PROTEGERSE ANTE LA AMENAZA DEL RANSOMWARE, UNA NECESIDAD

Impulsado por la inteligencia ante amenazas (*threat intelligence*), la Inteligencia Artificial y el *machine learning* de los laboratorios Sophos Labs, Sophos Iberia ofrece un completo catálogo de soluciones y servicios avanzados, para la protección, detección y repuesta frente al Ransomware y la amplia gama de ciberataques que afectan a usuarios, aplicaciones, puestos de trabajo, redes y también al entorno cloud.

La compañía ha publicado recientemente el estudio independiente "El Estado del Ransomware 2022", que revela que este tipo de ataques –consistentes en secuestrar y cifrar la información de las empresas y liberarlas a cambio de dinero– sigue al alza. "El Ransomware continua su ascenso y sigue siendo una lacra que afecta a gran cantidad de empresas de todos los tamaños y en todos los sectores", explica Ricardo Maté, Vicepresidente de Sophos para el Sur de Europa.

Los datos del estudio dejan entrever varios datos muy significativos. El primero de ellos es que a lo largo de 2021, un 66% de las empresas a nivel mundial se vieron afectadas por ataques de este tipo, una cifra que en el caso de España es aún mayor: el 71%. Además, un porcentaje muy alto de las empresas atacadas (un 65% a nivel mundial y un 73% en España) vieron como los ciberdelincuentes conseguían cifrar los datos de sus víctimas después de haber extraído información valiosa de ellas. Por otro lado, de las empresas que reconocen haber pagado el rescate, que fueron un 38% en España, tan solo fueron capaces de recuperar el 50% de la información cifrada.

El estudio revela otros datos especialmente preocupantes, como que los ciberatacantes estuvieron de media 15 días en los sistemas de sus victimas antes de cifrar los sistemas, y cuatro días antes de llevar a cabo esta acción ya habían robado toda la información que necesitaban para exigir un cuantioso rescate. A nivel de cifras, las demandas que exige este tipo de delincuentes son cada vez mayores. La media es de 810.000 dólares a nivel mundial y de 185.000 en España, pero se han multiplicado por tres los rescates de siete cifras, sobre todo en sectores como la energía y la fabricación. "Pese a todas esas cifras, una conclusión esperanzadora es que las empresas están mejorando no solo sus defensas, sino también la capacidad de recuperase ante un ataque de este tipo", explican desde Sophos Iberia.

Ricardo Maté Salgado, vicepresidente para el Sur de Europa y *Emerging* de Sophos

CONSECUENCIAS DE LOS ATAQUES

Los ciberataques por Ransomware afectan a la capacidad de operar de las empresas (un 92% de las empresas encuestadas lo padecieron), pero sobre todo traen consigo una pérdida importante de volumen de negocio y de facturación, algo que reconoce el 86% de las compañías atacadas. "La recuperación ante un ataque de este estilo tiene dos caras: la económica y la que tiene que ver con el tiempo. En el primer caso, el coste medio a nivel mundial de recuperación tras un ataque de Ramsonware fue este año de 1,4 millones de dólares, mientras que en España la cifra alcanza los 750.000 dólares, un 25% más que el año anterior. En cuanto a la vuelta a la normalidad, el tiempo medio de recuperación ante un ataque de Ransomware es de un mes, aunque sectores como la educación o las administraciones públicas puede ser aún mayor", afirma Ricardo Maté.

Los ciberseguros pueden cubrir las pérdidas económicas, pero no protegen la información de las empresas

PRECAUCIONES

Cada vez son más las empresas que deciden asegurar su estructura mediante un ciberseguro, algo que hace el 92% de las compañías encuestadas a nivel mundial, cifra que cae hasta el 83% en la contratación de ciberseguros que cubran un ataque de Ransomware. En el caso de España, las organizaciones que han decidido cubrir ese riesgo solo alcanzan el 51%. La pregunta que se plantea es clara: ¿son los seguros una solución? Para Ricardo Maté, "los ciberseguros cubrieron el coste de los rescates en el 98% de los casos, aunque las aseguradoras que los ofrecen están poniendo condiciones más estrictas a sus asegurados, como la contratación de determinadas soluciones y/o servicios, la inclusión de excepciones o el alza del coste de las primas. Por tanto, el seguro en sí mismo no es una solución, al igual que no lo es en el caso de un seguro de vida, o de robo, pero puede ser una ayuda importante en el caso de sufrir un ciberataque".

Para los responsables de Sophos, la solución más eficaz es implantar un plan de ciberseguridad basado en diversos puntos clave, como disponer de defensas de alta calidad en todos los puntos del entorno (servidores, dispositivos móviles y de escritorio, apps, cloud, redes…), contar con un equipo propio o externo que pueda llevar a cabo la búsqueda de amenazas e investigarlas, fortalecer su entorno informático, disponer de un Plan de Respuesta ante ciberincidentes, realizar copias de seguridad y restaurar a partir de ellas o recordar aspectos esenciales como la formación de los empleados, la aplicación de políticas de acceso y de autenticación y la instalación de los "parches" a las vulnerabilidades del software.

SOLUCIONES PERSONALIZADAS

A la hora de poner en marcha esos protocolos, muchas empresas recurren a herramientas dispares para proteger cada entorno, disponen de procesos manuales para responder de manera reactiva ante un ataque y requieren de recursos intensivos para garantizar su protección. "Frente a esto, Sophos ofrece un Ecosistema de Ciberseguridad Adaptativo y abierto, que garantiza resultados superiores en este entorno tan complejo y que contempla las mejores soluciones de protección, detección y respuesta de los *endpoints*, la red y la nube, todo desde una única consola de gestión denominada Sophos Central", cuenta Ricardo Maté.

Sophos apuesta por una solución integral para proteger a las empresas del Ransonware, una amenaza en constante evolución

Se trata de una solución completamente abierta que permite la integración de herramientas o soluciones de terceros, con el entorno más avanzado de búsqueda de amenazas que componen los laboratorios Sophos Labs, la Inteligencia Artificial y los Servicios de Operación de Ciberseguridad.

"Estos servicios de Operación de Ciberseguridad, denominados *Managed Threat Response*, permiten a cualquier empresa de cualquier tamaño, disponer de un servicio 24/7 que detecte cualquier potencial ataque en menos de 1 minuto y que sea capaz de responder en menos de 38 minutos.

Por lo tanto, se trata de un entorno que optimiza la prevención, minimiza el tiempo de detección y respuesta y automatiza todas las acciones", concluyen desde la empresa.

www.sophos.com