Tips básicos de ciberseguridad para 2022 de Sophos

CIUDAD DE MÉXICO. 30 de noviembre de 2021.- Vivimos en un mundo en el que los ciberataques y amenazas están a la orden del día. De hecho, el reporte del Estado del Ransomware 2021, publicado por Sophos, indica de las empresas encuestadas, **25% en México; 33% en Chile; 19% en Colombia y 37% a nivel mundial, fueron víctimas del ransomware en el último año.**

Ante dicho escenario, y en el marco del **Día Internacional de la Ciberseguridad**, que se conmemora este 30 de noviembre, Sophos, líder mundial en seguridad cibernética de la siguiente generación, presenta a las empresas la guía básica para la protección de sus organizaciones para el cierre del año y de cara al 2022.

¿Cómo proteger a las empresas?

1. Siempre suponer que una organización está en riesgo
No importa el rubro: todas se encuentran en riesgo de ser vulneradas. Datos del reporte de ransomware de Sophos, por ejemplo, indican que tanto los comercios minoristas (44%), escuelas (44%), gobiernos (40%) y empresas de sectores como tecnología (37%), energía (36%) y servicios financieros (34%) fueron atacados durante 2020.

Es decir, ningún sector, país u organización es inmune al riesgo, y es mejor estar preparado con soluciones de seguridad en capas y servicios de respuesta a amenazas para no ser afectados.

2. Recuerda, el pago de un rescate no garantiza nada
Pagar el rescate por la información robada es una forma ineficaz de recuperar los datos. Estudios de Sophos muestran que después de pagar un rescate, los adversarios restaurarán, en promedio, solo dos tercios de los archivos cifrados.

Además, existe incluso un porcentaje de firmas a nivel global (7%) que pagaron un rescate a los atacantes cuando no habían cifrado los datos robados, lo cual habla de dinero perdido sin necesidad de ser desembolsado. En promedio, las empresas en el mundo pagaron montos de alrededor de **USD $170,404 dólares por cada ataque de ransomware**.

3. Copias de seguridad, un 'must' frecuente
Realizar copias de seguridad debe ser una de las rutinas más frecuentes. Se trata del método más efectivo para recuperar los datos comprometidos, sobre todo porque algunos ciberdelincuentes no devuelven la totalidad de la información incluso tras el pago de un rescate.

En 2021, el 57% de las compañías que se vieron afectadas lograron restaurar su información gracias a las copias de seguridad realizadas con anticipación, un incremento de 1% con respecto a 2020.

4. Implementa protección en capas

Hay que mencionar, como una tendencia importante, la presencia de ataques basados en extorsión. Esto se debe a que diversas organizaciones realizan, de buena manera, las copias de seguridad necesarias para proteger sus datos. Ante ello, los ciberdelincuentes prefieren, en lugar de cifrar los datos, amenazar a la víctima con la posible filtración de información sensible y piden un pago para no hacerlo.

Ante ello, Sophos recomienda establecer una estrategia basada en colocar varias líneas de defensa, en diversas capas de la organización, para mejorar la detección y respuesta ante el cibercrimen.

5. Combinar expertos humanos y tecnología anti-ransomware.

La clave para detener el ransomware es la defensa que combina tecnología contra ciberataques y la caza de amenazas dirigida por humanos. La tecnología proporciona prevención, escala y automatización, mientras que los expertos humanos son los más capaces de detectar las tácticas, técnicas y procedimientos (TTPs) reveladores que indican cuándo un atacante experto está intentando entrar o incluso cuando ya ha entrado, además de las mejores acciones para evitar daños mayores.

De hecho, datos del reporte del Estado del Ransomware 2021 indican que el 60% de las empresas globales afectadas confían, hacia el futuro, en que tienen el personal suficientemente preparado para hacer frente a futuras amenazas, sumado al 52% que indican que tienen la tecnología anti ransomware adecuada. Una suma de ambos aspectos, genera mayor confianza de cara al siguiente año.

Seguir las buenas prácticas antes mencionadas, ayudarán a las compañías a proteger a sus organizaciones de una amenaza inminente, difícil de neutralizar al 100%, y de la que todas las firmas del mundo deben estar presentes, toda vez que el costo de ser vulnerados puede ser muy alto tanto en lo económico como la propia reputación del negocio.

###

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/