Los hogares: el nuevo perímetro en la estrategia de ciberseguridad de las empresas hacia 2021

- ***Datos de Sophos señalan que el 28% de las plantillas que trabajan a distancia desde múltiples ubicaciones han sido víctimas de ransomware.***

CIUDAD DE MÉXICO. 8 de diciembre de 2020.- El COVID-19 acabó con la normalidad tal y como la conocíamos en marzo de 2020. A partir de entonces, las empresas debieron ajustar, de forma drástica y rápida, sus modalidades de trabajo, convirtiendo al teletrabajo o ***Home Office*, en protagonista dentro de las organizaciones.**

Con una gran cantidad de empleados, de distintos niveles, enviados a casa para detener la propagación del virus, las empresas enfrentan hacia 2021 el reto de proteger a su organización con un perímetro que **se extendió más allá del control que podían tener al interior de sus oficinas.** Es decir, la ciberseguridad de las organizaciones se amplió hasta todos los rincones en los que los colaboradores conectan sus endpoints (ordenadores, celulares, tablets, etc.) a la red de la empresa.

Datos de Sophos indican que el **34% de las plantillas que trabajan a distancia desde múltiples ubicaciones han sufrido ataques de *malware*;** 29% han sido víctimas de exposición de datos; **28% han sufrido ataques de *ransomware***; 25% han visto sus cuentas comprometidas por amenazas propagadas por correo electrónico y el 17% han sido víctimas de *Criptojacking*.

Lo primero que deben entender las organizaciones es que el teletrabajo incrementará el número de **estafas propagadas por correo electrónico**, contemplando que los colaboradores en casa pueden volverse más vulnerables a caer en este tipo de fraudes. Datos de Sophos indican que tan solo en el primer mes de pandemia, la propagación de este tipo de correos fraudulentos **se incrementó un 3%**. Es importante que los equipos de seguridad cibernética y TI generen un mensaje de concientización entre los empleados y orienten al personal para reconocer correos apócrifos y amenazas de *phishing.*

Otra amenaza que conlleva el teletrabajo es la propagación de amenazas mediante el **protocolo de escritorio remoto (RDP) de Windows.** Se trata de un servicio estándar disponible en todas las versiones actuales de este sistema operativo que, con poco esfuerzo, permite a los administradores de TI o a usuarios acceder a un equipo cuando no están físicamente delante del mismo. Esa herramienta puede ser muy práctica y eficiente en épocas de pandemia en la que se requiere trabajar desde casa, pero lamentablemente también **se ha convertido en un blanco de los ciberdelincuentes** que optan por este tipo de vías para causar daños de gran magnitud a las empresas.

El Informe de Amenazas 2021 de Sophos indica que el principal riesgo, en este caso, radica en que el RDP es vulnerable si un ciberdelincuente decide atacar mediante intentos de acceso automatizados hasta conseguir su objetivo. Además, señala, el RDP no debe estar expuesto a las redes de internet domésticas, sino que deberían colocarse detrás de un *firewall* que requiera al usuario, primero, conectarse a una VPN u otro método de confianza, para luego acceder mediante una contraseña, *token,* o autenticación multifactor.

Una investigación de Sophos revela que, durante un periodo de 30 días, se registran alrededor de 467,000 intentos de inicio de sesión a través de un RDP, o alrededor de 600 intentos por hora.

Por lo anterior, las empresas deben enfocar una parte importante de su estrategia de ciberseguridad, para 2021, a los hogares de los colaboradores que, luego de la pandemia, seguirán haciendo sus labores de forma remota, expandiendo así las capacidades de protección y reacción ante amenazas de la organización.

Ahora, el módem en los hogares de los colaboradores de una empresa forma parte del perímetro de la red a proteger y las redes domésticas son la última línea de defensa ante ciberataques. Las compañías deben orientar sus esfuerzos hacia los endpoints remotos ya que, en ocasiones, las redes domésticas con las que operan están protegidas por sistemas de niveles de seguridad muy vulnerables o de niveles muy diversos, lo que hace que cuidar la seguridad de las empresas se complique.

###

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/