Gobierno digital informa respecto a un acceso no autorizado a sus sistemas

Tal como comprometimos públicamente el sábado 10 de octubre y luego reiteramos el miércoles 14, en el presente documento informaremos en detalle de los nuevos antecedentes con los que contamos acerca del acceso no autorizado al sistema de Gobierno Digital, que hoy investiga la Fiscalía Nacional.

I. ¿Qué ocurrió?

El jueves 8 de octubre la División de Gobierno Digital sufrió un acceso no autorizado a sus sistemas, el cual se originó mediante la publicación en la página web de la División de Gobierno Digital (DGD) de un mensaje de carácter político, anunciando la posesión de información reservada, manifestando posición política respecto del próximo plebiscito y profiriendo ofensas y amenazas a personas públicas, de diversos ámbitos.

El día viernes 9, una vez confirmada la vulneración de los servidores de la DGD, se instruyó de inmediato acciones que apuntaron a cuatro objetivos:

a) Proteger los sistemas y su información.

b) identificar la información que pudo haber sido expuesta.

c) Identificar las vulnerabilidades que permitieron el acceso no autorizado.

d) Poner en antecedentes al Ministerio Público y la PDI para que se identifique a los responsables y se les apliquen las máximas penas de la ley.

II. ¿A qué se tuvo acceso?

Después de un proceso de profundo análisis y asistidos por expertos internacionales, se han llegado a algunas conclusiones que queremos compartir:

En el proceso de análisis de los sistemas de la DGD que se está llevando adelante se ha confirmado que información alojada en servidores administrados por la División se vio expuesta a terceros. De hecho, el día jueves 15 los atacantes divulgaron un archivo con información relativa a trámites digitales de algunos órganos de la administración del Estado, archivo cuyo contenido está siendo aún objeto de análisis para determinar con precisión la naturaleza de la información y la gravedad de su alcance, todo lo cual será oportunamente puesto

en conocimiento del público, en conjunto con las medidas que se adopten para dar tranquilidad a la ciudadanía.

Adicionalmente, este nuevo antecedente fue oportunamente puesto en manos de la Brigada de Delitos Cibernéticos de la Policía de Investigaciones y de la Fiscalía.

Es importante reiterar que, a la fecha, no se ha encontrado evidencia de que la información de ClaveÚnica haya sido vulnerada. En cualquier caso, insistimos en que no existe una base de datos de RUT y contraseñas, por lo que mal podría alguien sustraerla. La tecnología de ClaveÚnica impide que el sistema conozca la clave de cada persona, pues solo se almacena un código cifrado no reversible.

Para dar mayor tranquilidad a la ciudadanía, sin embargo, se está promoviendo la actualización de ClaveÚnica por parte de los usuarios, proceso que a la fecha ya han realizado más de 500 mil personas.

La División de Gobierno Digital continúa analizando sus sistemas para lograr la mayor certeza respecto a lo anterior y a las vulnerabilidades que lo permitieron. Para ello cuenta con el apoyo del Ministerio del Interior y Seguridad Pública y ha sumado la ayuda de expertos internacionales.

III. ¿Qué otras medidas hemos adoptado?

En cuanto se tuvo conocimiento de la intromisión a los servidores se adoptaron estrictas medidas de seguridad para el acceso a los mismos, además de la instalación de una

herramienta de seguridad que protege a los servidores y aplicaciones frente a vulnerabilidades, malwares y cambios no autorizados, herramienta que incorpora machine learning y parches virtuales. Esto se suma a otras medidas que se han tomado en función del avance de la investigación.

Finalmente, es bueno mencionar que en la medida que el país avanza en su transformación digital, los riesgos y las amenazas de ciberseguridad aumentan, lo que ha quedado de manifiesto en diversos ataques a infraestructura pública y privada en los últimos años. Este no es el primero, ni será el último ataque informático, y para ello el sector público y privado tienen que estar preparados. Avanzar tanto en la gestión de riesgos de ciberseguridad, como en la legislación de cibercrimen que actualmente se tramita en el Congreso Nacional, es de suma importancia. Estamos seguros de que esta experiencia, finalmente nos ayudará a avanzar más rápido en estas materias. Lamentablemente, en Chile y en el resto del mundo, ocurre que los criminales intentan ir siempre delante, y es para eso debemos estar preparados y siempre alertas.

Gobierno Digital reafirma su compromiso con seguir facilitando la vida de las personas mediante la entrega de herramientas tecnológicas al Estado y, si bien se han logrado grandes avances en estas materias, estamos conscientes de los desafíos que tenemos hoy y siempre tendremos frente a ataques de este tipo.

Por último, queremos hacer hincapié en que la difusión de la información privada de las personas constituye un delito y que velaremos porque quienes la hayan obtenido y publicado sean identificados y llevados ante la justicia.