LITORALPRESS

Fecha: 01-10-2022
Medio: La Prensa de Curicó
Supl. : La Prensa de Curicó
Tipo: Actualidad
Título: "Chile no cuenta con suficiente capacidad técnica para contrarrestar cibercriminales"

Pág. : 5
Cm2: 613,8
VPE: $ 793.662

Tiraje: 4.200
Lectoría: 12.600
Favorabilidad: No Definida

"Chile no cuenta con suficiente capacidad técnica para contrarrestar cibercriminales"

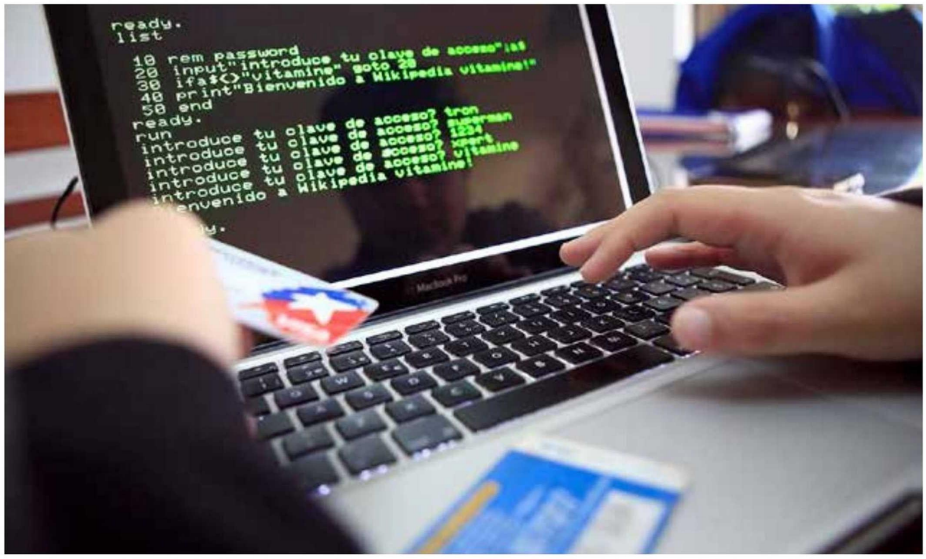
Académico. Rodrigo Bustamante, especialista en Seguridad de la Información, afirmó que no existe una cultura arraigada dentro de la sociedad por este tema.

TALCA. Los recientes ciberataques a los sistemas informáticos del Poder Judicial y del Estado Mayor Conjunto de las Fuerzas Armadas, ha puesto en tela de juicio la preparación que, como país, tenemos para contrarrestar o prevenir esos delitos.

Para el especialista en Seguridad de la Información y académico de la Facultad de Ingeniería de la Universidad de Talca, Rodrigo Bustamante, Chile está al debe en esta materia.

Dado el hackeo del EMCO (Estado Mayor Conjunto de las Fuerzas Armadas) y del Poder Judicial, ¿qué tan vulnerables como país estamos ante los hackers?

"Como país, estamos muy al debe respecto de la ciberseguridad en general. Si bien, este año se actualizó la ley de delitos informáticos, aún no se cuenta con una institucionalidad acorde con los requerimientos que un tema como la ciberseguridad lo requiere. El país no cuenta con un organismo que concentre todos los esfuerzos y recursos necesarios para hacer frente a los ciberataques, como una agencia nacional de ciberseguridad, y tampoco con la suficiente capacidad técnica para poder contrarrestar a las organizaciones cibercriminales".



Los recientes ciberataques a los sistemas informáticos a instituciones del Estado, ha puesto en tela de juicio la preparación para contrarrestar o prevenir esos delitos. (Fotos, Carlos Alarcón).

"Los ciberdelincuentes utilizan herramientas y técnicas especializadas para encontrar fallos y acceder a sistemas con el fin de dañar, obtener beneficio monetario o prestigio".

Si se puede vulnerar la seguridad de esas y otras instituciones, ¿qué tan expuestos podemos estar las personas comunes y corrientes?

"Las personas también estamos expuestas a amenazas diariamente. En general, cuando una persona utiliza una clave fácil de recordar, acepta a una persona desconocida en redes sociales o incluso abre un archivo adjunto en un email desconocido, se arriesga a ser víctima de un ciberataque. Esto se debe a que no existe una cultura arraigada dentro de la sociedad por el tema de la seguridad y solo cuando ocurren hechos como los vividos en los últimos días, nos comenzamos a cuestionar respecto de si estamos tomando las medidas necesarias para protegernos en el mundo digital, he incluso no pasamos de eso, de solo cuestionarnos y no tomar acción para cuidar nuestra identidad digital".

Rodrigo Bustamante: "Como país, estamos muy al debe respecto de la ciberseguridad en general".

¿Cómo trabajan los hackers, de qué manera pueden ingresar a las bases de datos, qué elementos emplean?

"Primero, hay que distinguir a los hackers de los ciberdelincuentes. Un hacker utiliza herramientas tecnológicas para identificar vulnerabilidades y fallos en los sistemas, he informar a los encargados para que tomen acción y puedan subsanar el problema, sin buscar dañar u obtener beneficios de esto. Los ciberdelincuentes son lo contrario. Estos últimos, utilizan herramientas y técnicas especializadas para encontrar estos fallos y acceder a sistemas con el fin de dañar, obtener beneficio monetario e incluso solamente prestigio. Aclarado esto, los ciberdelincuentes buscan blancos vulnerables, muchas veces sin un objetivo claro, y cuando los encuentran analizan todo el entorno dentro de la organización e instalan programas que pueden realizar mapas completos de la infraestructura de red y de activos de información (como bases de datos, entre otros) que posee su objetivo y con eso ya pueden extraer toda la información que les parezca relevante. Luego, y según sus objetivos, pueden robar esta información y publicarla, como lo que le sucedió al Estado Mayor Conjunto o encriptarla y solicitar un rescate a la organización para recuperarla".

CATÁSTROFE

Aunque suene cinematográfico, ¿es posible que los hackers provoquen una catástrofe mundial?

"Por supuesto. Hoy es de conocimiento general que existen grupos organizados y apoyados por gobiernos que buscan atacar la infraestructura crítica de ciertos países. Supongamos el caso de que un grupo ataca una planta de energía nuclear de un país y causa una catástrofe de proporciones y luego le endosa la culpa a un país con el cual tiene conflictos; claramente, el país afectado podría tomar represalias y si tiene un arsenal nuclear y decide utilizarlo, podría generar una catástrofe mundial. Puede sonar cinematográfico, pero si esto sucediera en el actual conflicto que tiene a Rusia y Ucrania en guerra, esto podría provocar un conflicto a gran escala".

"Es necesario contar con organismos especializados que apoyen todas las instituciones a enfrentar un ciberataque".

¿Qué se debe hacer para enfrentar los delitos informáticos, basta tener una legislación, qué otras medidas se deben adoptar?

"No basta con tener una legislación, que por supuesto ayuda, ya que desincentiva a los ciberdelincuentes. Sin embargo, si estos no se denuncian o se tratan de manejar entre 4 paredes, tampoco sirve de mucho la legislación. Es necesario contar con organismos especializados que apoyen todas las instituciones a enfrentar un ciberataque, a recuperarse y a sacar lecciones de estos. También es necesario crear capital humano avanzado en temas de ciberseguridad, que en Chile aún faltan muchos, pero también capacitar a la población en general, para crear una cultura de ciberseguridad a nivel país. Otra medida importante es generar instancias para fomentar la investigación avanzada en estos temas y ventanas de difusión para esta, donde los investigadores puedan exponer sus resultados a toda la comunidad y a sus pares. Es necesario también invertir recursos importantes, tanto públicos como privados, para crear empresas de base científico-tecnológicas que ayuden a generar productos que se puedan aplicar a las empresas e instituciones. Y como último punto, es crear redes de cooperación nacional e internacional para poder mirar lo que se hace en otros países y así poder aplicar las mejores prácticas para mejorar nuestro nivel de madurez en ciberseguridad".