H. Cámara de Diputados de la Nación

PROYECTO DE DECLARACIÓN

La Honorable Cámara de Diputados de La Nación

DECLARA

Preocupación por la falta de información publica sobre las actividades que se estén llevando a cabo en materia de Ciberseguridad desde el Poder Ejecutivo Nacional y en particular por la Dirección Nacional de Ciberseguridad. La preocupación se afianza ante el último ciberataque sufrido por la Dirección Nacional de Migraciones con secuestro de información sensible para la seguridad pública y por la relevancia de contar con un ciberespacio seguro y confiable para las operaciones de los organismos públicos y privados y en definitiva, de toda la ciudadanía.

Ingrid Jetter
Diputada de la Nación

Cofirmantes: Dip. Jose Luis Riccardo, Dip. Adriana Noemi Ruarte, Dip. Gabriela Lena, Dip. Alfredo Oscar Schiavoni, Dip. Alvaro De Lamadrid, Dip. Alicia Terada, Dip. Julio Sahad, Dip. Virginia Cornejo, Dip. Estela Regidor Belledone, Dip. Ignacio Torres, Dip. Marcelo Humberto Orrego, Dip. Alberto Asseff, Dip. Gonzalo Del Cerro, Dip. Jorge Enriquez.

FUNDAMENTOS

Señor Presidente:

El pasado 27 de agosto la Dirección Nacional de Migraciones fue objeto de un ciberataque *ransomware*, conocido como *Netwalker*, con supuesto secuestro de datos y posterior extorsión con vencimiento de pago para el 10 de septiembre.
El monto solicitado a cambio del rescate de los datos encriptados por el grupo cibercriminal asciende a 355 bitcoins, o sea aproximadamente unos 4 millones de dólares. Dicha suma publicada en un link del *Netwalker* y accesible a través de la denominada *deep web*, inicialmente fue de unos 2 millones de dólares pero a medida que transcurrió el tiempo y se acercó el plazo establecido, el monto total alcanzó el doble.
El hecho fue denunciado penalmente por extorsión, daño informático y acceso ilegitimo y hoy está en manos del Juez Federal Sebastián Casanello, bajo el expediente n. 685/2020.

Las pericias realizadas hasta el momento por la misma dependencia pública bajo el Ministerio del Interior, han confirmado que las máquinas afectadas por el virus sufrieron el encriptamiento de archivos locales y algunos del "Fill Server", donde se guardan gran parte de los archivos. Además se indicó que la base de datos no sufrió un ataque severo, es decir, sin modificaciones de los archivos.

Sin embargo, desde la semana pasada y a modo de prevención se está procediendo al reseteo manual de todas las máquinas afectadas y la investigación sobre el ataque aún se encuentra bajo proceso sin esclarecer del todo si el ataque se produjo desde la periferia del sistema o desde el interno de la misma sede central para luego expandirse al resto.

Por otra parte, según cuanto publicado en el *blog Netwalker* por el grupo que hackeó el sistema de la DNM , los archivos ya hoy publicados en ruso corresponden a la carpetas vinculados (al menos por su denominación) al Interpol, a embajadas y al AFI.

Ciber ataque de la Dirección Nacional de Migraciones (DNM)
La Dirección Nacional de Migraciones al momento de verificar el ciberataque decidió permanecer inoperable en todo su sistema de control de ingreso y egreso (SICaM - Sistema Integral de Captura Migratoria), afectando los servicios en los cinco pasos fronterizos terrestres habilitados más el del aeropuerto de Ezeiza y el de la terminal de Buquebus.

Efectivamente, ante las fallas verificadas y las confirmaciones de un posible virus en el sistema, posteriormente confirmado por Telefónica y Telecom, se procedió a cerrar el sistema, quedando las fronteras habilitadas cerradas por un lapso aproximado de cuatro horas, a fin de proteger la mayor cantidad de datos.

Cabe aclarar, que cuando el SICaM deja de funcionar se obliga a cerrar las fronteras ya que no es posible chequear órdenes judiciales o cédulas del Interpol. De este modo, el cierre del sistema una vez autorizado ocurrió a las 8 am y los problemas verificados por los distintos puestos fronterizos se iniciaron a notar desde aprox. las 5.45 am del jueves 27 de agosto.

Luego de algunas verificaciones técnicas, el ciberataque fue confirmado por la misma DNM y por las diferentes empresas del sector de ciber-seguridad en el país. La hipótesis de ataque se concluyó de confirmar por las publicaciones de las fotos de las carpetas mencionadas con posible información sensible.

La Dirección Nacional de Migraciones, expresó a través de sus redes sociales que el ataque había sido contenido en la tarde del 27 de agosto y que los datos críticos bajo su dependencia no han sido afectados. Asimismo, manifestó públicamente que no procedería con el pago de ningún rescate, dando detalle resumido del contenido de las carpetas de la imagen de captura de pantalla publicada por el grupo cibercriminal

Además de la renuncia solicitada del funcionario a cargo de la Dirección de Informática y Sistemas de la DNM, después de desempeñarse allí por más de 20 años, desde la semana pasada no solo se está procediendo con el reseteo manual de todas las computadoras afectadas sino que los puestos fronterizos habilitados continúan operativos bajo un sistema provisorio.

La identidad de los autores del delito es desconocida, y es muy probable como indican los expertos, que no se logre a identificarlos.

También permanece bastante difícil de definir el motivo que impulsó dicho acto criminal. Y las hipótesis al respecto comienzan a oscilar entre la intención de simplemente modificar o dañar datos al de sospechar sobre un ataque político o que el mismo haya sido realizado bajo encargo por algún grupo criminal con el fin de permitir o facilitar la comisión de otro delito tradicional.

En definitiva, se trata de un ataque que ha agravado el funcionamiento de un organismo público, el cual tiene bajo su tutela información sensible y crítica fundamental para la seguridad pública y por ello es relevante la actuación del Estado para garantizar junto a otros estados y actores intergubernamentales la seguridad y confiabilidad del ciber espacio.

Ciberseguridad en el país

La hiperconectividad que define prácticamente el mundo actual con sus posibilidades y oportunidades de crecimiento y transparencia pero también lo caracteriza por las amenazas y los ataques sin fronteras a la que encuentran expuestos los individuos y los sistemas a causa de la ciber- delincuencia.

La pandemia del COVID -19, ha puesto en mayor evidencia estos aspectos positivos y negativos y con ello la necesidad de garantizar un ciberespacio seguro y confiable a los ciudadanos y a las organizaciones públicas y privadas. Tal como expresado en las **Estrategias de Ciberseguridad de la República Argentina**[1], documento publicado en mayo del 2019 y fruto del trabajo desempeñado por el Comité de Ciber-seguridad interministerial, resulta imprescindible la definición de acciones de prevención, detección, respuesta y recuperación frente a las ciber-amenazas, junto al desarrollo de un marco normativo acorde y de capacidades de los entes involucrados.

Según los informes publicados en la plataforma de *Fortinet Threat Intelligence Inside Latin America*, en el país se registraron 270 millones de intentos de ciberataques entre el mes de enero y junio del corriente año. También otras empresas internacionales dedicadas a la ciber-seguridad como McAfee y Emsisoft confirman sobre el crecimiento en el 2020 sobre todo de robos de datos (aprox. 1 de 10 de los ciber ataques) que se suman al incremento verificado en las listas de los grupos que roban rutinariamente.

Asimismo, se destaca el incremento en las ganancias que estas actividades delictuales han alcanzado. Por ejemplo, se estima que desde el mes de marzo del 2020 los operadores de la *Netwalker ransomware* – software malicioso con que se atacó el sistema de la DNM - han ganado mediante las operaciones extorsivas seguidas a los secuestro de los datos robados un total de 25 millones de dólares. Estos resultados así como las dificultades que provoca el software para la desencriptación de los datos secuestrados lo posicionan para los expertos entre los primeros puestos de los *ransomwares* más dañinos en el mundo.

Según datos del Emsisoft, empresa que estima contar con un 25% del mercado nacional, en lo que va del 2020 se han registrado pedidos de desincriptación de archivos equivalentes al 98% del total alcanzado en todo el año del 2019 (es decir, registran un total de 5.858 pedidos contra los del total del año pasado de 6.111). Si bien, estos datos no distinguen entre los pedidos de instituciones públicas y privadas, nos permite comprender las dimensiones actuales de las amenazas y sobre el crecimiento de estos ante la mayor exposición y trabajo en red.

[1] http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/323594/res829-01.pdf

Respecto a las novedades verificadas en los últimos meses de los ciberataques realizados mediante el *ransomware Netwalker* en el mundo, el FBI alertó bajo un comunicado público sobre la diversificación de las acciones y de los canales utilizados para efectuar los ciber-asaltos, así como sobre la necesidad de que las dependencias gubernamentales realizaran actualizaciones permanente de sus sistemas porque estaban siendo también éstas desde junio también blancos de los ataques[2].

Dirección Nacional de Ciberseguridad

Por decisión administrativa n. 1224/2020 de la Jefatura de Gabinete de Ministros recién el 6 de julio del corriente se designó al Director Nacional de Ciber-seguridad: Lic. Gustavo Raúl SAIN[3], dependiente de la Secretaria de Innovación Publica. Y en base al organigrama[4] publicado por el Poder Ejecutivo Nacional, en el cual falta la indicación a dicha dirección, no se cuenta con otro organismo a nivel nacional específico en la materia y con competencias para como la anterior Subsecretaría de Tecnología y Ciber-seguridad entender para la supervisión, administración y gestión confiable y segura de los sistemas informáticos del Sector Público Nacional[5].

Por otra parte, respecto al ciberataque sufrido por el DNM en ningún momento se consideró además la intervención de la Dirección Nacional de Ciber-seguridad y sus actividades según cuanto publicado en la página del ente remontan solo a noticias con fecha del 2018.

Véase en: https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad

La falta de una política que siga los lineamientos establecidos en las Estrategias de Ciber-seguridad de la República Argentina o bien que se conozca sobre una mayor definición de estos u otros nuevos, nos exhorta preocupación sobre todo ante la relevancia hoy que la pandemia del COVID -19 ha dado a los servicios públicos dados por vía digital y la necesidad de que éstos se presten bajo total confiabilidad y seguridad de los datos personales de los ciudadanos argentinos y de los ciudadanos extranjeros. El reciente ciber-ataque a la Dirección Nacional de Migraciones, confirma la necesidad de una tutela activa de la seguridad del ciberespacio y sobre

---

[2] http://www.documentcloud.org/documents/7012381-FBI-flash-alert-about-NetWalker-ransomware.html

[3] https://www.boletinoficial.gob.ar/detalleAviso/primera/231868/20200708

[4] https://mapadelestado.jefatura.gob.ar/estructura_oescalar.php?n1=001

[55] Decreto 898/2016.

la exigencia de continuar a forjar una cooperación internacional con otros estados y organismos que trabajen en la materia.

Por todo lo expuesto, es que expreso preocupación por la aparente falta o reducida actividad de parte de la Dirección Nacional de Ciber-seguridad y es que solicito a mis pares me acompañen en la presente declaración.

Ingrid Jetter
Diputada de la Nación

Cofirmantes: Dip. Jose Luis Riccardo, Dip. Adriana Noemi Ruarte, Dip. Gabriela Lena, Dip. Alfredo Oscar Schiavoni, Dip. Alvaro De Lamadrid, Dip. Alicia Terada, Dip. Julio Sahad, Dip. Virginia Cornejo, Dip. Estela Regidor Belledone, Dip. Ignacio Torres, Dip. Marcelo Humberto Orrego, Dip. Alberto Asseff, Dip. Gonzalo Del Cerro, Dip. Jorge Enriquez.