LITORALPRESS

Fecha: 27-03-2026
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo C
Tipo: Noticia general
Título: Hackeo a Presidente Kast evidencia falencias en ciberseguridad y dificultad para identificar a responsables

Pág. : 5
Cm2: 680,6

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Este tipo de vulneraciones ha ocurrido también a diversas instituciones públicas en el pasado:

Hackeo a Presidente Kast evidencia falencias en ciberseguridad y dificultad para identificar a responsables

Se atacaron sus cuentas personales, confirmaron desde La Moneda. Expertos explican que se pueden configurar delitos que tengan "consecuencias penales reales".

E. CANDIA

"Estimados. Perdonen la hora. Pero les queremos avisar que las cuentas personales del Presidente en X y en Instagram han sido comprometidas por terceros. Por la eventualidad de que salga un mensaje adicional al que ya salió y fue borrado. Apenas recuperemos el control de las cuentas les avisaremos, pero nada de lo que se publique en esa cuenta en estas horas corresponde a la autoría del Presidente".

Ese fue el mensaje que comenzó a circular desde Presidencia durante la madrugada de ayer, luego de que la cuenta en X a nombre del jefe de Estado, José Antonio Kast, posteara una fotografía del mandatario estadounidense Donald Trump junto con un particular mensaje.

Se trataba de un contenido complejo, debido a las tensiones internacionales derivadas de la guerra en Medio Oriente. "Chile ha cambiado su postura respecto al presidente Trump tras sus recientes acciones, que han causado graves daños a nivel mundial. Ha traicionado sus promesas a Chile, y esto se ha prolongado demasiado. Donald Trumpler es peor que Hitler", decía la publicación que permitió a Presidencia percatarse del uso indebido, decía el mensaje que daba cuenta de un hackeo.

Tras el hecho, diversos expertos consultados comentan que este tipo de vulnerabilidades en el Estado es más habitual de lo que se podría creer. "Es bastante más común de lo que uno pensaría. No es un problema exclusivo del Estado, sino algo que afecta también a empresas y figuras públicas en todo el mundo. Los ataques de toma de cuentas son hoy uno de los incidentes más frecuentes en ciberseguridad", dice Edison Escobar, experto de Attsons Consulting.

Por su parte, Pedro Anguita, abogado y experto en derecho de la información de la U. de los Andes, comenta que "tanto la Presidencia de la República como muchos organismos suelen ser objeto de ataques informáticos, algunas veces para obtener información valiosa que les sirva para delinquir y otras veces por motivos ideológicos".

Gravedad por contexto, impacto y desconfianza

A pesar de que La Moneda tomó el control de las redes sociales y eliminó el mensaje, diversos expertos consignan que la situación es grave más allá del acceso no consentido a la cuenta. Así, Anguita dice: "La gravedad está dada por los efectos negativos que pudieran tener los contenidos emitidos por el hackeo en nombre del jefe de Estado", aunque destaca que "se detectó a tiempo". Pero, cree, "es conveniente elevar el nivel de las medidas de seguridad que poseen los dispositivos que utiliza tanto el Presidente Kast como de todo alto funcionario del Estado".

Escobar entiende que a pesar de que "es un hecho relevante", hay que contextualizarlo. "La gravedad no está tanto en una falla técnica del Estado, sino en el impacto que puede generar", dice. Y añade que "cuando se compromete una cuenta de este nivel, el problema es que se pueden emitir mensajes falsos con apariencia oficial, y eso afecta directamente la confianza pública. Dependiendo del contenido, incluso puede tener implicancias políticas o diplomáticas".

Coincide Luis Abarca, gerente de operaciones ciberseguridad e ingeniería del Grupo Tecnológico ITQ, quien plantea que "no todos los incidentes cibernéticos de este tipo equivalen a un 'ataque a la seguridad del Estado', pero sí pueden impactar la percepción pública de seguridad y control de las comunicaciones de un líder político".

Desde Presidencia solo informaron que tomaron el control de las redes sociales y no se refirieron a posibles acciones penales. Sin embargo, el hecho reviste características de delitos.

Consecuencias penales, "no es una falta menor"

Aunque Anguita señala que el hackeador podría "ser perseguido por el delito de usurpación de identidad, del artículo 214 del Código Penal, que se sanciona con la pena de presidio menor en su grado mínimo (61 a 540 días)".

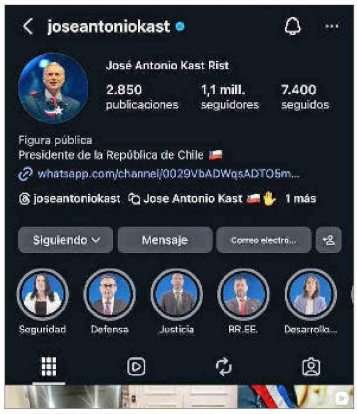
Mientras que Escobar considera que "lo más evidente es el acceso ilícito a sistemas, pero también puede haber uso fraudulento de credenciales". Y explica que "acceder a una cuenta de este tipo sin autorización no es una falta menor. Tiene consecuencias penales reales, y la experiencia internacional lo demuestra. Esto no es solo teórico. Hay casos concretos donde estos hechos terminan en condenas. El hackeo masivo de cuentas en X en 2020 terminó con responsables identificados y procesados. Graham Ivan Clark, por ejemplo, fue condenado a tres años de prisión, y Joseph O'Connor recibió una condena de cinco años". Abarca agrega que los delitos pueden incluir "acceso ilícito a cuenta informática; suplantación de identidad y uso fraudulento de medios digitales".

Dificultades técnicas, legales y probatorias

Sin embargo, puntualiza el gerente del Grupo Tecnológico ITQ, "la calificación exacta depende de la investigación". En ese sentido, además de la necesidad de denuncia, se requiere de un imputado, lo cual se dificulta en este tipo de hechos.

Anguita detalla que "determinar al responsable de un hackeo, ya sea en redes sociales u otro sistema informático, presenta algunas dificultades técnicas, legales y probatorias y otras como el lugar donde se encuentra el ciberdelincuente". Porque, dice, "los *hackers* suelen recurrir a herramientas avanzadas como VPN, servidores *proxy* y redes que les permiten ocultar su ubicación real e identidad, rebotando su tráfico a través de múltiples nodos en todo el mundo". También los delincuentes digitales avezados suelen eliminar sus rastros "empleando tácticas para suprimir los *logs* que registran las actividades, o bien todo rastro digital que dejen al acceder a un sistema informático. Por último, los *hackers* en muchas ocasiones suelen vivir en países distintos a los de sus víctimas, por lo que se requiere cooperación internacional y entrar en procesos judiciales complejos, al igual que la respuesta de empresas tecnológicas que se requiere para la individualización".

Según Abarca, en definitiva, "la probabilidad de identificar y sancionar al responsable dependerá de la calidad de la investigación técnica forense, la cooperación de las plataformas (X, Meta/Instagram) y la capacidad de las autoridades de perseguir delitos cibernéticos".



REFORZAR SEGURIDAD.— Si bien expertos consideran que hackeo se detectó a tiempo, advierten de riesgos asociados a estos delitos. Recomiendan "elevar el nivel de las medidas de seguridad que poseen los dispositivos que utiliza tanto el Presidente Kast como de todo alto funcionario del Estado".

2022, UN AÑO COMPLEJO

- **FRECUENCIA** A través de los años, algunas autoridades o instituciones del Estado han sufrido graves hackeos. Sin embargo, en 2022 la situación fue crítica.
- **EJÉRCITO** Así quedó en evidencia tras el robo de miles de correos electrónicos del Estado Mayor Conjunto, los que terminaron por ser difundidos. El mismo año cientos de computadores fueron afectados por un virus informático en el Poder Judicial.
- **EDUCACIÓN** Por ese entonces, la Comisión Nacional de Acreditación confirmaba un "ataque informático" que terminó con la publicación de información interna del organismo.
- **DEFENSORÍA** Por su parte, la Defensoría Penal Pública corrió con mayor suerte, pues pudo detectar tempranamente un ataque, lo que le permitió a la institución evitar la situación.