2 millones de dólares: el costo promedio que enfrentan las empresas de servicios financieros afectadas por ransomware

- **El 34% de las organizaciones de servicios financieros encuestadas fueron afectadas por ataques de ransomware en 2020, de acuerdo con Sophos.**

CIUDAD DE MÉXICO. 13 de octubre de 2021.- Sophos, líder mundial en ciberseguridad de última generación, anunció los hallazgos de El estado del ransomware en los servicios financieros 2021, que muestra cómo las organizaciones de este sector en todo el mundo gastaron más de **USD $2 millones de dólares** en recuperación promedio, cuando fueron víctimas de algún ataque de ransomware.

Esa cifra supera el promedio mundial que es de USD $1.85 millones, aunque los resultados también muestran que el sector financiero se encuentra entre los más resistentes contra del secuestro de datos: casi dos tercios (62%) de las víctimas encuestadas en este sector pudieron recuperar sus datos cifrados con el uso de copias de seguridad.

Otros hallazgos relevantes del reporte son:

- El 34% de las organizaciones de servicios financieros encuestadas fueron afectadas por ransomware en 2020.
- El 51% de las organizaciones afectadas dijeron que los atacantes lograron cifrar sus datos.
- Solo el 25% pagó el rescate exigido para recuperar sus datos cifrados. Este es el segundo porcentaje más bajo de entre todas las industrias encuestadas, debajo del promedio mundial que fue 32%.

Los servicios financieros se encuentran entre las industrias más reguladas del mundo: estas organizaciones deben cumplir con una serie de regulaciones, tales como el GDPR y PCI DSS, que incluyen costosas sanciones por el incumplimiento y violaciones de datos. Muchas de estas firmas también deben preparar algunos planes de continuidad del negocio y recuperación ante desastres para minimizar cualquier daño potencial de los datos robados, infracciones o interrupciones operativas derivadas de un ciberataque.

"*Las directrices estrictas en el sector de servicios financieros fomentan defensas sólidas*", dijo John Shier, Asesor Senior de Seguridad de Sophos. "*Desafortunadamente, también significan que es probable que el impacto directo que se produzca con el ransomware sea muy costoso para las organizaciones de este rubro. Si sumamos el precio de las multas reglamentarias, la reconstrucción de los sistemas y equipos de TI, además de lo destinado a estabilizar la reputación de la marca, especialmente cuando se pierden los datos del cliente, podemos*

entender por qué encontramos que los costos de recuperación para este sector superan los 2 millones de dólares".

"*Otros dos puntos de datos preocupantes son el hecho de que el 8% de las organizaciones de este tipo experimentaron lo que se conoce como ataques de "extorsión", donde los datos no son cifrados, pero sí son robados y las víctimas se ven amenazadas con la publicación en línea de la información a menos que paguen el rescate. Las copias de seguridad no pueden proteger contra este riesgo, por lo que las organizaciones de servicios financieros no deben confiar en esta medida como una defensa contra la extorsión",* señala Shier.

"Además, el 11% de las organizaciones financieras creen que no serán atacadas porque "no se consideran un objetivo". Esta es una percepción peligrosa porque cualquiera puede ser una víctima de los cibercriminales. El mejor enfoque es asumir que usted será un objetivo y construir defensas ante esa probabilidad", añade.

De las organizaciones de servicios financieros que creen que se verán afectadas por ransomware en el futuro, el 47% dijo que esto se debe a que los ataques ahora son tan sofisticados que se han vuelto más difíciles de detener. El 45% siente que se convertirá en un objetivo porque otras organizaciones en su industria ya han sido afectadas El 40% cree que, dado que el ransomware es tan frecuente, es inevitable que se vean atacados próximamente.

"El sector financiero tiene demasiado en juego como para no establecer un plan defensivo en profundidad para proteger, detectar y bloquear ciberataques", dijo Shier. "Si bien deberían seguir invirtiendo en copias de seguridad y sus esfuerzos de recuperación de desastres para minimizar el impacto de un ataque, también deben buscar extender sus defensas anti-ransomware mediante la combinación de tecnología con la caza de amenazas dirigida por humanos, esto para neutralizar los ciberataques avanzados dirigidos por humanos en la actualidad".

Para realizar el Estado del Ransomware de Servicios Financieros 2021 fueron encuestados 5,400 tomadores de decisión y líderes de TI de 550 organizaciones en 30 países de Europa, América, Asia Pacífico y Central, Oriente Medio y África.

###

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/