Conoce las consecuencias de los ciberataques en la cadena de suministros

Las cadenas de suministros que aún se encuentran desorganizadas por la pandemia, se han puesto nuevamente en tensión debido al conflicto entre Rusia y Ucrania, como el hecho de que empresas de transporte marítimo como Maersk, han anunciado que se suspendería temporalmente todos los envíos hacia y desde Rusia por vía marítima, aérea y ferroviaria, a excepción de los alimentos y los medicamentos.

Otros de los grandes transportistas como Ocean Network Express, Hapag-Lloyd y MSC han anunciado suspensiones similares.

Ciberataques y suministros

Asimismo, en la última semana, los ciberataques han generado una interrupción en la cadena de suministros, sobre todo la europea, donde se ha provocado las cancelaciones o desvíos de vuelos, sin embargo, este no es el objetivo principal de los ciberataques rusos, pues se trataría de los daños colaterales y de consecuencias de la guerra cibernética en Ucrania.

De acuerdo con la consultora CyberCx, un arma cibernética utilizada imprudentemente podría causar grandes daños colaterales a las organizaciones, por ello, puede que no se

vea un aumento de los ataques directos, sino más bien un aumento de las consecuencias de las amenazas de Estado a Estado, señaló el Idexcam.

Sin embargo, ello no excluye a las empresas europeas de la cadena logística. Uno de los ciberataques más costosos contra el transporte marítimo fue en el 2017 por una campaña ransomware, el cual infectó sistemas y equipos, bloqueando los archivos y exigiendo un pago para desbloquearlos, también amenaza con filtrar datos y así aumentar la presión.

Este ataque se originó en medio de un ciberataque a Ucrania, posteriormente vinculado a Sandworm, un grupo de hacking ruso de la Dirección Principal de Inteligencia, lo que provocó cuantiosas pérdidas con impacto en el mundo entero.

Ataque de sparphishing

Con respecto a los ataques cibernéticos, la empresa de transporte marítimo Hapag-Lloyd, en la segunda semana de marzo del presente año, sufrió un ataque de spar-phishing al haberse clonado la página web y correos electrónicos que se utilizan para redirigir a los usuarios a este sitio.

Estos inician sesión con sus datos de acceso personal y que luego son interceptados por delincuentes, revelando estos datos a los estafadores. Sin embargo, aún no hay pruebas suficientes para vincularlo con el conflicto.

Sin fronteras

A diferencia de la guerra tradicional, un ciberataque no tiene fronteras, por lo que las consecuencias se pueden extender a todos los que estén conectados a la red mundial de internet.

Los ataques de pishing y ransomware usan virus que escapan al control de los atacantes, y la frecuencia de estos se encuentra en aumento.

Teniendo en cuenta que en el 2021, los países latinoamericanos más afectados por ataques cibernéticos, fueron México, Brasil, Perú y Colombia, donde se generó la mayor distribución del malware a través de pishing, y ello se relacionó con el aumento del trabajo remoto.

En ese sentido, es necesario que se tomen medidas para prevenir una mayor amenaza a la ciber seguridad, resaltando que lo que ocurre actualmente en el mundo podría incidir aún más en el país.