LITORALPRESS

Fecha: 27-11-2024
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: Colaboración y asociatividad son clave para el éxito de una estrategia de ciberseguridad

Pág. : 7
Cm2: 641,7
VPE: $ 8.429.637

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

DESAFÍOS PARA CHILE:

Colaboración y asociatividad son clave para el éxito de una estrategia de ciberseguridad

Además, dicen los especialistas, es imprescindible avanzar en materia de regulación, que las empresas mejoren sus estándares de vulnerabilidad digital y educar a los usuarios para que, uniendo fuerzas entre distintos sectores, podamos prevenir y responder mejor y más rápido ante cualquier incidente.

PAMELA CARRASCO T.

En un mundo donde prácticamente todo lo que hacemos está mediado por un dispositivo tecnológico, resguardar la ciberseguridad es fundamental. Sin embargo, los expertos advierten que, si bien hemos avanzado en el uso de ciertas herramientas digitales, aún somos muy descuidados con nuestra información personal o laboral.

"En general, no usamos buenas claves o confiamos muchas veces en sistemas en los que no deberíamos confiar", dice Daniel Álvarez, coordinador nacional de Ciberseguridad y presidente del Comité Interministerial sobre Ciberseguridad.

Añade que debemos entender que tenemos frente a nosotros a un adversario muy diverso. "Hay organizaciones criminales de distintos niveles; hay descuidos organizaciones; hay delincuencia menor, además de robo y suplantación de identidad para después cometer otros delitos, y de todo eso debemos hacernos cargo. Por mucho tiempo, pensamos que la ciberseguridad era un problema técnico y de grandes empresas, pero hoy sabemos que es un tema que nos compete a todos como sociedad", afirma.

Álvarez analizó el estado del arte de Chile en el campo de la seguridad cibernética en el programa "Ciberseguridad en Universo", de Radio Universo. En ese contexto, comentó las mejoras que ha tenido el país gracias a la Ley de Ciberseguridad y el avance en materia de protección de datos.

"Hoy, la política de ciberseguridad se ha transformado en un asunto de Estado: tenemos ley, vamos a tener una Agencia de Ciberseguridad el próximo año y hemos avanzado en temas como regulación *fintech*, datos personales y delitos económicos e informáticos. Actualmente, nuestro sistema regulatorio es uno de los más completos de Latinoamérica y el mundo, pero todavía hay mucho por avanzar y el gran desafío es implementar todo esto de buena forma", resaltó.

"POR MUCHO TIEMPO, PENSAMOS QUE LA CIBERSEGURIDAD era un problema técnico y de grandes empresas, pero hoy sabemos que es un tema que nos compete a todos como sociedad", señala Daniel Álvarez, coordinador nacional de Ciberseguridad.

ESCENARIO HETEROGÉNEO

Junto con la educación de los usuarios y la ciudadanía en general, también es primordial poner énfasis en que las empresas chilenas mejoren sus estándares de vulnerabilidad digital y se encaminen hacia una cultura donde la seguridad esté en el centro.

Rocío Ortiz, subdirectora de Industrias del Futuro del Centro de Innovación UC Anacleto Angelini, explicó en "Ciberseguridad en Universo" que hoy hay mucha heterogeneidad: "Las grandes empresas han avanzado mucho en consolidar sus capacidades, competencias y conocimientos en términos de ciberseguridad, pero hay un gran desafío en la cadena de suministro, que muchas veces son proveedores de estas grandes compañías. Y ahí tenemos una serie de empresas pequeñas y medianas que requieren progresar en este sentido", dijo.

La experta agregó que el tema es complejo, ya que se centra en el capital humano y se necesitan personas capacitadas en las pymes, lo que aumenta los costos. "Pero incluso si pudiéramos hacerlo, no tenemos la cantidad de personas suficientemente preparadas para ocupar esos puestos", sostuvo.

Por eso, manifestó que es importante apoyar a este segmento y poner a su disposición capacidades y recursos humanos para gestionar de manera sencilla la seguridad digital. Y en esto, trabajar unidos entre distintos sectores es fundamental.

"Para que una buena estrategia de ciberseguridad funcione, hay que abordar el elemento humano y también la colaboración y asociatividad. Tenemos el desafío de compartir información entre sector público, privado y académico para hacer frente a esto", aseguró Ortiz.

En este sentido, mencionó el nuevo Laboratorio de Ciberdefensa para Protección de Infraestructura Crítica, una iniciativa del Centro de Innovación UC y del Ejército de Chile, que permitirá pilotear tecnología, compartir información y colaborar, de modo de ir "polinizando" entre estas distintas áreas y tomar ventaja frente a la ciberdelincuencia.

INDUSTRIAS SENSIBLES

Los especialistas también advierten que hay que poner ojo en las industrias críticas para el país o aquellas que pueden ser más atractivas para los ciberdelincuentes. Una de ellas es la minería, que ha tenido un fuerte avance tecnológico en los últimos años. Las estadísticas muestran que los ciberataques en este sector aumentaron en un 40% entre 2021 y 2023.

"El ciberdelincuente que quiere atacar a una industria específica, como el coordinador eléctrico, los servicios sanitarios, la minería o cualquier otra industria importante, es un especialista que tiene muchos más conocimientos, preparación y recursos para hacerlo que un delincuente informático común y, por eso, el principal foco nuestro debe ser prevenir", dijo en "Ciberseguridad en Universo" Katherina Canales, directora ejecutiva de la Corporación de Ciberseguridad Minera.