Ataques de ransomware en el sector médico aumentaron 94% en 2021

- *En 2021, el 66% de las organizaciones de atención médica, según el Estado del Ransomware de Sophos.*

CIUDAD DE MÉXICO. 07 de junio de 2022.- Sophos, líder mundial en ciberseguridad de última generación, publicó el informe sectorial del Estado del Ransomware 2022, enfocado en las empresas del sector médico, que indica que en 2021 hubo un incremento de 94% en los ataques de ransomware hacia las organizaciones encuestadas en este sector.

El informe titulado "El estado del ransomware en el cuidado de la salud 2022", indica que el 66% de las organizaciones de atención médica se vieron afectadas; de ellas, el 34% también fueron vulneradas en 2020.

Sin embargo, el lado positivo radica en que las organizaciones de atención médica están mejorando en el manejo de la situación posterior al ataque, según los datos de la encuesta. El informe muestra que el 99% de las organizaciones de atención médica afectadas por el ransomware recuperaron al menos algunos de sus datos.

Entre otros hallazgos destacan:

- Las organizaciones del sector médico tuvieron el segundo costo promedio más alto de recuperación de ransomware con USD $1.85 millones, y tardaron una semana en promedio en recuperarse de un ataque.

- El 67% de las organizaciones de atención médica piensan que los ataques cibernéticos son más complejos.

- Si bien las organizaciones médicas pagan el rescate con mayor frecuencia (61%), están pagando los rescates promedio más bajos, USD $197,000, en comparación con el promedio general (todos los sectores) de USD $812,000.

- De aquellas organizaciones que pagaron el rescate, sólo el 2% recuperó todos sus datos.

- El 61% de los ataques resultaron en encriptación, un 4% menos que el promedio mundial (65%)

"*El ransomware en el espacio de la atención médica tiene más matices que otras industrias en términos de protección y recuperación"*, dijo John Shier, experto senior en seguridad de

Sophos. "*Los datos que aprovechan las organizaciones de atención médica son extremadamente sensibles y valiosos, lo que los hace muy atractivos para los atacantes. Además, la necesidad de un acceso eficiente y generalizado a este tipo de datos, para que los profesionales de la salud puedan brindar la atención adecuada, significa que la autenticación de dos factores típica y las tácticas de defensa de confianza cero no siempre son factibles",* añade.

Esto, según el especialista, deja a las organizaciones de atención médica particularmente vulnerables, y cuando se ven afectadas, pueden optar por pagar un rescate para mantener accesibles los datos pertinentes de los pacientes, que a menudo salvan vidas. Debido a estos factores únicos, las organizaciones de atención médica deben expandir sus defensas contra el ransomware al combinar la tecnología de seguridad con la búsqueda de amenazas dirigida por humanos para defenderse de los ciberatacantes avanzados de la actualidad, de acuerdo con Shier.

Cada vez más organizaciones de atención médica (78%) en la actualidad optan por un seguro cibernético, pero el 93% de estas entidades con cobertura de seguro informan que les resultó más difícil obtener cobertura de póliza en el último año. Dado que el ransomware es el mayor impulsor de reclamos de seguros, el 51% informó que el nivel de ciberseguridad necesario es cada vez más alto, lo que ejerce presión sobre las organizaciones de atención médica con presupuestos más bajos y menos recursos técnicos disponibles.

¿Qué hacer al respecto?

Los expertos de Sophos recomiendan las siguientes prácticas para todas las organizaciones de todos los sectores:

- Instalar y mantener defensas de alta calidad en todos los puntos del entorno de la organización. Revisar los controles de seguridad regularmente y asegurarse de que continúen satisfaciendo las necesidades de la organización.

- Reforzar el entorno de TI buscando y cerrando brechas de seguridad clave: dispositivos sin parches, máquinas desprotegidas y puertos abiertos de protocolo de escritorio remoto. Las soluciones de detección y respuesta extendidas (XDR) son ideales para ayudar a cerrar estas brechas

- Realizar copias de seguridad y practicar la restauración a partir de ellas para que la organización pueda volver a funcionar lo antes posible, con la mínima interrupción.

- Buscar amenazas de manera proactiva para identificar y detener a los adversarios antes de que puedan ejecutar su ataque; si el equipo no tiene el tiempo o las habilidades para hacerlo internamente, subcontratar a un especialista en Detección y Respuesta Administradas (MDR).

- Prepararse para lo peor. Es indispensable saber qué hacer si ocurre un incidente cibernético y mantener la tecnología de respuesta actualizada.

###

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/