6 consejos básicos para fortalecer tu estrategia anti-ransomware

CIUDAD DE MÉXICO. 26 de agosto de 2020.- El ransomware, en la actualidad y desde hace ya 10 años, se ha convertido en una de las principales amenazas en cuanto a seguridad cibernética para las organizaciones a nivel mundial. Tan solo en 2019, el 51% de las organizaciones fueron víctimas de ransomware y el 73% de esos incidentes tuvieron éxito al cifrar los datos de las empresas afectadas, de acuerdo con datos del 'Estado del Ransomware 2020', publicado por Sophos.

Durante los últimos meses, se han presentado casos de ransomware de gran magnitud, como el ataque a la firma estadounidense Garmin, cuyos datos fueron secuestrados por el ransomware WastedLocker; o Canon, cuya información fue robada por el grupo de cibercriminales Maze a inicios de agosto. Pero pese a ello, existen organizaciones que parecen desestimar el problema y reducir tanto la inversión como el tamaño en sus equipos de ciberseguridad, derivado de la pandemia por el COVID-19 y el impacto económico que generó.

"*La seguridad de la información debe ser una prioridad para las empresas y sus departamentos de TI, ya que los ciberdelincuentes están aumentando sus ataques y los equipos de seguridad deben estar completamente operativos y listos para prevenir el riesgo de ser atacados y manejar una situación de ese tipo*", indicó Ben Verschaeren, Global Solutions Engineer de Sophos, cuando también se hizo público el ataque de ransomware que sufrió la compañía turística Carnival Cruise Line.

Una de las soluciones más efectivas anti ciberataques es la protección para endpoints, pero además existen 6 mejores prácticas para la correcta configuración de los equipos y para maximizar la efectividad de tus defensas anti-ransomware que a continuación te recomendamos:

1. Políticas de seguridad siempre habilitadas: Puede sonar obvio, pero es la primera forma infalible de obtener la mejor protección para sus endpoints. Habilitar las funciones que detecten las distintas técnicas de ataque sin archivos y el comportamiento de ransomware es crucial para anticiparse a la posibilidad de ser vulnerado.

2. Revisiones periódicas de exclusiones de tu proveedor: En ocasiones, esas exclusiones o condiciones establecidas en las pólizas de los proveedores de seguridad están hechas para suavizar las quejas de los usuarios sobre las soluciones obtenidas. Es usual que los ciberdelincuentes obtengan información sobre los puntos excluidos en las pólizas para ingresar infiltrarse en los sistemas.

3. Habilita la autenticación multifactor: La Autenticación multifactor (MFA por sus siglas en inglés) proporciona una capa adicional de seguridad después de un primer factor que por lo general es una contraseña. Estas claves pueden ser fáciles de obtener para organizaciones de ciberdelincuentes con sistemas complejos, por lo que consisten en una capa de protección poco sólida contra entes maliciosos.

4. Garantizar que cada endpoint esté actualizado: Debes revisar los dispositivos de tu organización con regularidad para saber si están completamente actualizados con los parches de seguridad necesarios, lo que garantiza una protección óptima inmediata. Esta es una buena forma de mantener una protección adecuada en los equipos, que no solo mitiga el riesgo de ser víctima de ciberataques, sino que también puede ahorrarle mucho tiempo al equipo de seguridad cuando se trata de posibles riesgos en el futuro.

5. Indaga siempre al interior de tu red: Los actores maliciosos son astutos. Además de prevenir que sea atacada la organización, se debe aprovechar la tecnología de protección disponible para identificar amenazas avanzadas y adversarios activos en sus endpoint, incluso aunque todavía no se manifiesten.

6. Confía en la intervención humana de tus encargados de TI: Los piratas informáticos suelen dedicar mucho tiempo a explorar su red antes de implementar ransomware. La mejor manera de detectar esta actividad es combinar la experiencia humana con el trabajo de la tecnología y la Inteligencia Artificial. Recuerda que detrás de cada ataque, hay una persona al mando, por lo que pensar de forma anticipada a ese individuo es crucial.

En la actualidad, el costo promedio de recuperarse de ransomware es de hasta 1.4 millones de dólares, debido a que muchas empresas optan por pagar el rescate de la información secuestrada, según datos de Sophos. Es por eso que las organizaciones deben estar alertas a todos los indicios de ciberataques, así como no limitar la inversión en ese aspecto, ya que el costo de hacerlo puede ser mucho mayor.

###

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/