

El estado del ransomware en México 2022

Resultados de una encuesta independiente y desvinculada de cualquier proveedor a 200 profesionales de TI de organizaciones de tamaño mediano de México.

Acerca de la encuesta

Sophos encargó a la empresa de investigación especializada Vanson Bourne la realización de una encuesta independiente y desvinculada de cualquier proveedor a 5600 profesionales de TI en organizaciones de tamaño mediano (100-5000 empleados) de 31 países, entre ellos 200 en México. La encuesta se realizó durante enero y febrero de 2022 y a los encuestados se les pidió contestar según sus experiencias del año anterior.

Principales conclusiones

- ▶ **El 74 % de las organizaciones mexicanas se vieron afectadas por el ransomware en el último año**, una cifra que triplica la proporción registrada en 2020, que fue del 25 %. A nivel mundial, en comparación, el 66 % de los encuestados sufrieron un ataque de ransomware en 2021.
- ▶ **El 57% de los ataques comportaron el cifrado de datos**. Esta cifra es ligeramente inferior a la media mundial del 65 %, y supone un aumento considerable con respecto al 22 % registrado por los encuestados en México en 2020.
- ▶ **El 100 % de los encuestados mexicanos cuyos datos fueron cifrados recuperaron parte de los datos**. Esto concuerda con los resultados globales de la encuesta, ya que el 99 % afirmaron haber recuperado al menos parte de sus datos.
- ▶ **Las copias de seguridad fueron el principal método utilizado para restaurar los datos**, usado por el 79 % de los encuestados en México cuyos datos fueron cifrados. El 44 % pagó el rescate. Está claro que el uso de varios métodos de recuperación en paralelo es ya habitual. Por su parte, a nivel mundial, el 73 % de los encuestados utilizaron copias de seguridad y el 46 % pagaron el rescate para restaurar los datos.
- ▶ **Las organizaciones mexicanas que pagaron el rescate recuperaron, de media, el 58 % de sus datos**. A nivel global, las organizaciones que pagaron el rescate restauraron el 61 % de los datos cifrados, un ligero descenso respecto a la cifra de 2020, que fue del 65 %.
- ▶ 37 encuestados de México que pagaron el rescate compartieron la cantidad desembolsada, **siendo el pago medio de 482 446 USD**. El 16% pagó menos de 10 000 USD, mientras que el 16% pagó 1 millón USD o más. A nivel mundial, el importe de rescate medio fue de 812 360 USD, y la proporción de víctimas que pagaron 1 millón USD o más se multiplicó casi por tres (pasó del 4 % en 2020 al 11 % en 2021).
- ▶ **La factura media mexicana para recuperarse de un ataque de ransomware en 2021 fue de 0,88 millones USD**. Esto supone un descenso considerable con respecto a los 2,03 millones USD registrados en 2020.
- ▶ **El 88 % de los encuestados en México dijeron que el ataque de ransomware afectó a su capacidad operativa**. Esto sigue la línea de la cifra mundial del 90 %.
- ▶ **El 79% afirmó que el ataque de ransomware causó pérdidas de negocio/ingresos a su organización**. De nuevo, esto sigue la línea de la cifra mundial del 86 %.
- ▶ **Las organizaciones mexicanas tardaron una media de un mes en recuperarse del ataque**.
- ▶ **El 85 % de los encuestados en México señalaron que su organización tiene un ciberseguro que les cubre en caso de verse afectados por el ransomware**. A nivel mundial, esta proporción es del 83 %.
- ▶ **El 95 % afirmó que le resultó más difícil contratar un ciberseguro en el último año**. El 59 % señaló que el nivel de ciberseguridad necesario para optar a un seguro ha aumentado; el 53 % afirmó que las ciberpólizas se han vuelto más complejas; el 29 % manifestó que el proceso es más largo, y el 32 % aseguró que es más caro. Dado que la subidas de precio más importantes de los ciberseguros se produjeron durante el segundo y el tercer trimestre de 2021, es probable que muchas organizaciones experimenten un aumento de precios considerable cuando renueven sus pólizas.

- ▶ **El 99 % de las organizaciones mexicanas ha realizado cambios en sus ciberdefensas durante el último año para mejorar su posición frente a las ciberseguradoras.** A nivel global, el 97 % realizó cambios; en concreto, el 64 % implementó nuevos servicios/tecnologías, el 56 % aumentó las actividades de formación y concienciación del personal, y el 52 % cambió sus procesos y comportamientos.
- ▶ **El ciberseguro pagó el 100 % de las reclamaciones por ransomware en México.** De las organizaciones afectadas por el ransomware y que contaban con un ciberseguro que lo cubría, el 69 % afirmaron que el seguro pagó los costes para recuperar su actividad, el 40 % señalaron que pagó el rescate, y el 29 % dijeron que pagó otros costes.

Conclusión

El desafío que el ransomware representa para las organizaciones mexicanas no deja de crecer. Optimizar la ciberseguridad es imperativo para todas las organizaciones. Nuestros cinco consejos más importantes son:

- ▶ Garantice que las defensas en todos los puntos de su entorno sean de alta calidad. Revise los controles de seguridad y asegúrese de que siguen siendo válidos para sus necesidades.
- ▶ Busque las amenazas de forma proactiva con el fin de detener a los atacantes antes de que puedan ejecutar su ataque. Recorra a un especialista en MDR externo si no dispone del tiempo ni de los conocimientos necesarios.
- ▶ Refuerce su entorno buscando y cerrando las brechas de seguridad: dispositivos sin parchear, equipos sin proteger, puertos RDP abiertos, etc. La detección y respuesta ampliadas (XDR) es ideal en este sentido.
- ▶ Prepárese para lo peor. Sepa qué hacer en caso de un ciberincidente y con quién tiene que contactar.
- ▶ Haga copias de seguridad y practique la restauración de datos a partir de ellas. Su objetivo es recuperar su actividad lo más rápido posible con interrupciones mínimas.

Más información

Lea el informe [El estado del ransomware 2022](#) para conocer los resultados completos a nivel global y los datos por sector.

Consulte el [Centro de información sobre amenazas de ransomware de Sophos](#) para obtener información detallada sobre distintos grupos de ransomware.

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 funciones next-gen probadas, los datos de su empresa estarán protegidos de forma eficaz por productos basados en la IA y el Machine Learning.