Escuelas, las más afectadas por ransomware: el 60% fueron atacadas en 2021

- *Se trata de un importante incremento para las instituciones educativas que registraron un 44% en 2020; estas organizaciones son las más propensas a experimentar impactos operativos y comerciales por el ransomware.*

CIUDAD DE MÉXICO. 12 de Julio de 2022.- Sophos, líder mundial en ciberseguridad de última generación, publicó el Estado del Ransomware en la Educación 2022, que revela que el 60% de las instituciones educativas, tanto en el nivel básico como superior, se vieron afectadas por el ransomware en 2021, un incremento considerable desde el 44 % en 2020.

El reporte indica, además, que las instituciones educativas enfrentaron la tasa de cifrado de datos más alta (73%) en comparación con el promedio global de los sectores investigados por Sophos (65%); además, el tiempo de recuperación es el más largo, ya que el 7% tardó al menos tres meses en recuperarse, casi el doble del tiempo medio del resto de las industrias (4%).

Los principales hallazgos del reporte señalan que:

- Las instituciones educativas son las más propensas a experimentar impactos operativos y comerciales de los ataques de ransomware en comparación con otros sectores; el 97% de los encuestados de educación superior y el 94% de los encuestados de nivel básico dicen que los ataques afectaron su capacidad para operar.

- En el caso de las organizaciones privadas de educación superior, el 96% informaron que tuvieron pérdidas comerciales y de ingresos. Ese porcentaje es del 92% en el caso de las organizaciones privadas de nivel básico.

- Apenas el 2% de las instituciones educativas recuperaron todos sus datos cifrados después de pagar un rescate (frente al 4% en 2020); las escuelas, en promedio, pudieron recuperar el 62% de los datos cifrados después de pagar rescates (frente al 68% en 2020)

- Las instituciones de educación superior, en particular, registran el tiempo de recuperación de ransomware más largo; mientras que el 40% dice que se tarda al menos un mes en recuperarse (20% para otros sectores), el 9% informa que se tarda de tres a seis meses.

"*Las escuelas se encuentran entre las más afectadas por el ransomware. Son los principales objetivos de los atacantes debido a su falta general de fuertes defensas de ciberseguridad y la 'mina de oro' de los datos personales que poseen",* dijo Chester Wisniewski, científico investigador principal de Sophos. *"Las instituciones educativas tienen menos probabilidades*

que otras de detectar ataques en curso, lo que naturalmente conduce a mayores tasas de éxito en la vulneración y en el cifrado de datos", añade.

"Considerando que los datos cifrados generalmente son registros confidenciales de los estudiantes, el impacto es mucho mayor de lo que experimentaron la mayoría de las industrias. Incluso si se restaura una parte de los datos, no hay garantía de qué información devolverán los atacantes, lo que incrementa aún más los costos de recuperación y, a veces, incluso las puede llevar a la bancarrota. Desafortunadamente, estos ataques no se detendrán, por lo que la única forma de salir adelante es priorizar la creación de defensas contra el ransomware para identificar y mitigar los ataques antes de que sea posible el cifrado", explica.

Curiosamente, las instituciones educativas informan la tasa más alta de pago de seguro cibernético en reclamos de ransomware (100% educación superior, 99% educación básica). Sin embargo, en su conjunto, el sector tiene una de las tasas más bajas de cobertura de seguros cibernéticos contra ransomware (78% frente al 83% de otros sectores).

"Cuatro de cada 10 escuelas dicen que menos proveedores de seguros les ofrecen cobertura, mientras que casi la mitad (49%) informan que el nivel de seguridad cibernética que necesitan para calificar para la cobertura ha aumentado", dijo Wisniewski. *"Los proveedores de seguros cibernéticos se están volviendo más selectivos cuando se trata de aceptar clientes, y las organizaciones educativas necesitan ayuda para cumplir con estos estándares más altos. Con presupuestos limitados, las escuelas deben trabajar en estrecha colaboración con profesionales de seguridad confiables para garantizar que los recursos se asignen a las soluciones correctas que brindarán los mejores resultados de seguridad y también ayudar a cumplir con los estándares de seguros".*

Derivado de los resultados de la encuesta, los expertos de Sophos recomiendan las siguientes prácticas para todas las organizaciones, de este y otros sectores:

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

- Buscar amenazas de manera proactiva para identificar y detener a los adversarios antes de que puedan ejecutar ataques; si el equipo no tiene el tiempo o las habilidades para hacerlo internamente, se debe subcontratar a un equipo de Detección y respuesta administrada (MDR).

- Reforzar el entorno de TI buscando y cerrando brechas de seguridad clave: dispositivos sin parches, máquinas sin protección y puertos RDP abiertos, por ejemplo. Las soluciones de detección y respuesta extendidas (XDR) son ideales para este propósito.
- Prepararse para lo peor y tener un plan actualizado para un incidente.

- Realizar copias de seguridad y practicar la restauración a partir de ellas para garantizar que se minimicen las interrupciones y el tiempo de recuperación.

El Estado del Ransomware en Educación 2022 se hizo mediante encuestas a 5600 profesionales de TI, incluidos 320 encuestados de educación básica y 410 encuestados de educación superior, en organizaciones medianas (100-5000 empleados) en 31 países.

###

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/