El ecommerce mexicano crece como ninguno en el mundo, ¿cómo protegerlo durante el Hot Sale?

En la última década, el comercio electrónico en México ha experimentado un crecimiento sin precedentes. Según la Asociación Mexicana de Venta Online (AMVO), México se posiciona como el país número uno en crecimiento de ecommerce a nivel mundial desde el año pasado. Sin embargo, este auge viene acompañado de retos significativos en materia de seguridad digital, especialmente en temporadas de alta demanda como el Hot Sale, que comienza este 15 de mayo.

Proteger a las redes de los comercios durante esta época es relevante considerando que se trata de una temporalidad que atrae la intención de compra de 8 de cada 10 personas en México. En este contexto de alta demanda, Netskope destaca que el sector retail, que conforma en gran medida al ecosistema del ecommerce, se enfrenta a amenazas cibernéticas cada vez más sofisticadas.

Los criminales cibernéticos apuntan especialmente a las aplicaciones en la nube, siendo estas una herramienta cotidiana para los profesionales del sector. Netskope revela que, en promedio, los empleados del sector interactúan con alrededor de 20 aplicaciones en la nube cada mes, y el 1% más activo usa hasta 85 apps diferentes; esto hace del retail el tercer sector a nivel global (60%) más atacado mediante ese tipo de plataformas.

A diferencia de otros sectores donde Microsoft OneDrive lidera como la aplicación más usada y la principal fuente de descargas de malware, en el retail, Google Drive, Google Gmail y WhatsApp ocupan los lugares principales para la infiltración de malware. El mecanismo de ataque primario son los troyanos, que frecuentemente se utilizan para engañar a los empleados y hacer que descarguen cargas útiles de malware adicionales, como ladrones de información, puertas traseras y ransomware, causando daños significativos.

Los troyanos pueden alojarse en Google Drive y compartirse con las víctimas o, en ocasiones, un usuario puede cargar accidentalmente un archivo infectado en una ubicación compartida, lo que facilita su rápida propagación a todos los accesos disponibles. Entre las familias de malware más populares se encuentran Guloader y Remcos, que a menudo tienen como objetivo robar información bancaria, credenciales y datos personales y de tarjetas de crédito.

- Estrategias de protección para el ecommerce durante el Hot Sale

Vigilancia constante: Es crucial que los equipos de seguridad aseguren la inspección de todas las descargas desde la web y las aplicaciones en la nube confiables, utilizando soluciones como Netskope NG-SW, por mencionar un ejemplo, con una política de Protección contra Amenazas, que analiza el tráfico web y en la nube de manera transparente.

Uso de Aislamiento del Navegador Remoto: Cuando los empleados necesiten visitar sitios web de alto riesgo, como dominios nuevos o aplicaciones en la nube con puntuaciones de confianza bajas o nulas, es aconsejable emplear el Aislamiento del Navegador Remoto, que permite acceder a un sitio mediante una sesión de navegador a distancia en lugar del dispositivo de punto final habitual del usuario.

Sistemas de Prevención de Intrusiones: Establecer este tipo de sistemas es esencial para capturar y bloquear patrones de tráfico comunes de actividades maliciosas, como el tráfico de comando y control asociado con malware. Al impedir esta comunicación, se limita la capacidad de los atacantes de realizar acciones adicionales tras una vulneración exitosa.

Educación cibernética continua: Reforzar la educación sobre ciberseguridad del personal, resaltando la importancia de examinar correos electrónicos y mensajes, y pensar antes de hacer clic en enlaces atractivos pero peligrosos. Asimismo, es crucial recordar a los usuarios las políticas sobre el uso personal de dispositivos de la empresa.

El Hot Sale representa una oportunidad extraordinaria para el sector ecommerce en México, pero también un momento crítico para asegurar que las operaciones se mantengan seguras. Implementar estas estrategias no solo protegerá a las empresas contra amenazas actuales, sino que también fortalecerá su resiliencia frente a futuros ataques cibernéticos.