LITORALPRESS

Fecha: 01-10-2022
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo C
Tipo: Actualidad
Título: CNA reconoce "ataque informático" con filtración de cientos de archivos

Pág. : 10
Cm2: 403,0
VPE: $ 5.293.553

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: Neutra

Comisión Nacional de Acreditación recibe apoyo de Interior:

CNA reconoce "ataque informático" con filtración de cientos de archivos

DIERK GOTSCHLICH

Hackers robaron información de su página en junio y ayer era la fecha límite para el pago del "rescate" mediante monedas digitales. Como este no ocurrió, publicaron desde licencias médicas hasta documentos universitarios.

La Comisión Nacional de Acreditación (CNA) confirmó ayer que fue víctima de un "ataque informático", que se tradujo en el secuestro y publicación de información interna del organismo, entre licencias médicas, resoluciones externas y documentos de universidades.

En detalle, el robo de información se produjo en junio de este año, y el grupo responsable del hackeo, conocido como Lockbit, dio un plazo de tres meses a la institución para el pago de una suerte de "recompensa" en monedas digitales. Esto mediante una cuenta regresiva que caducaba ayer al mediodía, cuando fueron filtrados los datos.

En la CNA dicen que notaron el robo por la caída de la página oficial de la institución, momento en el cual se contactó al Equipo de Respuesta ante Emergencias Informáticas o CSIRT, que depende del Ministerio del Interior.

El organismo de seguridad activó un cortafuego digital y trasladó los archivos a un nuevo dominio para bloquear nuevos traspaso de datos.

Ayer, al conocerse la filtración, la CNA declaró que "inmediatamente se realizó la denuncia a los organismos competentes y ahora todo esto es parte de una investigación en curso".

Además, señaló, los datos liberados serían administrativos y no de procesos de acreditación que pusieran en riesgo a planteles de educación superior. No obstante, la CNA ya prepara acciones legales por la liberación de datos sensibles de sus funcionarios, como los relacionados con licencias médicas.

CNA

ENCARGADO.— El académico de la U. Católica Andrés Bernasconi preside la Comisión Nacional de Acreditación desde marzo de este año.

> *Recibimos un ataque informático. Inmediatamente* ***se realizó la denuncia a los organismos competentes y ahora todo esto es parte de una investigación en curso".***
>
> COMISIÓN NACIONAL DE ACREDITACIÓN

"La tormenta perfecta"

El ataque se suma a una serie de delitos digitales de este tipo en el último tiempo. De hecho, varias empresas han sido víctimas de fraudes informáticos este año, entre ellas una multitienda y un par de bancos, los que sí habrían pagado el "rescate" en monedas digitales para proteger su información privada y la de sus clientes.

Lo que han planteado expertos en informática es que actualmente se vive "la tormenta perfecta" para este tipo de delitos, impulsada por una fuerte aceleración y evolución digital en los negocios, la masificación del teletrabajo a causa de la pandemia, el aumento de activos y datos de clientes, y la existencia de nuevas herramientas para realizar ciberataques.

Para Alberto Castañeda, gerente general de Netprovider, hoy existe una "explosión del cibercrimen por la evolución digital en todo tipo de industrias", que se mezcla con el impulso del trabajo desde los hogares luego de la contingencia sanitaria.

Eso último, detalla, "genera que la superficie de riesgo ahora esté tanto dentro como fuera de las organizaciones, porque la innovación puede ser usada tanto para el bien como para el mal por los ciberdelincuentes".

El especialista también puntualiza en que "hoy los activos digitales son tanto o más valiosos que los activos físicos, por lo que le generan mayor retorno a la criminalidad".

Con todo, Castañeda concluye que "si no asumimos esta nueva realidad y seguimos subvalorando la importancia de la ciberseguridad, probablemente estos casos dejarán de ser episodios aislados para convertirse en una lamentable nueva forma de delinquir o generar daño".

Esa alerta también la dieron otros especialistas ayer en redes sociales, donde se debatió ampliamente el tema. Algunos de ellos, incluso, se aventuraron en apuntar a que el *modus operandi* del grupo de *hackers* se asemeja a cómo han operado criminales informáticos rusos en los últimos meses, por lo que podría estar ligado a ese país.