Manufactureras: las menos propensas a pagar por un rescate de datos por ransomware

- *Apenas el 19% de las empresas del sector pagaron por el rescate de la información robada, menor al promedio global de 32% en el resto de las industrias.*

CIUDAD DE MÉXICO. 22 de noviembre de 2021.- Sophos, líder mundial en ciberseguridad de última generación, publicó el Estado del ransomware en la manufactura y producción 2021, que revela que las empresas de este sector son las menos propensas **(con un 19%)** a pagar por el rescate de los archivos cifrados.

Además, el informe señala que las manufactureras fueron, durante 2020, las que más **éxito tuvieron (68%) al restaurar los datos de las copias de seguridad** de los archivos vulnerados.

La práctica de realizar copias de seguridad podría ser una razón por la que este sector también fue el más afectado por los ataques de ransomware basados en extorsión, una técnica de presión en la que los atacantes no cifran los archivos, sino que amenazan con filtrar información robada en línea si no se paga el rescate.

El reporte mide el alcance y el impacto de los ataques de ransomware durante 2020 y los hallazgos para el sector de fabricación y producción indican:

- El 36% de las empresas del sector se vieron afectadas por ransomware en 2020
- El 9% de las víctimas de ransomware se vieron afectadas por ataques basados en extorsión, en comparación con un promedio mundial del 7%.
- El costo promedio de recuperación de ransomware fue de USD $1.52 millones, menor al promedio global de USD $1.85 millones.

"La alta capacidad del sector para restaurar los datos a partir de copias de seguridad permite a muchas empresas rechazar las demandas de pago de los atacantes en el caso de ransomware tradicionales basados en cifrado", dijo Chester Wisniewski, científico investigador principal de Sophos. *"Sin embargo, también significa que los adversarios se ven obligados a encontrar otros enfoques para ganar dinero con las víctimas, como robar datos y amenazar con filtrar información de la empresa si no se satisfacen sus demandas financieras".*

"Las copias de seguridad son vitales, pero no pueden proteger contra este riesgo, por lo que las empresas de manufactura y producción no deben confiar en ellas como defensa contra la extorsión. Las organizaciones necesitan ampliar sus defensas contra el ransomware combinando tecnología con la detección de amenazas dirigida por humanos para neutralizar los ciberataques avanzados en la actualidad", añade.

Los hallazgos también muestran que las empresas de este sector se preocupan más que cualquier otro por ser atacadas con ransomware en el futuro. El 60% dijo que esto se debe a que los ataques son tan sofisticados que se han vuelto más difíciles de detener. Por otra parte, el 46% cree que, dado que el ransomware es tan frecuente, es inevitable que se vean afectados.

Ante los resultados de la encuesta, los expertos de Sophos recomiendan las siguientes prácticas recomendadas para todas las organizaciones:

- **Suponer que la organización se verá afectada**. El ransomware sigue siendo muy común. Ningún sector, país u organización es inmune al riesgo. Es mejor estar preparado y no ser golpeado que al revés.
- **Realizar copias de seguridad frecuentes.** Las copias de seguridad de rutina son el método número uno que utilizan las organizaciones para recuperar sus datos después de un ataque. Incluso si las organizaciones pagan el rescate, los atacantes rara vez devuelven todos los datos, por lo que las copias de seguridad son esenciales de cualquier manera.
- **Implementar protección en capas.** Ante el considerable aumento de los ataques basados en la extorsión, es más importante que nunca mantener a los adversarios fuera de la red en primer lugar. Utilice protección en capas para bloquear a los atacantes en tantos puntos como sea posible.
- **Combinar expertos humanos y tecnología anti-ransomware.** La clave para detener el ransomware es la defensa que combina tecnología contra el ransomware y la búsqueda de amenazas dirigida por humanos. La tecnología proporciona escala y automatización, mientras que los expertos humanos son los más capaces de detectar las tácticas, técnicas y procedimientos reveladores que indican cuándo un atacante experto está intentando entrar.
- **No pagar el rescate.** Independientemente de cualquier consideración ética, pagar el rescate es una forma ineficaz de recuperar los datos. La investigación de Sophos muestra que después de pagar un rescate, los adversarios restaurarán, en promedio, solo dos tercios de los archivos cifrados.
- **Tener un plan de recuperación de malware y actualizarlo continuamente.** La mejor manera de evitar que un ciberataque se convierta en un caos es prepararse con anticipación. Las organizaciones que son víctimas de un ataque a menudo se dan cuenta de que podrían haber evitado muchos costos si hubieran tenido un plan de respuesta a incidentes.

###

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que 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 para la detección 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, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de

gestión integral basada en la nube llamada Sophos Central, el eje 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 distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

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