NEWSLETTER

ideas PARA AVANZAR

COPARMEX

SEÑAL COPARMEX:

GRAVE Y PREOCUPANTE EL HACKEO A LA SEDENA

El hackeo a la Secretaría de la Defensa Nacional (SEDENA) es un hecho inédito. Es una dependencia fundamental para la preservación de la soberanía y la seguridad nacional, particularmente en este gobierno, una secretaría estratégica que concentra de acuerdo con el Inventario Nacional de lo Militarizado, realizado por el Programa de Política de Drogas (PPD) del Centro de Investigación y Docencia Económicas (CIDE), de 2018 a 2021, 31 tareas de otras dependencias federales o de gobiernos estatales o municipales. Por lo tanto, el ciberataque del que fue presa y la filtración de su información puede tener severas implicaciones que podrían poner en riesgo no sólo al Estado mexicano sino hasta personas y sus familias. En esta Señal COPARMEX analizaremos este hecho y su gravedad.

¿En qué consistió el ciberataque?

La información hackeada por el grupo Guacamaya es una filtración de 6 Terabytes de información que según expertos podrían representar entre 24 y 40 millones de documentos y miles de correos electrónicos alojados en los servidores de la SEDENA, archivos que datan del año 2016 hasta septiembre de este año.

Se señala que eso es aproximadamente el doble de la información divulgada en otra filtración como fue el caso de los Pandora Papers (2,9 Terabytes que se tradujo en 11.9 millones de documentos) que expusieron en 2021 operaciones financieras secretas a nivel global; o dos veces y media el caso de los Panama Papers (2.6 Terabytes) en 2016. Podría considerarse que es uno de los más graves ataques a nivel global por el volumen de información expuesta.

Según los expertos, la vulnerabilidad aprovechada en el caso Guacamaya Leaks fue producto de una debilidad del servidor Microsoft Exchange detectada durante el primer semestre del 2021, y que el gobierno mexicano no corrigió por falta de recursos para adquirir y realizar actualizaciones. Se trató, por lo tanto, de una situación posiblemente causada por falta de recursos económicos y humanos para monitoreo y prevención.

Muestra de ello es que profesionales en investigación forense aseguran que este ataque debió haber necesitado 3 días como mínimo para copiar la información, lo cual supone una falta de monitoreo e inacción de los encargados de la informática de la institución.

Aristas de preocupación

De acuerdo al Índice de Ciberseguridad Nacional (NCSI) 2022, México es el país que más ataques cibernéticos recibe en Latinoamérica y ocupa el lugar 84 de 160 a nivel global en materia de ciberseguridad, por debajo de países como Colombia, Jamaica, Panamá o Perú.

Por su parte, el estudio "Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, Reporte Ciberseguridad 2020", que elabora el Banco Interamericano de Desarrollo (BID) estima que, a nivel agregado, los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del Producto Interno Bruto (PIB) en algunos países y la cifra de ataques a la infraestructura crítica podría alcanzar hasta 6% del PIB.

En la Confederación Patronal de la República Mexicana vemos con preocupación que este ciberataque revela 3 aristas de análisis o implicaciones importantes:

1. La primera, desde una perspectiva puramente tecnológica, se confirma una falla patente en los estándares mínimos de ciberseguridad en las dependencias del gobierno de México. Pese a que estos ataques ya habían ocurrido en otros países, la inacción y la restricción presupuestal bajo la premisa de austeridad agravaron la situación de vulnerabilidad de una institución estratégica como lo es la SEDENA.
2. La segunda, la carente clasificación que deben tener como "INSTALACIONES CRÍTICAS" bajo la categorización internacional para todas aquellas instalaciones que contengan información sobre temas confidenciales o de seguridad nacional. Es necesario que las autoridades del gobierno mexicano realicen un peritaje y dictamen para identificar plenamente el volumen y relevancia de la información extraída, para hacer una correcta evaluación del riesgo y se implementen medidas inmediatas de mitigación.
3. Ha quedado manifiesta la necesidad de una Ley Federal sobre Ciberseguridad, que si bien ya se encuentra en proceso de creación en el Congreso, esta debería dar origen a un organismo institucional con entidad autónoma constitucional y con la creación de 32 autoridades, una por entidad federativa, a políticas públicas y a dotación presupuestal para hacer frente de forma ágil a este tipo de amenazas en un mundo cada vez más dependiente de las tecnologías de la información.

Postura COPARMEX

Prevención. Las Fuerzas Armadas tienen todo nuestro reconocimiento y estamos convencidos del enorme aporte que hacen al país, creemos que asignarles tareas que no se encuentran dentro de su marco legal y constitucional, las distrae y las ha expuesto a estos riesgos. La SEDENA y las dependencias encargadas de la seguridad nacional y la seguridad pública necesitan ser fortalecidas, particularmente, en sus unidades cibernéticas para combatir delitos como es la extorsión que ha crecido 55.6% entre 2018 y 2022 (cifras del 1er cuatrimestre).

Inversión. La Ciberseguridad es una inversión prioritaria para COPARMEX, lo vemos así para las empresas y para el gobierno. Por eso, contamos con una Mesa de Expertos en Ciberseguridad dentro de nuestra Comisión Nacional de Seguridad y Justicia, que ha advertido que el Paquete Económico para el

año 2023, se encuentra desconectado de la realidad y del crecimiento de la delincuencia que padecemos. La muestra es que el gasto total en seguridad sí refleja un aumento, pero este se concentra en la SEDENA con un incremento real de 16% pero que está relacionado con construcción de las obras emblemáticas, no estrictamente con tareas de seguridad; mientras que para la Secretaría de Seguridad y Protección Ciudadana (SSPC) tiene un minúsculo aumento de presupuesto del 1% que no responde a las necesidades cuando este año la inflación ha alcanzado una tasa de 8.7%. Sin duda, la inversión en seguridad debe replantearse tomando como ejemplo lo que han hecho los gobiernos de EE. UU., Reino Unido, Francia, Japón, Italia, Australia y Alemania. La administración Biden firmó un decreto en mayo del 2021 diseñado para fomentar las iniciativas de ciberseguridad, nombró a un director cibernético nacional para supervisar las políticas de seguridad digital y anunció medidas para proteger sus sistemas de información.

Planeación. Se requiere un Plan Maestro que guíe todas las iniciativas de ciberseguridad y facilite la coordinación gubernamental transversal, considerando al ciberespacio como una parte más del territorio nacional que requiere de un sistema de defensa.

Gobernanza. Ese Plan Maestro no debe quedar en papel, se requiere crear un organismo coordinador ex profeso que además actúe de forma inmediata y adaptable a los rápidos cambios tecnológicos. Un claro ejemplo de este ejercicio es EEUU que reforzó la autoridad de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional (DHS) para responder ante incidentes cibernéticos graves; Mientras que el Congreso aprobó legislación para codificar y financiar algunos de estos esfuerzos.

Talento digital. Se calcula que, en todo el mundo, faltan más de dos millones de especialistas en ciberseguridad, ante ello muchos gobiernos colaboran con universidades y escuelas para animar a los estudiantes a formarse en este ámbito. México debe sumarse al esfuerzo y acercarle a los jóvenes alternativas en estos rubros.

Diplomacia cibernética. Estas amenazas no conocen fronteras, por ello la cooperación internacional es esencial. Los miembros de la OTAN, por ejemplo, participan en ejercicios anuales denominados Escudos Bloqueados donde se simulan más de 2.500 ataques simultáneos. En América Latina y el Caribe, el BID y la OEA llevan a cabo diferentes actividades a lo largo del año para facilitar que los países de la región compartan conocimiento.

Trabajo conjunto entre el sector empresarial y el gobierno. En COPARMEX hemos generado una importante sinergia con la Dirección General Científica de la Guardia Nacional para promover la

educación y la prevención de delitos cibernéticos como son los robos de identidad y malwares. Debe incrementarse esta colaboración.

El gobierno no puede ni debe minimizar el hackeo que sufrió la SEDENA, la gravedad del caso amerita que se reconozca el hecho en su justa dimensión y se implemente una estrategia de mitigación de riesgos, insistimos, es gravísimo lo que ocurrió: está de por medio no solo la seguridad nacional, la operación de dependencias y proyectos, sino también la vida de personas.