EL VUELO DE LA GUACAMAYA

PALABRAS ARTICULADAS
Guillermo Deloya
gdeloya @gdeloya
Guillermo Deloya
www.guillermodeloya.com.mx
g_deloya@hotmail.com

La preocupación que motiva la corrección llega después de la consumación del acto delictivo que vulnera la secrecía de la información militar y gubernamental. Una discusión tardía pone en relevancia lo que en muchos otros países resulta prioridad: un cerco de real ciberseguridad es una necesidad tanto pública como social para mantener un equilibrio ante la gobernabilidad, la transparencia y la protección de datos tanto personales como en materia de seguridad nacional.

En este panorama donde un colectivo de hackers ha podido acceder —al parecer sin mayor complicación— a un cúmulo de archivos que revelan y revelarán diversas cuestiones, la labor legislativa para procurarle un cerco a la actividad es ya ociosa remedialmente. Si un marco normativo, suponiendo que existiese el idóneo, no se acompaña de una suficiencia presupuestal que vuelva operativamente eficiente el cometido de protección, es al igual incapaz de cerrar el paso a este tipo de delincuentes que día a día perfeccionan su actividad con la tecnología más vanguardista.

En nuestro país desde 2017 se presentaron cinco iniciativas cuyo cometido sería proveer de un andamiaje adecuado para contar con normas que protejan tanto a Estado como a particulares por los diversos frentes de ataque cibernético. Una modificación constitucional a los artículos 6 y 73 de la Carta Magna se propuso para elevar a rango de obligatorio el deber del Estado para otorgar seguridad en esta materia, así como para facultar al Congreso a legislar en lo específico.

Por otra parte, una de las propuestas incluso planteó la creación de un organismo público especializado denominado Centro Nacional de Seguridad Cibernética. Pero bien se dice que la atención no se concede hasta que el problema explota; este es el caso presente.

Directivas

Habrá que tomar en cuenta la dimensión de este problema a nivel mundial. Un estudio anual que elabora la empresa Comparitech, practicado este año a 75 países incluido México, aporta datos de interés. Conforme a tal investigación los últimos lugares en ciberseguridad los ocupan China, Bangladesh y Tayikistán en el fondo remoto. Por otra parte, en la cúspide de la protección cibernética está Dinamarca, que conforme a los 15 criterios aplicados logra el mayor puntaje de protección posible en temas como dispositivos infectados con *malware*, *troyanos* y *ransomware*, ordenadores infectados con *malware web*, ataques de telnet originados en el país y ataques de minería de criptomonedas, entre otros.

Curiosamente, México está poco más abajo de la media tabla y a pesar de nuestro asombro es líder en protección en temas como ataques por *troyanos* orientados a la banca móvil.

> "Delincuentes que día a día perfeccionan su actividad".

En este escenario se podría pensar que no estamos mal, pero cuando nos adentramos al estudio de referencia existen rubros señalados como condicionantes para la ubicación en los lugares concedidos a los países, cuyos datos no necesariamente se aplican ante lo complejo que resulta obtenerlos para una organización civil. Este es el caso del mantenimiento y actualización de software especializado en protección y defensa de privacidad y datos. Una reducción importante en el presupuesto específico de la Sedena parece haber sido esa condicionante que permitió el paso al ataque que apenas empieza a dar materia para la controversia empapada por un clima político.

Por otra parte, las potencias mundiales se endurecen en este tema después de la invasión rusa a Ucrania. En EU Joe Biden firmó en el pasado marzo la Ley de Fortalecimiento de la Ciberseguridad Americana, con la cual procura un manto de protección de todos aquellos organismos y empresas relacionadas con la operación, proveeduría y atención de la infraestructura crítica de este país. Se fortalece presupuestalmente a la Cybersecurity and Infrastructure Security Agency (CISA) y se le dota de capacidades de respuesta inmediata.

Por su lado, la Unión Europea implementa el Equipo Multinacional de Respuesta Cibernética para la mejora y fortalecimiento de la resiliencia cibernética. Establece reglamentos y directivas para el financiamiento útil y expedito en la materia y facilita la cooperación entre diversos organismos.

México debe tomar esta incursión a sus entrañas como un fuerte llamado de atención. No solo está en juego el evidenciar a un gobierno, sino proteger en conjunto a un país. V

Tecnología vanguardista.