66% de las empresas del mundo fueron víctimas de ransomware; en Latinoamérica es de hasta el 74%

- *En México el 74% de la totalidad de firmas encuestadas admitieron haber sido víctimas, un incremento notable desde el 25% registrado en 2020.*

- *El 46% de las empresas a las que los atacantes lograron encriptar la información, pagaron un rescate.*

11 de mayo de 2022.- Sophos, la compañía líder en ciberseguridad de última generación, publicó hoy su reporte anual 'The State of Ransomware 2022' que revela que el 66% de las compañías a nivel global fueron víctimas de ransomware en 2021, cifra considerablemente mayor al 37% reportado en 2020.

El informe destaca además que las empresas de Latinoamérica incluso rebasan el promedio. Destaca el caso de México, en donde el 74% admiten haber sido vulneradas en el año. El 17%, además, indican que si bien no han sido vulneradas previamente, esperan serlo en el 2022.

En el caso de Colombia, el porcentaje de víctimas es de 63% mientras que destaca un 18% que esperan ser atacadas en el futuro. En el caso de Chile, el 63% de las firmas ya han sido afectadas por cibercriminales, mientras que el 26% espera serlo este año.

El reporte global revela que las empresas que tenían datos encintados por ciberdelincuentes pagaron un rescate promedio de USD $812,360, cifra casi cinco veces mayor a la reportada el año previo.

Indica también que el 46% de las organizaciones que tenían datos encriptados pagaron el rescate para recuperar sus datos, incluso si tenían otros medios de recuperación, tales como copias de seguridad.

En el caso de Latinoamérica, destacan los porcentajes de empresas que lograron recuperar la información robada tras el ataque. En el caso de Colombia, el 65% de las compañías vulneradas recuperaron su información mediante copias de seguridad, cifra que en el caso de Chile es del 77% y en México del 79%.

El informe resume el impacto del ransomware en 5600 organizaciones medianas en 31 países de Europa, América, Asia-Pacífico y Asia Central, Oriente Medio y África.

"Además de los crecientes montos que pagan las empresas a cibercriminales que les acechan con ransomware, el estudio de Sophos muestra que la proporción de empresas que pagan ese tipo de 'rescates' también está aumentando de forma notable incluso cuando pueden tener otras opciones disponibles", dijo Chester Wisniewski, científico investigador principal de Sophos.

"Podría haber varias razones para ello, incluidas las copias de seguridad incompletas o el deseo de evitar que los datos robados aparezcan públicamente. Después de un ataque de ransomware, a menudo hay una gran presión para volver a funcionar lo antes posible. La restauración de datos cifrados mediante copias de seguridad puede ser un proceso difícil y lento, por lo que puede ser tentador pensar que pagar un rescate por una clave de descifrado es una opción más rápida", añade.

El especialista indica que el pago de un rescate también implica demasiados riesgos. Las organizaciones no saben qué podrían haber hecho los atacantes, como agregar puertas traseras, copiar contraseñas y más.

"Si las organizaciones no limpian a fondo los datos recuperados, terminarán con todo ese material 'contaminado' en su red y posiblemente expuestos a un nuevo ataque", destaca.

Entre los principales resultados del reporte destacan:

- **Los pagos de rescate crecen notablemente.** En 2021, el 11% de las organizaciones admitieron que pagaron hasta USD $1 millón por un rescate de datos encriptados, mucho más que el 4% de 2020. Del mismo modo, el porcentaje de empresas que pagaron menos de USD $10,000 cayó a 21%, desde el 34% del año previo.

- **¿Cuánto cuesta ser víctima de ransomware?** Más allá del monto pagado en un 'rescate', las afectaciones totales por ser vulnerado en 2021 fueron de alrededor de USD $1.4 millones. Además, toma cerca de un mes recuperarse por completo del daño, tanto económico como en reputación.

- **Confianza.** El 83% de las empresas medianas tienen un seguro contra ciberataques y confían en este. Indican que en el 98% de los incidentes su seguro habría cubierto una parte o la totalidad de los costos.

Recursos adicionales:

- Para ver la encuesta sobre ransomware del año pasado, consulte el Estado del ransomware 2021
- Para obtener detalles de la investigación de Sophos sobre una amplia gama de grupos de ransomware individuales, consulte el Centro de Inteligencia de Amenazas de Ransomware de Sophos
- Los productos terminales de Sophos, como Intercept X, protegen a los usuarios detectando las acciones y comportamientos de los atacantes
- Más detalles sobre la evolución del panorama de las ciberamenazas en el Informe de Amenazas de Sophos 2022

- Tácticas, técnicas y procedimientos (TTPs) y más para diferentes tipos de amenazas están disponibles en SophosLabs Uncut, que proporciona la última inteligencia de amenazas de Sophos
- La información sobre el comportamiento de los atacantes, los informes de incidentes y los consejos para los profesionales de las operaciones de seguridad están disponibles en Sophos News SecOps
- Conozca más sobre el Servicio de Respuesta Rápida de Sophos que contiene, neutraliza e investiga los ataques 24/7
- Los cuatro consejos principales para responder a un incidente de seguridad de Sophos Rapid Response y el equipo de respuesta a amenazas gestionadas
- Lea las últimas noticias y opiniones sobre seguridad en el sitio web de noticias galardonado de Sophos Naked Security, y en Sophos News

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/