Consejos para blindar a tu empresa en el Día Mundial de la Ciberseguridad

- *Las víctimas de ransomware pagan en promedio $233,817 dólares por el rescate de su información*

CIUDAD DE MÉXICO. 26 de noviembre.- El 30 de noviembre se conmemora el **Día Mundial de la Ciberseguridad,** pero este es un tema del cual se debe generar consciencia todo el año y no únicamente en esta fecha, ya que las amenazas cibernéticas acechan a organizaciones de todos los tamaños y están en constante evolución, volviéndose cada vez más sofisticadas y peligrosas.

Este tipo de peligros, de acuerdo con datos del Informe de amenazas 2021 de Sophos, le cuestan cada vez más a las compañías en el mundo: tan solo en el tercer trimestre de 2020 el monto promedio que las víctimas de ransomware pagan por rescates de información fue de **$233,817.30 dólares,** aproximadamente, por lo que representó un incrementó de 21% respecto al periodo anterior. Un año antes, dicho monto era alrededor de $84,116 dólares.

Es por eso que **la ciberseguridad no tiene fin**, sino que se trata de un constante camino en el que se debe invertir, innovar y aplicar soluciones proactivas que permitan anticiparse a las acciones de los entes maliciosos, tanto a nivel corporativo como para los consumidores domésticos.

A continuación te decimos hacia dónde deberías enfocar la estrategia de ciberseguridad de tu negocio para protegerlo de las principales amenazas y cómo afrontarlas, de cara al 2021.

1. Ransomware

Los ciberdelincuentes continúan innovando en sus formas de operar para propagar el ransomware. **El robo de datos y la extorsión** continúan siendo los principales fines para la propagación de este tipo de ataques y el panorama hacia 2021 no luce alentador, es por eso que se requiere de una estrategia que contemple tecnología y soluciones que utilicen la inteligencia artificial y el *deep learning* para anticiparse a este tipo de amenazas.

Cabe destacar que durante 2020, **el 51% de las organizaciones en el mundo fueron víctimas de este tipo de ataques**; el 73% de estos incidentes tuvieron éxito al cifrar los datos de las empresas afectadas, de acuerdo con datos de Sophos.

2. El tiempo es 'oro' al protegerte

Parte fundamental de la estrategia de ciberseguridad de tu empresa debe basarse en actuar de forma rápida. Esto debido a que, de acuerdo con investigaciones de Sophos, un ataque que

antes tomaba semanas o días en propagarse de forma exitosa, **actualmente requiere de algunas horas para completarse.**

También es importante decir que los ataques han tomado como principales objetivos a aquellos sistemas o redes que se ejecutan en sistemas operativos **Windows y Linux**, ya que tienen vulnerabilidades que son aprovechadas para atacar a las organizaciones desde adentro de su red.

3. Voltea hacia el '*malware* básico'
Una estrategia de ciberseguridad no debe únicamente estar enfocada en detener aquellos ataques con alto nivel de sofisticación, ya que de manera reciente **se ha detectado un incremento en la propagación de ataques de 'gama baja'** que, pese a ser bastante más simples, pueden provocar afectaciones importantes.

Este tipo de familias de *malware*, indica el Sophos Threat Report, se convierten en **redes de distribución de contenido malicioso** debido a que las empresas dejan de poner atención en aspectos básicos de seguridad cibernética por enfocar sus esfuerzos en amenazas de mayor tamaño.

4. El trabajo remoto, un nuevo desafío
Los especialistas de Sophos han encontrado en el trabajo desde casa un importante reto para las organizaciones. Esta modalidad obliga a las empresas a expandir su perímetro de seguridad hacia miles de redes domésticas protegidas por niveles de ciberseguridad muy variables. Para ello, las organizaciones pueden voltear hacia la adquisición de **soluciones de ciberseguridad *On Demand* o como servicio**, que han tomado un impulso relevante derivado de la pandemia.

Con este tipo de herramientas, las empresas ya no necesitan hacer un gasto elevado para comprar una licencia completa y tener acceso a soluciones, sino que pueden adquirirlo como **un servicio basado en la nube mediante una suscripción mensual.**

###

Sobre Sophos
Como líder mundial en seguridad cibernética de última generación, Sophos protege de las amenazas cibernéticas más avanzadas de la actualidad a más de 400,000 organizaciones de todos los tamaños en más de 150 países. Desarrolladas por SophosLabs -un equipo global de inteligencia de amenazas y ciencia de datos-, las soluciones basadas en la nube y en IA de Sophos aseguran endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las técnicas de ciberataque que están evolución, incluyendo ransomware, malware, exploits, extracción de datos, violaciones de adversarios activos, phishing, entre otras. Sophos Central, plataforma de administración nativa de la nube, integra la cartera completa de productos de última generación de

Sophos, incluida la solución de endpoint Intercept X y el firewall de próxima generación XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita www.sophos.com.

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