Retail, el sector más afectado por el ransomware durante la pandemia

- ***El 44% de las firmas del sector se vieron afectadas durante la pandemia, porcentaje más alto intersectorial a nivel global según Sophos.***

- ***El 32% de las empresas de retail admitieron haber pagado por el rescate de su información, pero solo el 9% lograron recuperar la totalidad de los datos robados.***

CIUDAD DE MÉXICO. 20 de septiembre de 2021.- El sector minorista se convirtió, desde que inició el periodo de cuarentena en 2020 hasta la fecha, en el objetivo principal del *ransomware* a nivel mundial. De acuerdo con una investigación de Sophos, **el 44% de las organizaciones del sector del *retail* han sido afectadas a nivel mundial** por este tipo de cibercrimen en el periodo antes citado, **un porcentaje mayor al 37% registrado por el empresariado promedio global y el más alto del Estado del Ransomware 2021.**

De acuerdo con el estudio titulado el Estado del Ransomware del Retail 2021, realizado por Sophoslabs, señala que las empresas minoristas se volvieron el blanco predilecto de los ciberdelincuentes derivado del incremento en el volumen de ventas en línea prestado en la pandemia, además del alto número de transacciones en línea que se registraron en el periodo.

"El sector minorista siempre ha sido un objetivo atractivo para los ciberataques, con su complejo y distribuido. Entornos de TI, que incluyen una multitud de dispositivos de punto de venta conectados, un entorno relativamente transitorio y mano de obra no técnica y acceso a una amplia gama de datos de clientes personales y financieros ", dijo Chester Wisniewski, científico investigador principal de Sophos. *"El impacto de la pandemia introdujo desafíos de seguridad adicionales que los ciberdelincuentes aprovecharon rápidamente.*

El informe indica, además, que los ataques de *ransomware* no solo fueron más en cantidad sino que se presentaron más a menudo: **las firmas de *retail* fueron atacadas 19% más frecuentemente que el resto de las industrias en el mundo**. Sumado a lo anterior, **el 54% de las organizaciones afectadas indicaron que los cibercriminales tuvieron éxito al cifrar sus datos, mismo porcentaje que el promedio en el resto de las industrias**.

Es importante destacar que **el 32% de las empresas de *retail* admitieron haber pagado por el rescate de su información**, lo cual se encuentra en línea con el promedio global, aunque muy por debajo de otros sectores como las **empresas de Energía (43%), Gobiernos (42%), y Educación (35%) por mencionar ejemplos**.

En cuanto al monto pagado por dicho rescate, las empresas de *retail* se vieron obligadas a pagar una cifra menor al del resto de las industrias. En este caso, los minoristas tuvieron que

pagar en promedio $147,811 dólares, mientras que en el resto del empresariado el monto ronda los $170,404 dólares, según datos de Sophos.

Aunque se puede asumir que el pago de un rescate culminará con el problema, es importante mencionar que en el sector minorista **las empresas que realizaron ese pago recuperaron apenas el 67% de los datos comprometidos**, dejando el resto inaccesible. Únicamente el 9% de las firmas víctimas de *ransomware* lograron recuperar todos los datos cifrados.

Otro aspecto preocupante radica en el costo total de recuperación por el ciberataque que sufrieron las empresas del *retail:* mientras que en promedio **el sector privado en general pagó alrededor de $1.85 millones de dólares, las firmas minoristas pagaron aproximadamente $1.97 millones de dólares.** Este costo no solo implica el rescate pagado, sino que engloba los costos por la inactividad derivado del ataque, las horas invertidas por parte del personal de TI para mitigarlo, el costo de los dispositivos afectados, las repercusiones económicas directas por las afectaciones a la red, las oportunidades de negocio perdidas y el impacto a la reputación.

A futuro, es importante mencionar que el **62% de las empresas de *retail* en el mundo esperan ser víctimas de al menos un ciberataque durante el próximo año**, lo que habla de un sector alerta. Los motivos son diversos: el 20% considera que existen brechas importantes en sus sistemas de seguridad mientras que el 21% indica que es complicado controlar el riesgo de que sus usuarios comprometan la seguridad cibernética del negocio. La mayoría, el 47%, señalan que el *ransomware* es una tendencia creciente que es difícil de detener incluso utilizando herramientas sofisticadas de ciberseguridad.

Pese a lo anterior, aún existen algunos comercios (13%) que no consideran ser el tipo de empresas que suelen ser objetivo del *ransomware*, mientras que el 60% de las firmas que aún no han sido atacadas argumentan que han entrenado correctamente a sus equipos de IT y ciberseguridad para hacer frente a las amenazas, razón por la que creen que no se verán afectados pronto.

- **¿Cómo proteger a las empresas de retail?**

La primera recomendación desde Sophos es siempre asumir que el riesgo de ser víctimas de ransomware existe. Se trata de la amenaza más común, misma que afecta a empresas de diversos tamaños y sectores, por lo que la preocupación debe ser mayor aún cuando se trata de la industria más afectada a nivel global.

En segundo lugar, se deben realizar copias de seguridad offline de manera constante, ya que son el método predilecto para recuperar la información y desde luego uno de los más efectivos. Es importante también establecer una estrategia de protección en capas, ya que uno de los objetivos principales de los equipos de ciberseguridad es mantener, en la medida de lo posible, a los atacantes fuera de sus entornos y bloquearlos en la mayor cantidad de puntos posibles.

###

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que 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 para la detección 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, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje 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 distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/