberseguridad había aumentado durante 2020, seguramente por la necesidad de acomodar la rápida transición al teletrabajo provocada por la pandemia. Aunque esto habría afectado negativamente a la capacidad de los equipos de TI de detectar y responder rápidamente a los problemas de ciberseguridad, el lado positivo es que el 70 % de los equipos de TI afirmaron que su capacidad de desarrollar conocimientos y habilidades de ciberserguridad se vio incrementada durante el transcurso del año, lo que les resultará muy útil de cara al futuro.

Las organizaciones de servicios financieros deben seguir invirtiendo en copias de seguridad y planes de recuperación de desastres a fin de minimizar el impacto de cualquier ataque. También deben tratar de ampliar sus defensas antiransomware combinando la tecnología con la búsqueda de amenazas realizada por humanos para neutralizar los ataques avanzados de hoy día perpetrados por personas.

La incidencia del ransomware en los servicios financieros

Servicios financieros afectados por el ransomware en el último año

De los 550 encuestados de servicios financieros, el 34 % se vieron afectados por el ransomware en el último año, en el sentido de que *múltiples ordenadores recibieron un ataque de ransomware, pero no se cifraron datos necesariamente*.

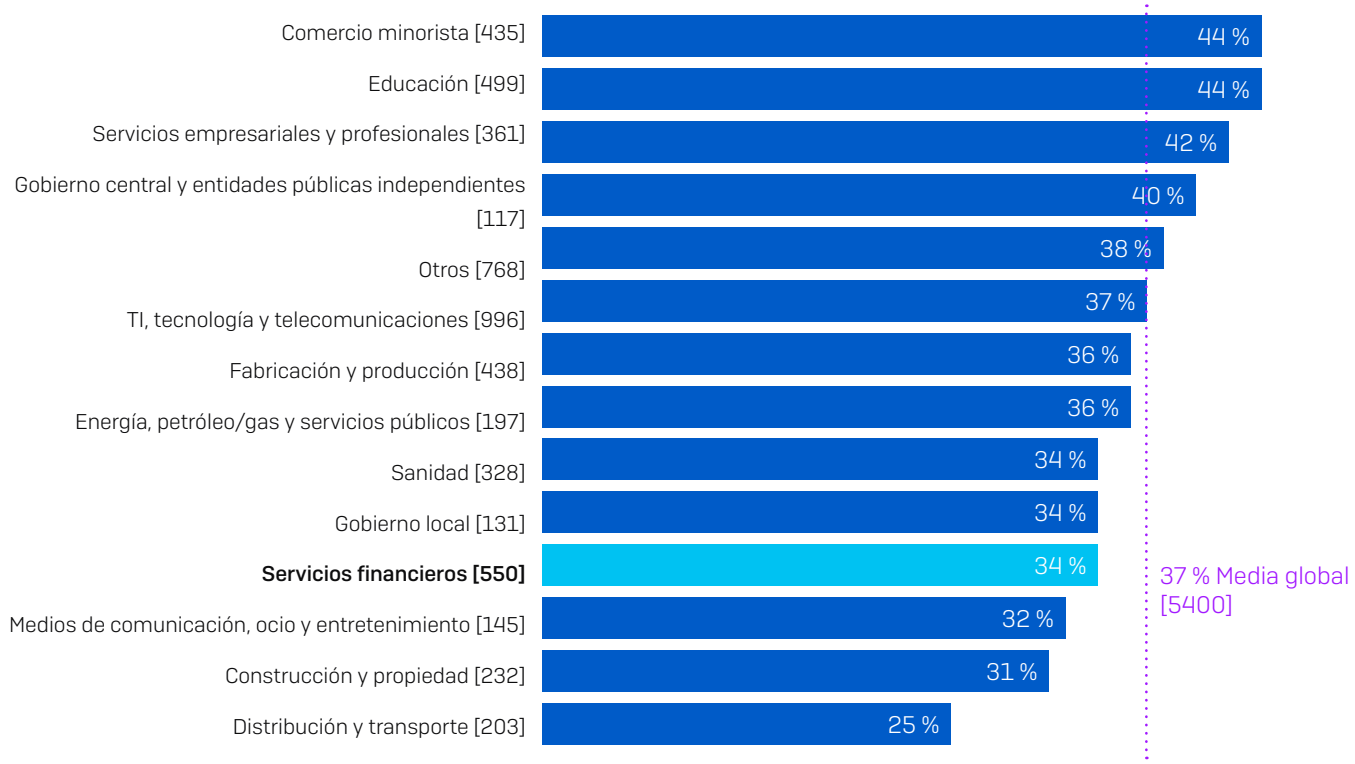
En el último año, ¿se ha visto afectada por el ransomware su organización? [550 encuestados de servicios financieros]

De las organizaciones que no se vieron afectadas en el último año, el 42 % afirmaron que esperaban ser atacadas por el ransomware en el futuro, mientras que el 22 % estaban seguras de que no sufrirían futuros ataques. Más adelante en el informe, exploraremos más a fondo las razones tras la expectativa de sufrir una ataque en el futuro, además de qué es lo que da confianza a los demás de cara a futuros ataques.

Los servicios financieros sufren menos el ransomware que la media global

Si comparamos el sector financiero con otros, vemos que, en realidad, sufrió un volumen de ataques inferior a la media. El comercio minorista y la educación sufrieron la mayor cantidad de ataques de ransomware, ya que el 44 % de los encuestados de estos sectores afirmaron haberse visto afectados, en comparación con la media global del 37 %.

% de encuestados afectados por el ransomware en el último año



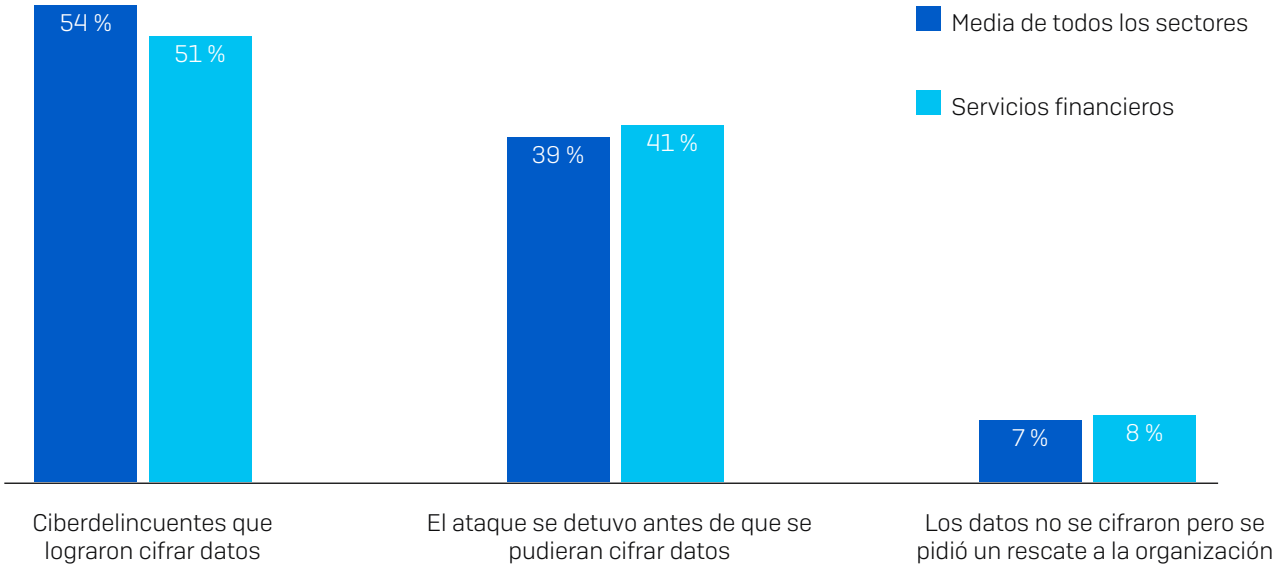
En el último año, ¿se ha visto afectada por el ransomware su organización? Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

De manera generalizada en todos los sectores, el porcentaje de organizaciones afectadas por el ransomware en el último año ha disminuido considerablemente en comparación con el año anterior, cuando el 51 % admitieron haber sido atacadas. Si bien este descenso es una buena noticia, probablemente se debe en parte a la evolución de los comportamientos de los atacantes observados por SophosLabs y el equipo de Sophos Managed Threat Response. Por ejemplo, muchos delincuentes han pasado de los ataques automatizados, genéricos y a gran escala a ataques más dirigidos que incluyen hacking manual realizado por humanos. Si bien el número total de ataques es inferior, según nuestra experiencia, el potencial de daños de estos ataques dirigidos es muy superior.

El impacto del ransomware

Capacidad de los servicios financieros de detener el cifrado de datos

Preguntamos a los encuestados cuyas organizaciones habían sido víctimas del ransomware en el último año si los ciberdelincuentes lograron cifrar sus datos. El 51 % de los encuestados de servicios financieros dijeron que sí, un porcentaje algo inferior a la media global del 54 %.



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? [2006/185 organizaciones de servicios financieros que se vieron afectadas por el ransomware en el último año]

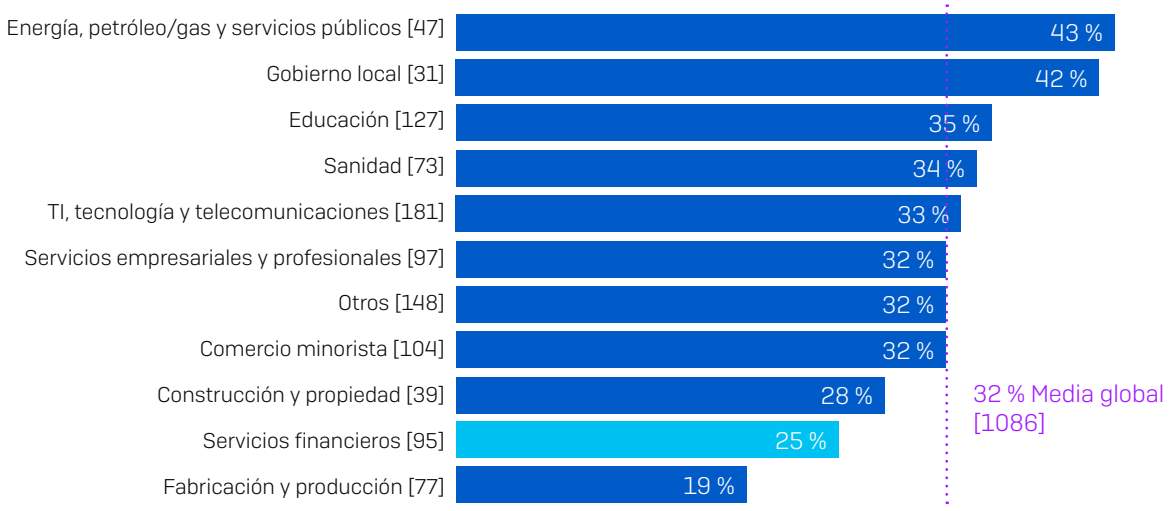
Si bien el sector de los servicios financieros consiguió detener el cifrado con mayor éxito que la media global (detuvo el 41 % de los ataques frente a una media del 39 %), este sector fue vulnerable a una nueva tendencia pequeña pero en crecimiento: los ataques de solo extorsión, en que los operadores del ransomware no cifran los archivos, sino que amenazan con filtrar la información robada online si no se paga un rescate. De hecho, el 8 % de las organizaciones de servicios financieros que se vieron afectadas por el ransomware sufrieron un ataque de tipo extorsión.

SophosLabs ha observado un incremento en este estilo de ataques durante el último año. Requieren menos esfuerzo por parte de los atacantes ya que no necesitan cifrar ni descifrar archivos, y los adversarios suelen aprovecharse de las sanciones oficiales por filtraciones de datos en sus exigencias a fin de presionar aún más a las víctimas para que paguen.

Predisposición a pagar el rescate

La encuesta reveló que los servicios financieros tienen una predisposición mucho menor a pagar el rescate que la mayoría de las demás industrias. Una de cada cuatro organizaciones de servicios financieros (25 %) cuyos datos se cifraron accedieron a la demanda de un rescate frente a una media global del 32 %. Una posible explicación de esto, tal como veremos más adelante, es la impresionante capacidad del sector para restaurar los datos cifrados a partir de copias de seguridad.

% que pagaron el rescate para recuperar sus datos



¿Su organización recuperó los datos en el ataque de ransomware más importante? Sí, pagamos el rescate; [número base en el gráfico] organizaciones en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante, omitiendo algunas opciones de respuesta, divididas por sector

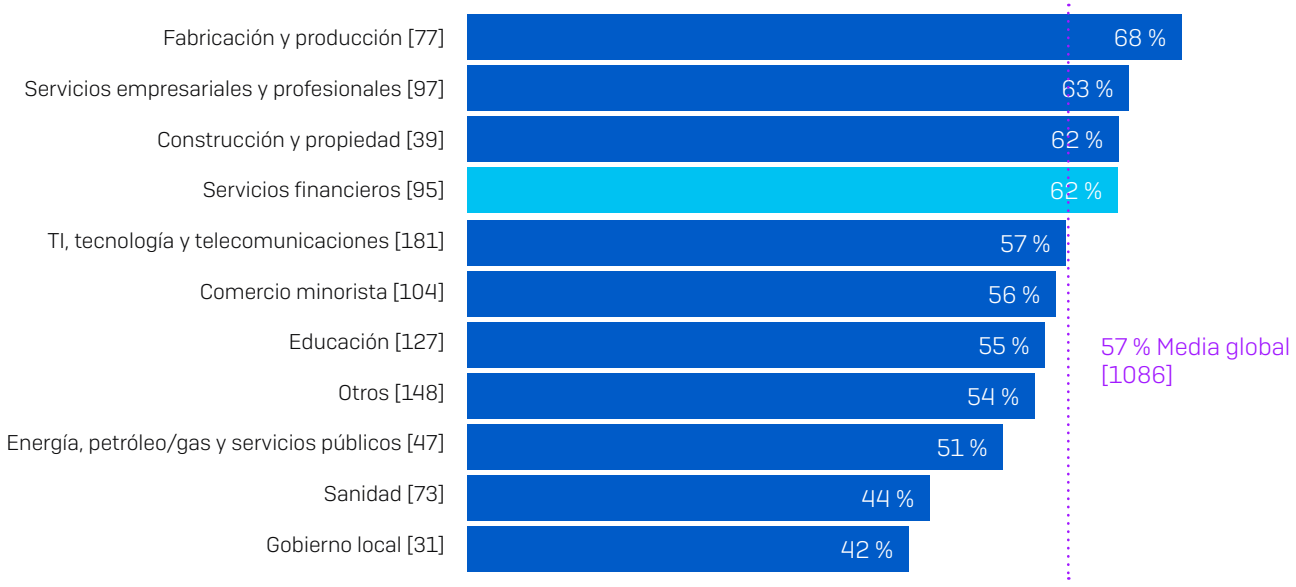
De todos los sectores, el de la **energía, petróleo/gas y servicios públicos** es el más predispuesto a pagar el rescate, ya que el 43 % accedió a la demanda de un rescate. Este sector suele tener mucha infraestructura heredada que no puede actualizarse fácilmente, de modo que las víctimas podrían sentirse obligadas a pagar el rescate a fin de permitir la continuidad de los servicios.

El **gobierno local** es el sector con el segundo nivel más alto de pagos de rescates (42 %). También es el sector con más probabilidades de que se cifren sus datos. Es muy posible que la predisposición de las entidades de gobiernos locales a pagar esté provocando que los delincuentes dirijan sus ataques más complejos y efectivos contra este colectivo.

Capacidad de restaurar datos usando copias de seguridad

Si comparamos esta sección con la anterior, la correlación entre la capacidad de restaurar datos a partir de copias de seguridad y la predisposición a pagar el rescate es muy evidente: los sectores con mayor capacidad de utilizar copias de seguridad también son menos propensos a pagar.

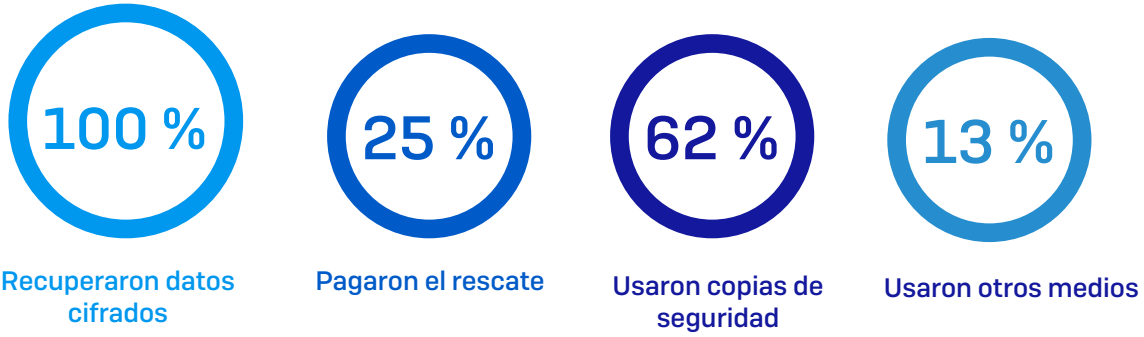
% que usaron copias de seguridad para restaurar datos cifrados



¿Su organización recuperó los datos en el ataque de ransomware más importante? Sí, usamos copias de seguridad para restaurar los datos [números base en el gráfico] organizaciones en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante, omitiendo algunas opciones de respuesta, divididas por sector

Los encuestados de servicios financieros (62 %) fueron de los más capaces para restaurar datos cifrados a partir de copias de seguridad. Es probable que esto se deba a que los bancos y muchas otras organizaciones de servicios financieros están obligados a tener planes de continuidad empresarial y de recuperación de desastres (BC-DR) a fin de evitar enormes pérdidas si se produce un desastre o una filtración de datos. No contar con un plan puede conllevar sanciones económicas y/o subidas en su cuota de la FDIC. Crear copias de seguridad y practicar la restauración de datos a partir de ellas será una parte integral de cualquier buen plan.

Todas las organizaciones de servicios financieros recuperaron sus datos cifrados

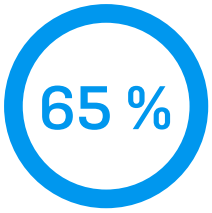


¿Su organización recuperó los datos en el ataque de ransomware más importante? [95] organizaciones de servicios financieros en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante.

La buena noticia para los servicios financieros es que es el único sector en que todas las organizaciones cuyos datos fueron cifrados pudieron recuperarlos. Como hemos visto, el 25 % pagó el rescate, el 62 % utilizó copias de seguridad y el 13 % se sirvió de otros medios para recuperar sus datos.

Pagar el rescate solo permite recuperar parte de los datos

Sin embargo, los que pagaron el rescate no recuperaron todos sus datos. Lo que los atacantes no mencionan al exigir un rescate es que, aunque pague, las probabilidades de que recupere todos sus datos son escasas.

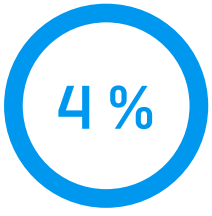


Porcentaje de datos restaurados después de pagar el rescate **MEDIA DE TODOS LOS SECTORES**

Porcentaje de datos restaurados después de pagar el rescate **MEDIA DE LOS SERVICIOS FINANCIEROS**

Cantidad media de datos que recuperaron las organizaciones en el ataque de ransomware más importante. [344/24] organizaciones que pagaron el rescate para recuperar sus datos

El número base de encuestados de servicios financieros no es suficientemente elevado como para sacar conclusiones sólidas. Sin embargo, a título anecdótico, los encuestados de servicios financieros afirmaron que recuperaron una media de solo el 63 % de sus datos después de pagar el rescate, con lo que más de un tercio quedaron inaccesibles. Esto es algo inferior a la media global (65 %). Es probable que no se trate de una maniobra deliberada por parte de los atacantes, sino de una indicación de que los adversarios dedican más tiempo y esfuerzo a desarrollar herramientas de cifrado potentes que quienes deben descifrarlos.



Recuperaron TODOS sus datos

Recuperaron la mitad o menos de sus datos

Cantidad de datos que recuperaron las organizaciones en el ataque de ransomware más importante. [24] organizaciones de servicios financieros que pagaron el rescate para recuperar sus datos

Para hacer más hincapié en este punto, solo un 4 % de las organizaciones de servicios financieros que pagaron el rescate recuperaron **todos** sus datos, y el 33 % recuperaron **la mitad o menos** de sus datos. Es evidente que pagar no compensa. De nuevo, el número base de los servicios financieros es algo bajo, de modo que solo puede considerarse orientativo.

El coste del ransomware

Revelamos los importes de los rescates pagados

De los 357 encuestados de todos los sectores que afirmaron que su organización había pagado el rescate, 282 también revelaron el importe exacto pagado.

170 404 USD

Importe de rescate GLOBAL medio

¿Cuál fue el importe del rescate que pagó su organización en el ataque de ransomware más importante? [282] Organizaciones que pagaron el rescate para recuperar sus datos

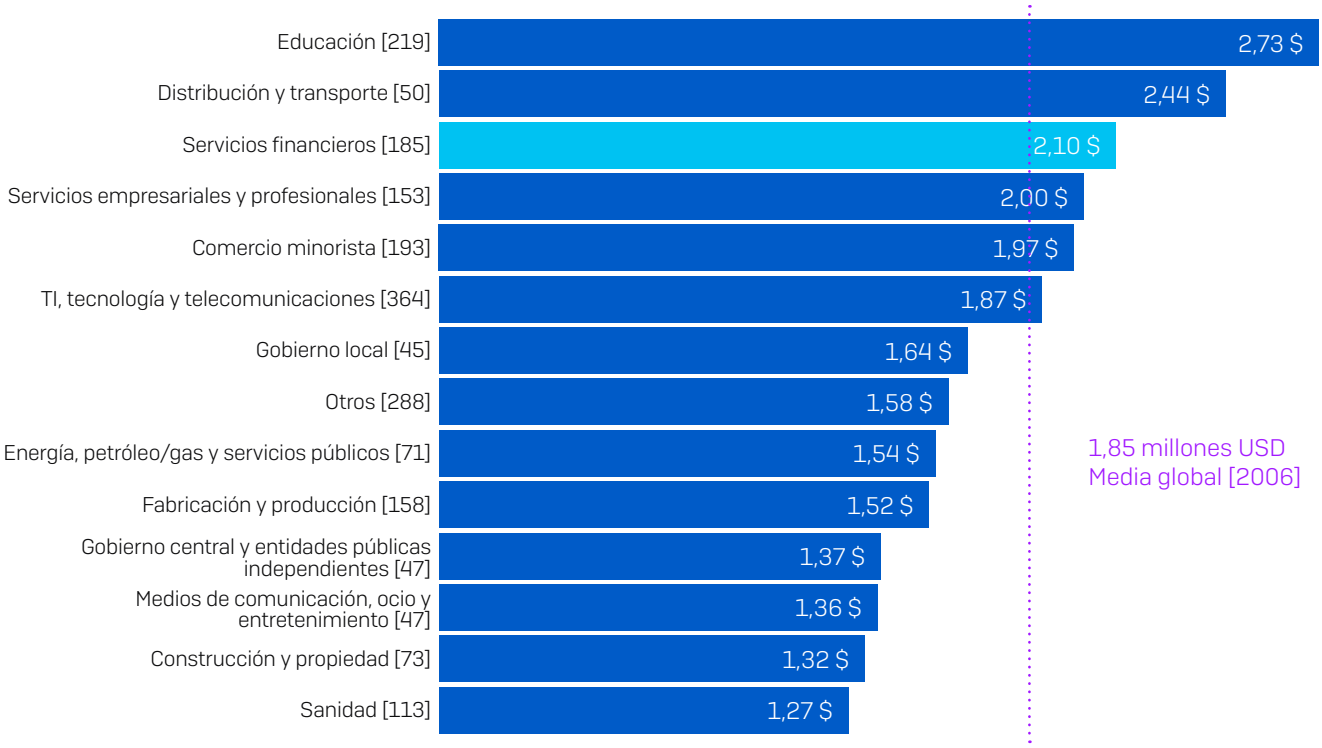
De forma global **en todos los sectores**, el importe de rescate medio fue de 170 404 USD. 13 encuestados de organizaciones de **servicios financieros** compartieron los importes de sus rescates: el pago de rescate medio fue de 69 369 USD, 100 000 USD por debajo de la media global. Este nivel de pagos tan bajo puede deberse, en parte, a la considerable capacidad de este sector de restaurar datos utilizando copias de seguridad. Asimismo, pagar un rescate puede exponer a las organizaciones de servicios financieros a un mayor riesgo legal y de cumplimiento, incluida la violación de leyes contra el blanqueo de capitales y la financiación del terrorismo.

Estas cifras divergen mucho de los pagos de ocho cifras en USD que suelen verse en los titulares por varias razones.

1. **Tamaño de la organización**. Nuestros encuestados pertenecen a organizaciones medianas de entre 100 y 5000 usuarios que, en general, tienen menos recursos financieros que las organizaciones de mayor tamaño. Los responsables del ransomware adaptan los rescates que exigen a la capacidad de pago de sus víctimas, por lo que normalmente aceptan importes menores de empresas más pequeñas. Los datos lo demuestran, ya que el rescate medio para organizaciones de 100 a 1000 empleados fue de 107 694 USD, mientras que el rescate medio pagado por las organizaciones de 1001 a 5000 empleados asciende a 225 588 USD.
2. **Tipo de ataque**. Hay muchos responsables del ransomware y muchos tipos de ataques de ransomware, desde atacantes altamente cualificados que utilizan tácticas, técnicas y procedimientos (TTP) sofisticados que se centran en objetivos individuales, hasta operadores menos habilidosos que utilizan ransomware "listo para usar" y un enfoque genérico de ataque "a ciegas". Los atacantes que realizan una gran inversión en un ataque dirigido exigen un elevado rescate que compense su esfuerzo, mientras que los responsables de ataques genéricos suelen aceptar un menor retorno de la inversión (ROI).
3. **Ubicación**. Como hemos visto al comienzo, esta encuesta cubre 30 países de todo el mundo, con distintos niveles de PIB. Los atacantes exigen los rescates más altos en economías occidentales desarrolladas, basándose en su percepción de que pueden pagar sumas mayores. Los dos importes de rescate más elevados fueron mencionados por encuestados de Italia. En cambio, en la India, el rescate medio fue de 76 619 USD, menos de la mitad de la cifra global (base: 86 encuestados).

Coste de recuperación del ransomware en los servicios financieros

El rescate es solo una pequeña parte del coste total de la recuperación de un ataque de ransomware. Las víctimas se enfrentan a una amplia variedad de gastos adicionales, como el coste de reconstruir y proteger sus sistemas de TI, costes de RR. PP. y análisis forenses.



Coste medio aproximado para las organizaciones de rectificar las consecuencias del ataque de ransomware más reciente (considerando el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.) [números base en el gráfico] encuestados cuya organización se ha visto afectada por el ransomware en el último año, divididas por sector

La encuesta reveló que el sector de los servicios financieros registra un coste medio de remediación del ransomware de 2,10 millones de USD (considerando el tiempo de inactividad, las horas perdidas, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, las sanciones legales y por incumplimiento, etc.), que es considerablemente superior a la media global de 1,85 millones USD.

Hay varios factores que podrían explicar esto. Primeramente, las organizaciones de servicios financieros guardan una gran cantidad de datos altamente confidenciales de personas, empresas y organizaciones públicas, de modo que incurren en altos costes de notificación de filtraciones de datos como parte de sus esfuerzos de remediación. En segundo lugar, la interrupción de las operaciones de las organizaciones de servicios financieros puede causar estragos a escala mundial. Esto ejerce una enorme presión sobre los negocios para volver a ponerse en marcha lo antes posible y a cualquier coste.

Además, los servicios financieros son uno de los sectores más regulados del mundo. Las organizaciones deben adherirse a un sinfín de normativas, como la ley SOX, el RGPD y el estándar PCI DSS, que comportan ingentes sanciones por incumplimiento. Las sanciones punitivas por filtraciones de datos incurridas como parte de un ataque de ransomware se añaden a los costes totales de recuperación.

Y, por último, como normalmente los clientes pueden cambiar de proveedor con facilidad, las organizaciones de servicios financieros están totalmente expuestas al impacto empresarial de los daños en su reputación, que conlleva la pérdida de clientes y la cancelación de cuentas.

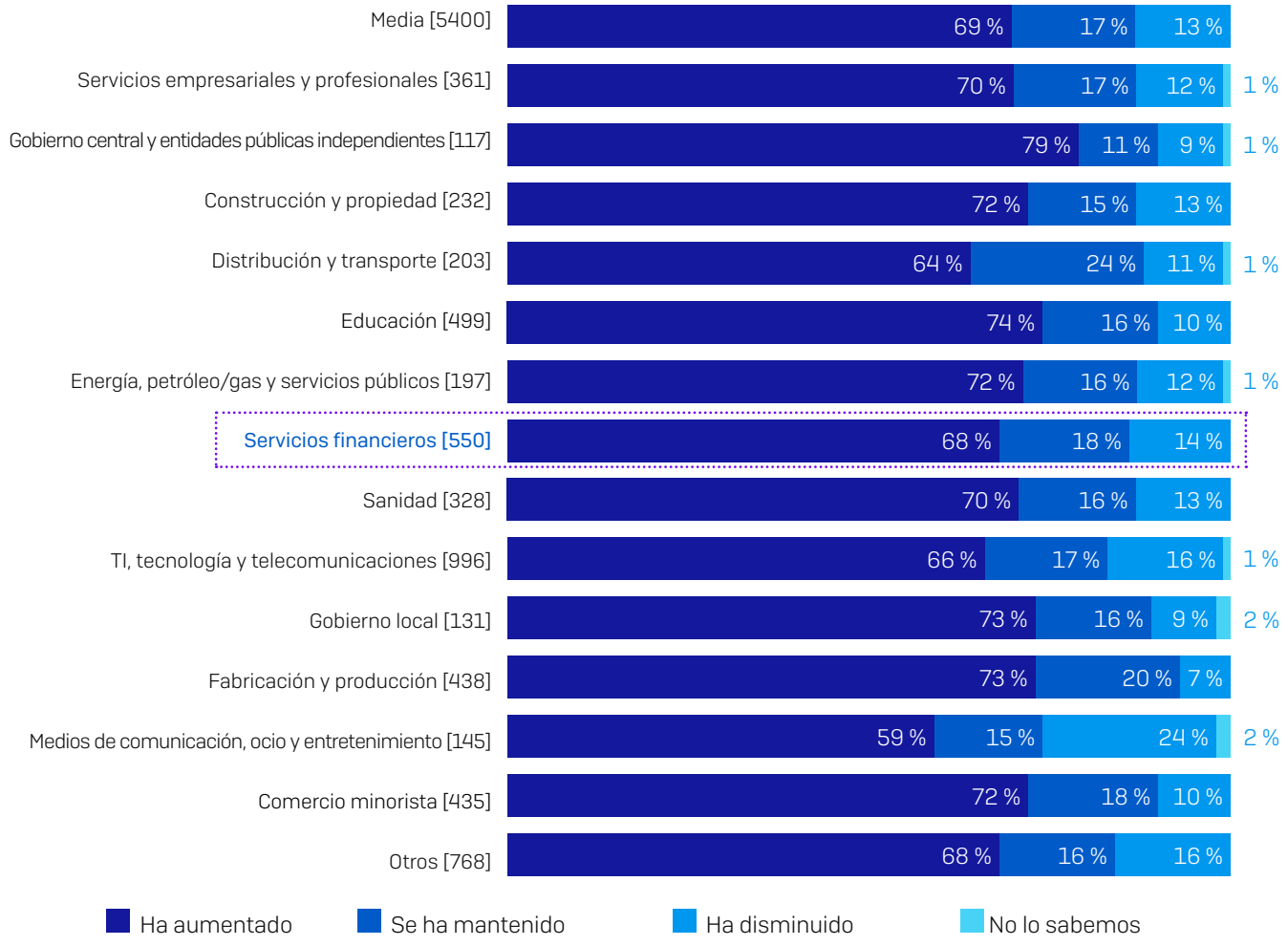
El ransomware es solo una parte del reto de la ciberseguridad

El ransomware es un importante problema de ciberseguridad para las organizaciones de servicios financieros, pero no es el único. Los equipos de TI hacen malabarismos para tratar de satisfacer múltiples demandas de ciberseguridad, y este reto se ha visto agravado por la pandemia.

La carga de trabajo en ciberseguridad ha aumentado en 2020

Los equipos de TI del sector de los servicios financieros se vieron muy afectados por la pandemia: el 68 % experimentaron un aumento de la carga de trabajo de ciberseguridad durante el transcurso de 2020. La mayoría de los encuestados de todos los sectores registraron un incremento, pero el sector del gobierno central tuvo el mayor crecimiento de la carga de trabajo.

Cómo ha cambiado la carga de trabajo en ciberseguridad durante 2020



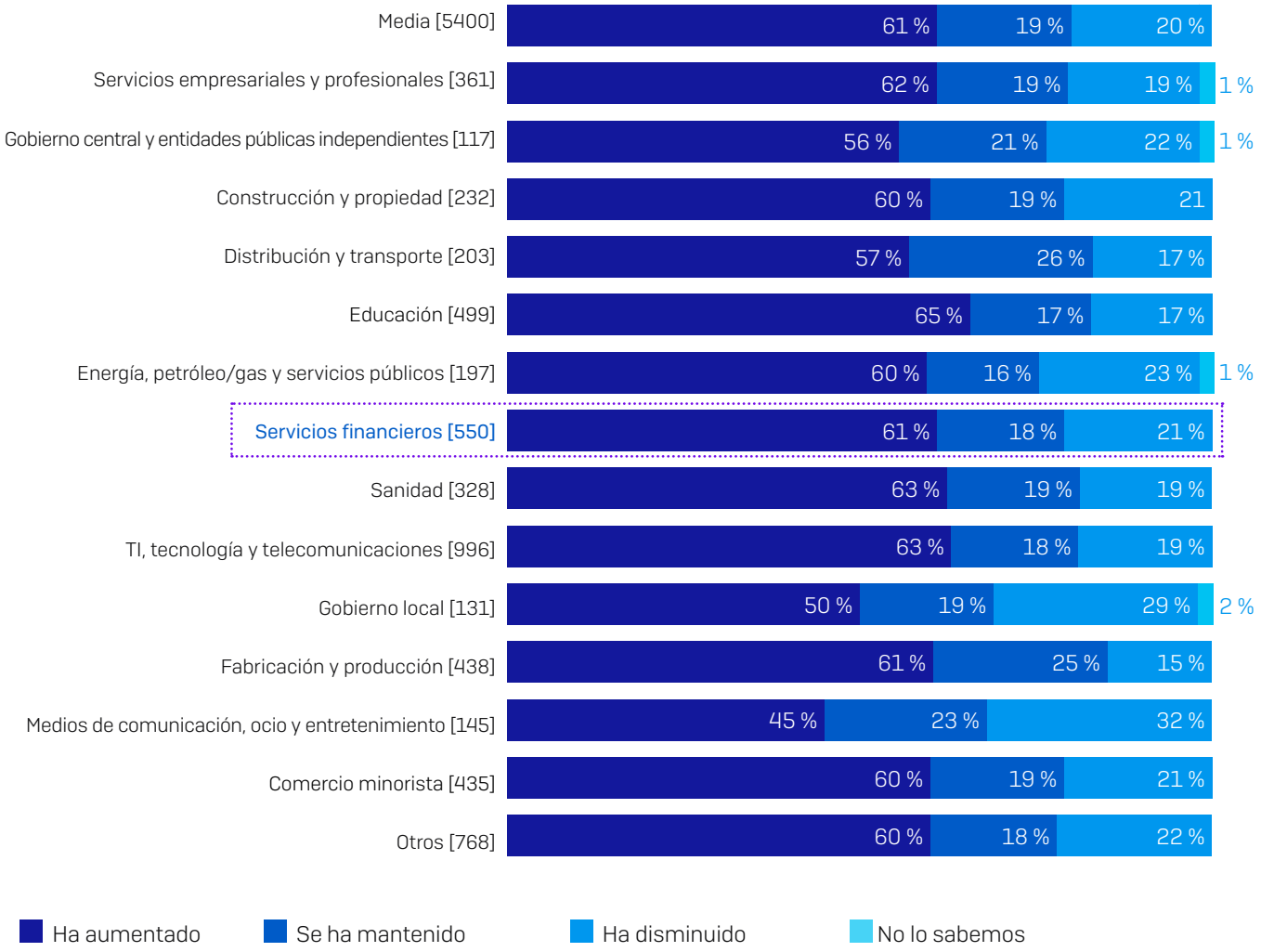
Durante 2020, nuestra carga de trabajo en ciberseguridad ha disminuido/aumentado/se ha mantenido igual [números base en el gráfico], dividida por sector

El rápido traslado al teletrabajo y la necesidad de desplegar servicios y soluciones adicionales para los empleados y los clientes a fin de mantener la actividad fue probablemente un factor decisivo tras el incremento de la carga de trabajo de los equipos de TI. El hecho de tener que centrarse sobre todo en la protección de las nuevas plataformas online seguramente redujo la capacidad de los equipos de TI para supervisar las amenazas de ransomware y responder a ellas.

El incremento de la carga de trabajo ralentizó los tiempos de respuesta

Una de las consecuencias del aumento de la carga de trabajo de ciberseguridad durante 2020 fue la ralentización del tiempo de respuesta a los casos de TI. El sector de los servicios financieros se vio considerablemente afectado, ya que el 61 % de los encuestados afirmaron que el tiempo de respuesta había aumentado en el último año.

Cambios en el tiempo de respuesta a los casos de TI durante 2020



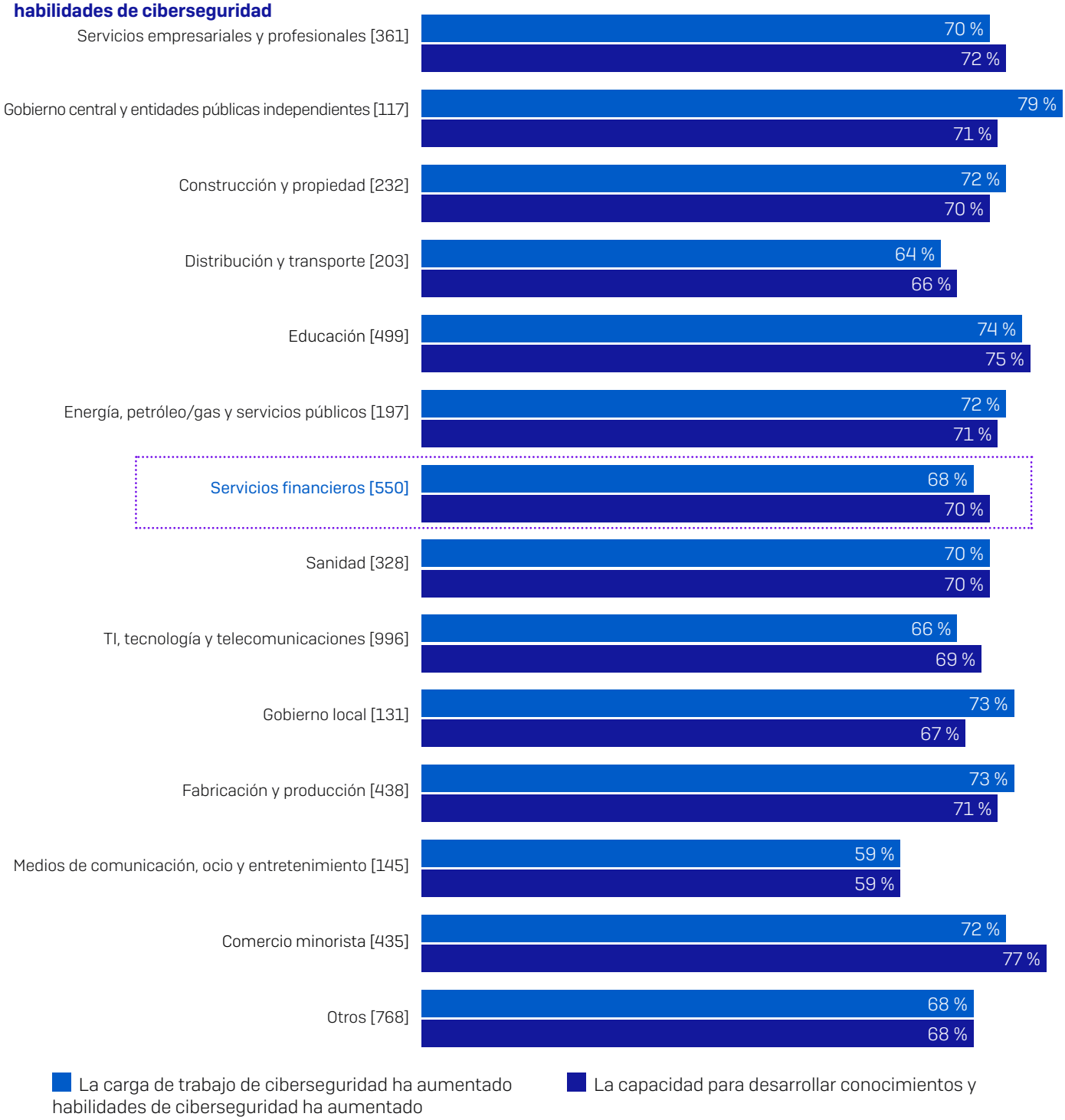
Durante 2020, nuestro tiempo de respuesta a los casos de TI ha disminuido/aumentado/se ha mantenido igual. [números base en el gráfico], dividido por sector

Cuando un adversario se encuentra en su entorno, es imperativo detenerlo lo antes posible. Cuanto más tiempo se le permita explorar su red y acceder a sus datos, mayor será el impacto financiero y operativo del ataque. La ralentización del tiempo de respuesta es por lo tanto un motivo de alarma.

El aumento de la carga de trabajo incrementó conocimientos y habilidades

No hay mal que por bien no venga. También existe una clara correlación entre el aumento de la carga de trabajo en ciberseguridad y el aumento de la capacidad para desarrollar conocimientos y aptitudes en ciberseguridad.

Aumento de la carga de trabajo en ciberseguridad y aumento de la capacidad para desarrollar conocimientos y habilidades de ciberseguridad



Durante 2020, ha aumentado nuestra carga de trabajo de ciberseguridad/nuestra capacidad para desarrollar más nuestros conocimientos y habilidades de ciberseguridad [números base en el gráfico], dividido por sector

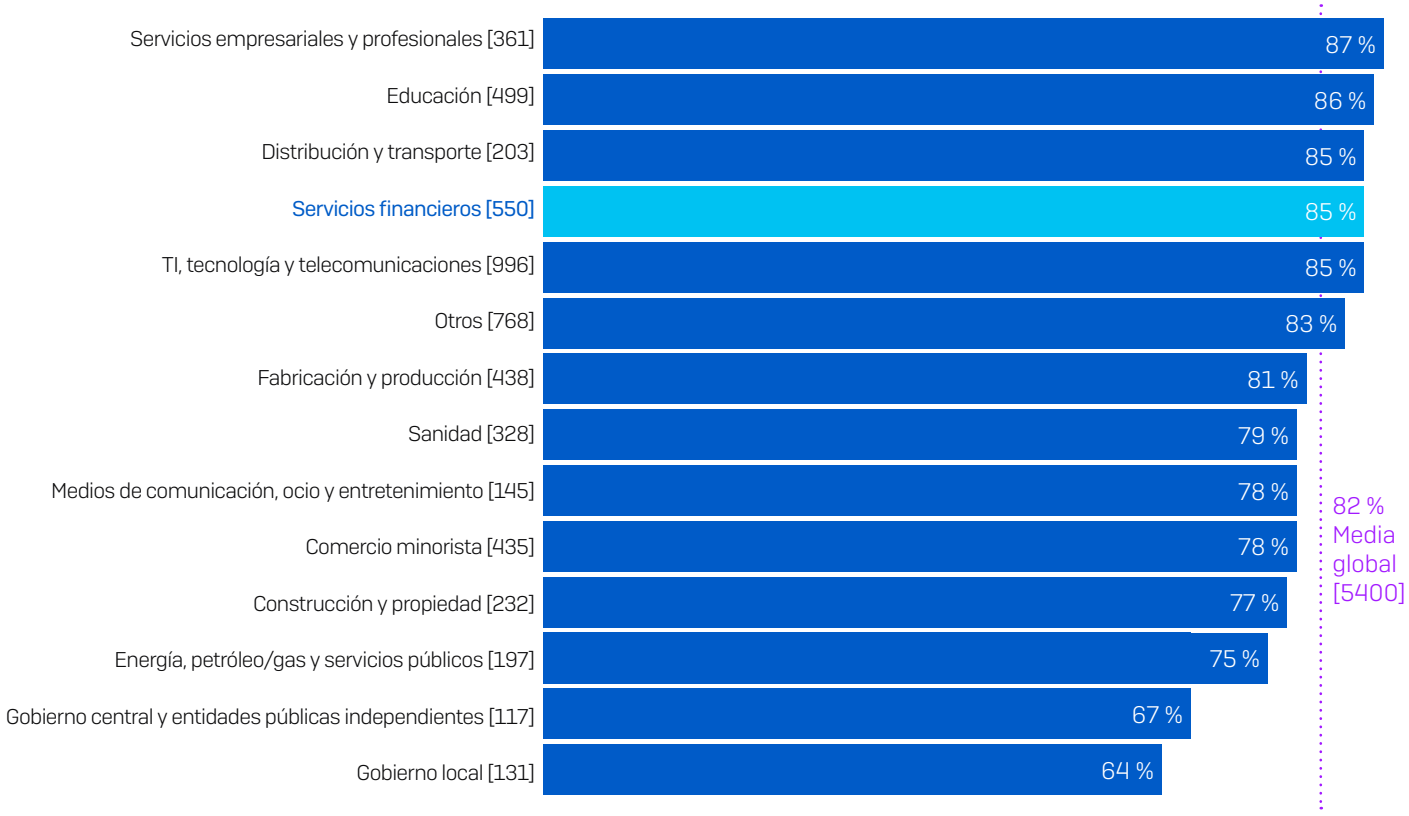
El 70 % de los equipos de TI de los servicios financieros afirmaron que su capacidad para desarrollar conocimientos y habilidades de ciberseguridad se vio incrementada durante el transcurso de 2020.

Si bien una mayor carga de trabajo añade presión, también ofrece más oportunidades para aprender cosas nuevas. Es probable que las circunstancias únicas de la pandemia obligaran a los equipos de TI a ofrecer un rendimiento que nunca antes se les había requerido.

Nivel de preparación para asumir futuros retos

El 85 % de los encuestados de los servicios financieros coinciden en que, si detectan actividades sospechosas en su organización, tienen las herramientas y los conocimientos necesarios para investigar a fondo, que es más que la media global (82 %). Esto es una gran noticia para este sector dado el incremento en la carga de trabajo de ciberseguridad que ha experimentado. Tener las herramientas y los conocimientos adecuados es clave para poder investigar y remediar las ciberamenazas.

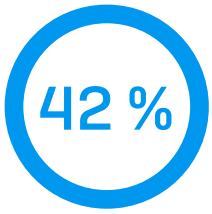
Tienen las herramientas y los conocimientos necesarios para investigar la actividad sospechosa



Si detecto actividades sospechosas en mi organización, tengo las herramientas y los conocimientos que necesito para investigar a fondo: Muy de acuerdo, De acuerdo. Omitiendo algunas opciones de respuesta [números base en el gráfico], divididas por sector

El futuro

Expectativas de los servicios financieros frente a futuros ataques



Esperan ataques de ransomware en el futuro

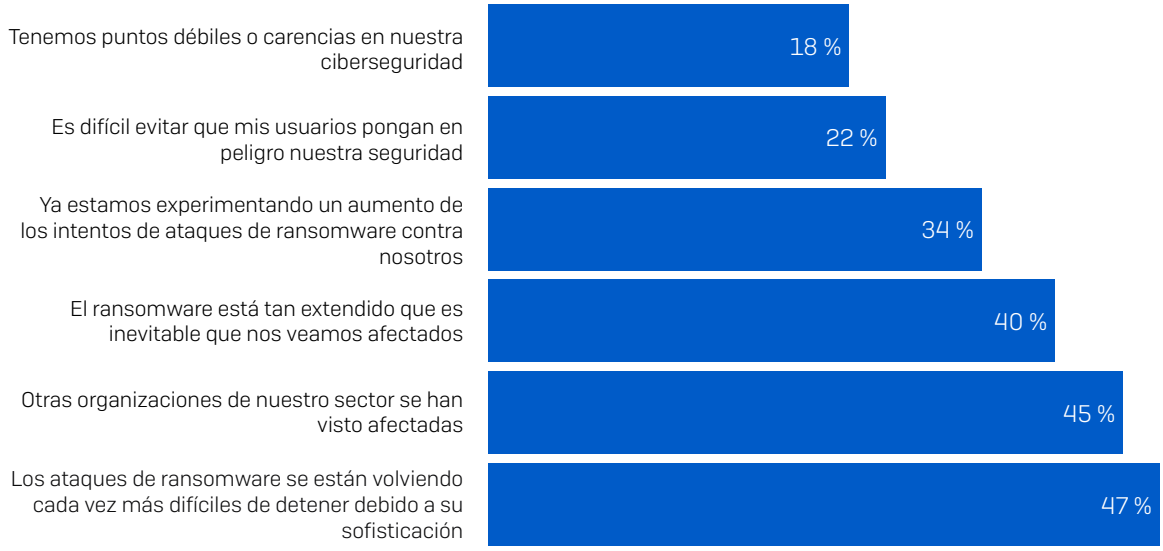
No esperan ataques de ransomware en el futuro

[550] Encuestados de servicios financieros que contestaron "No" a la pregunta "En el último año, ¿se ha visto afectada por el ransomware su empresa?"

Anteriormente en este informe, hemos visto que el 63 % de los encuestados del sector de los servicios financieros no se vieron afectados por el ransomware en el último año. El 42 % esperan sufrir ataques de ransomware en el futuro. En cambio, el 22 % no prevén ningún ataque.

Por qué prevé ataques el sector de los servicios financieros

Entre las organizaciones de servicios financieros que no fueron víctimas del ransomware pero que esperan serlo en el futuro, la razón más común (47 %) es que los ataques de ransomware se están volviendo cada vez más difíciles de detener debido a su sofisticación. Aunque este número es elevado, el hecho de que estas organizaciones estén alerta ante la posibilidad de que el ransomware se vuelva más avanzado es algo positivo, y es probable que sea un factor que ha contribuido a que hayan conseguido bloquear cualquier posible ataque de ransomware durante el último año.



¿Por qué espera que su organización sea atacada por el ransomware en el futuro? [229 organizaciones de servicios financieros que no han sido atacadas por el ransomware en el último año pero que esperan serlo en el futuro, omitiendo algunas opciones de respuesta]

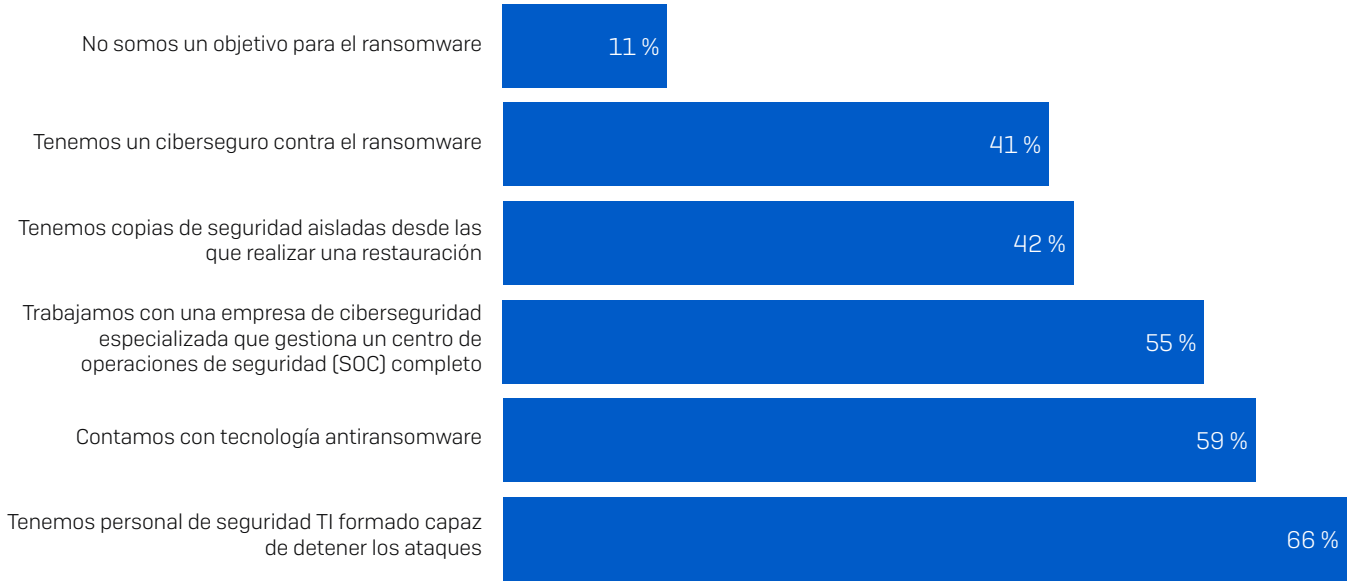
Además, el 45 % de los encuestados afirmaron que otras organizaciones de su sector han sido víctimas, lo que aumenta sus probabilidades de sufrir ataques.

El 22 % de los encuestados ven el hecho de que los usuarios comprometan la seguridad como uno de los principales factores para sufrir un ataque de ransomware en el futuro. Resulta alentador observar que, frente a los atacantes sofisticados, la mayoría de los equipos de TI no eligen la opción fácil de culpar a sus usuarios.

De forma similar, el 18 % de encuestados de servicios financieros admiten tener puntos débiles o carencias en su ciberseguridad. Aunque lógicamente no es nada bueno tener carencias de seguridad, reconocer que estos problemas existen es un importante primer paso para mejorar las defensas.

Por qué el sector de los servicios financieros no prevé ataques de ransomware

119 encuestados de servicios financieros dijeron que su organización no había sufrido ataques de ransomware en el último año y que no esperan sufrir ninguno en el futuro.



¿Por qué no espera que su organización sea atacada por el ransomware en el futuro? [119] entidades de servicios financieros que no han sido atacadas por el ransomware en el último año y no esperan serlo en el futuro, omitiendo algunas opciones de respuesta

La razón número uno de esta confianza es que han formado a personal de TI para que sea capaz de detener los ataques

(66 %), seguida del uso de tecnología antiransomware (59 %). Si bien las tecnologías avanzadas y automatizadas son elementos fundamentales de una defensa antiransomware efectiva, detener los ataques manuales también requiere una monitorización e intervención humanas por parte de profesionales cualificados. Ya sean empleados en plantilla o profesionales subcontratados, solo los expertos humanos pueden identificar algunos de los indicios de que los atacantes del ransomware le tienen en el punto de mira. Recomendamos encarecidamente a todas las organizaciones que refuercen sus conocimientos humanos ante la amenaza continuada del ransomware.

El 55 % de encuestados de servicios financieros que no esperan ser atacados por el ransomware trabajan con una empresa de ciberseguridad especializada que gestiona un centro de operaciones de seguridad (SOC) completo. Resulta alentador observar que las organizaciones están subcontratando servicios de ciberseguridad en caso necesario, lo que amplía su protección.

No todo son buenas noticias. Algunos resultados son preocupantes:

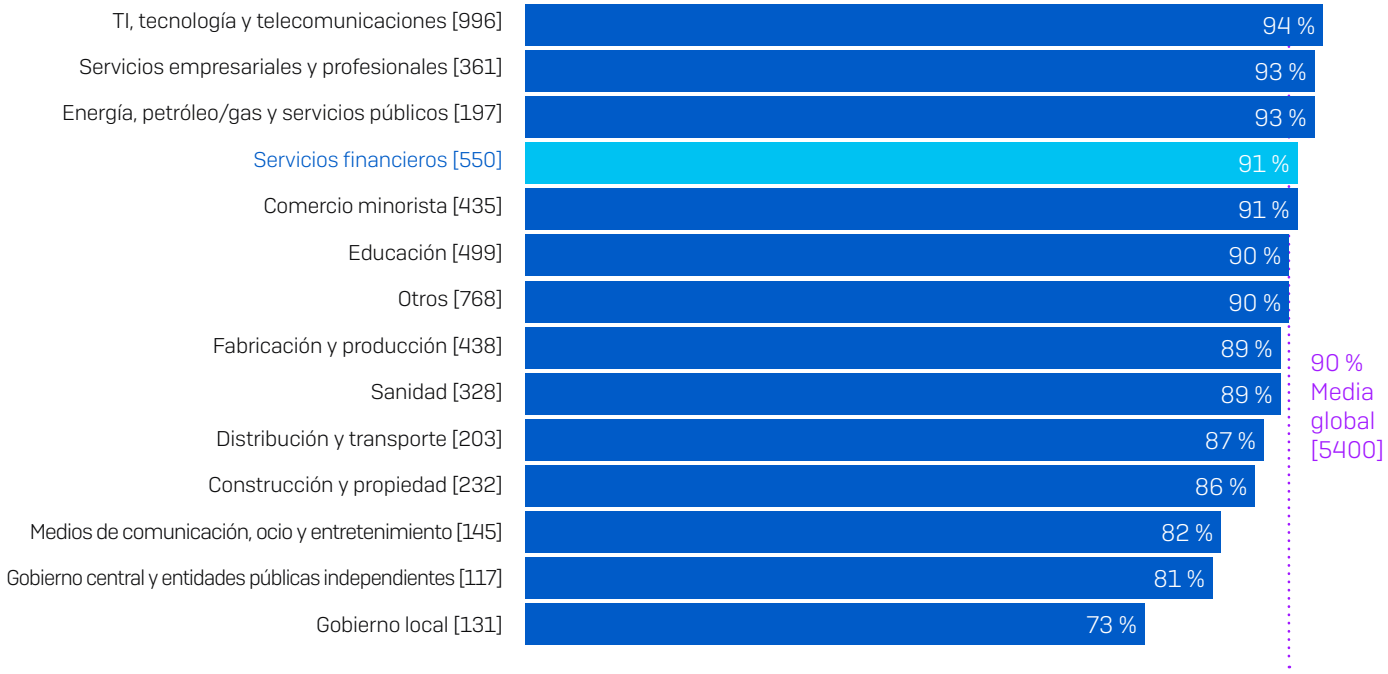
- El 61 % de los encuestados de servicios financieros que no esperan sufrir ningún ataque depositan su confianza en enfoques que no ofrecen ninguna protección contra el ransomware.
  - El 41 % citaron un ciberseguro contra el ransomware. Los seguros ayudan a cubrir el coste de lidiar con un ataque, pero no evitan que el ataque se produzca.
  - El 42 % citaron copias de seguridad aisladas. Aunque las copias de seguridad son herramientas valiosas para restaurar los datos después de un ataque, no evitan el ataque en sí.

  N. B. Algunos encuestados seleccionaron las dos opciones anteriores, y el 61 % seleccionaron al menos una de estas dos opciones.
- El 11 % creen que no son un objetivo para el ransomware. Lamentablemente, esto no es así. Ninguna organización está a salvo.

Las organizaciones de servicios financieros están bien preparadas

Responder a un ciberataque o incidente crítico puede ser increíblemente estresante. Aunque nada puede aliviar por completo el estrés que supone lidiar con un ataque, contar con un plan de respuesta a incidentes efectivo es una forma segura de minimizar el impacto.

% que tiene un plan para recuperarse de un incidente de malware importante



¿El plan de continuidad empresarial (BCP) o plan de recuperación de desastres (DRP) de su organización incluye planes para recuperarse de un incidente de malware importante? Sí, tenemos un plan de recuperación de incidentes de malware completo y detallado, y Sí, tenemos un plan de recuperación de incidentes de malware parcialmente desarrollado; [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

Por esta razón, resulta alentador descubrir que el 91 % de los encuestados de servicios financieros cuentan con un plan de recuperación de incidentes de malware: un poco más de la mitad (51 %) tienen un plan completo y detallado, mientras que el 40 % tienen un plan parcialmente desarrollado. Estas estadísticas están en la línea de las cifras medias de todos los sectores (90 %).

Recomendaciones

En vista de los resultados de la encuesta, los expertos de Sophos recomiendan las siguientes prácticas para las organizaciones de todos los sectores:

1. **Dé por hecho que sufrirá un ataque**. El ransomware sigue estando muy extendido. No hay ningún sector, país ni organización a salvo del riesgo. Es mejor prepararse y no sufrir ningún ataque que lo contrario.
2. **Realice copias de seguridad.** Las copias de seguridad son el principal método utilizado por las organizaciones para recuperar sus datos tras un ataque. Y como ya hemos visto, incluso si paga el rescate, rara vez conseguirá recuperar todos sus datos, así que depende de las copias de seguridad en cualquiera de los casos.

   Una sencilla regla mnemotécnica para las copias de seguridad es "3-2-1". Debería tener al menos **tres** copias distintas (la que esté usando en el momento actual, más dos o más aparte), utilizar al menos **dos** sistemas de copia de seguridad diferentes (por si uno le falla) y tener al menos **una** copia almacenada sin conexión y preferiblemente en una ubicación externa (donde los delincuentes no puedan manipularla durante un ataque).
3. **Despliegue una protección por capas**. Ante el importante aumento de los ataques basados en la extorsión, es más importante que nunca mantener a los adversarios fuera de su entorno como primera medida. Utilice una protección por capas para bloquear a los atacantes en tantos puntos como sea posible dentro de su entorno.
4. **Combine expertos humanos y tecnología antiransomware**. La clave para detener el ransomware es una defensa exhaustiva que combine una tecnología antiransomware dedicada y la búsqueda de amenazas realizada por humanos. La tecnología le brinda el alcance y la automatización que necesita, mientras que los expertos humanos están más capacitados para detectar las tácticas, técnicas y procedimientos que indican que un atacante habilidoso está intentando infiltrarse en su entorno. Si no dispone de las capacidades en plantilla, plantéese la opción de contratar a una empresa especializada en ciberseguridad para que le ayude. Ahora los SOC son opciones realistas para las organizaciones de todos los tamaños.
5. **No pague el rescate**. Sabemos que esto es fácil de decir pero mucho menos fácil de hacer cuando la actividad de su organización se encuentra interrumpida a causa de un ataque de ransomware. Con independencia de cualquier consideración ética, pagar el rescate no es una forma efectiva de recuperar sus datos. Si opta por pagar, asegúrese de incluir en su análisis de costes y beneficios la expectativa de que los adversarios restaurarán, de media, solo dos terceras partes de sus archivos.
6. **Tenga un plan de recuperación del malware**. La mejor manera de evitar que un ciberataque acabe en una infracción de seguridad es prepararse con antelación. Las organizaciones que sufren un ataque a menudo se dan cuenta de que podrían haber evitado muchos costes, molestias e interrupciones si hubieran contado con un plan de respuesta a incidentes.

Más recursos

La Guía de respuesta a incidentes de Sophos ayuda a las organizaciones a definir el marco de su plan de respuesta a incidentes de ciberseguridad y explica los 10 principales pasos que debe incluir su plan.

A los responsables de la seguridad también puede interesarles consultar el artículo Cuatro consejos clave de los expertos en respuesta a incidentes, que pone de relieve las principales lecciones que todo el mundo debería aprender en lo que respecta a responder a incidentes de seguridad.

Ambos recursos se basan en experiencias del mundo real de los equipos de Sophos Managed Threat Response y Sophos Rapid Response, que han respondido de forma conjunta a miles de incidentes de ciberseguridad.

Obtenga más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su organización.

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 empresa estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

1-09-2021 (SB-ES)

SOPHOS