Factor humano: clave para proteger a las organizaciones en México

- El 40% de las organizaciones en México ya tienen una estrategia de 'caza de amenazas' liderada por equipo humano

CIUDAD DE MÉXICO. 15 de octubre de 2020.- Sophos, líder mundial en ciberseguridad de última generación, reveló que, de acuerdo con su encuesta *"Cybersecurity: the human Challenge"*, el factor humano es clave si se quiere proteger a las organizaciones a nivel mundial de las crecientes amenazas cibernéticas que se encuentran en constante evolución.

El estudio señala que el 40% de las organizaciones en México ya tienen una estrategia de 'caza de amenazas' liderada por equipo humano, porcentaje similar al promedio a nivel global, de 48%. Además, el 69% ya cuenta con un equipo subcontratado de profesionales en Tecnologías de la Información (TI) dedicados a ciberseguridad, un promedio mayor al del resto del mundo que es de apenas 39%. Asimismo, 80% planean subcontratar más personal para dichas tareas hacia 2022.

Además, el informe indica que a nivel global más de un tercio (35%) de las víctimas de ransomware en el mundo dijeron que reclutar y retener a personal experto en TI fue su mayor desafío cuando se trata de ciberseguridad, en comparación con el 19% del año anterior. En lo que respecta al enfoque de seguridad, la encuesta encontró que las empresas que han sido víctimas de ransomware gastan 42.6% menos tiempo en la contratación de personal para la prevención de amenazas que el año pasado, y por el contrario invierten más tiempo en la respuesta a ciberataques (27%) en comparación con aquellos que nunca se han visto afectados.

"*La diferencia en las prioridades de recursos podría indicar que las víctimas de ransomware tienen más incidentes por atender que el resto de las empresas. Sin embargo, también podría indicar que están más alerta a los múltiples riesgos por ciberataques avanzados y, por lo tanto, dedican más recursos a detectar y responder a las señales que revelan que un ataque de este tipo es inminente*", dijo Chester Wisniewski, líder científico en Sophos.

El hecho de que los atacantes de ransomware continúen evolucionando sus tácticas, técnicas y procedimientos, genera una mayor presión a los equipos de ciberseguridad de TI, tal y como lo indica la investigación de Sophos *"Dentro de un ataque de Ransomware Ryuk*". El artículo deconstruye un ataque reciente a la técnica Ryuk, elaborada para el secuestro de datos, en donde hallaron que los ejecutantes usaban versiones modificadas de herramientas legítimas para comprometer una red específica e implementar ransomware.

De este modo, hallaron que los ataques progresaban de tal forma que en tres horas los archivos maliciosos adjuntos penetraban y realizaban un reconocimiento interno de la red y

conseguían, en menos de 24 horas, acceso a un controlador de dominio interno para propagar su ataque.

"Nuestra investigación del reciente ataque de ransomware de Ryuk destaca que las empresas se enfrentan a una necesidad de alerta total, las 24 horas del día, los siete días de la semana, dichas empresas deben tener un conocimiento completo de la inteligencia anti-amenazas más actualizado para comprender el comportamiento de los atacantes. Está claro que cuando se trata de ciberseguridad, las organizaciones nunca son las mismas luego de haber sido atacadas por ransomware", indicó Wisniewski.

El informe completo, "*Dentro de un ataque de Ransomware Ryuk*", está disponible en el blog SophosLabs Uncut 2, mediante el cual los investigadores de Sophos publican periódicamente sus investigaciones e innovaciones.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall 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/