LITORALPRESS

Fecha: 19-11-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: LOS DESAFIOS QUE PERSISTEN EN PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS

Pág. : 18
Cm2: 426,4

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

LOS DESAFÍOS QUE PERSISTEN EN PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Este tipo de construcción se ha vuelto un blanco de ataques cibernéticos y también es vulnerable a amenazas físicas, por lo que proteger y garantizar su integridad y funcionamiento es fundamental.

POR SOFÍA PREUSS

El concepto de infraestructuras críticas incluye los activos, redes, instalaciones sistemas y otros elementos que abarcan numerosas industrias del país, entre ellos energía, telecomunicaciones, fabricación y transporte. La mayoría tiene una alta dependencia a internet para su operación, gestión y automatización, y son pilares fundamentales para la mantención de la seguridad nacional, la vitalidad económica, la salud pública y seguridad local.

Es por ello que este tipo de construcciones se han vuelto objetivos codiciados tanto para ataques cibernéticos como físicos, por lo que la protección y garantía de su integridad, disponibilidad y confidencialidad son hoy temas fundamentales.

Para el director nacional de seguridad de Grupo Eulen Chile, Andrés Muñoz, el ataque a dichas instalaciones atenta contra el desarrollo y el crecimiento, afectando directamente a las personas y a las instituciones o empresas del país. "En diversos sectores económicos de Chile ya hay instalaciones donde los sistemas tecnológicos operan con alertas tempranas y registros que permiten, además de la detección, la búsqueda rápida por criterios, el análisis forense de causas y la identificación de condiciones que facilitan la comisión de delitos", explica.

En esa medida, el coronel (r) de Carabineros y consultor en seguridad pública y privada, Pedro Valdivia, expone que la seguridad en todo sentido no es un costo, sino una inversión. "A esta altura, especialmente en el sector empresarial, se debe pensar que un evento crítico que afecte a sus instalaciones tiene costos directos, pero probablemente muchos costos indirectos en su entorno, a veces incuantificables en la comunidad", indica.

Regulaciones

Durante los últimos cinco años los reguladores de la industria financiera, de las telecomunicaciones y del sector público han establecido normativas específicas para sus respectivos sectores, lo que ha ayudado a las distintas organizaciones a la prevención y respuesta ante posibles ataques, señala la socia de cyber technology and transformation de Deloitte, María Luisa Acuña. "Esto es lógico si pensamos que son sectores altamente atractivos, producto de la gran cantidad de datos personales y altas transacciones digitales que manejan diariamente", expone.

En esa línea, Acuña destaca que la ley 21.663 marca un hito en la protección de estas infraestructuras. "Chile es el primer país en Latinoamérica que contará con una normativa tan completa y detallada en el ámbito de la ciberseguridad", indica, y detalla que todos los sectores considerados como críticos para el funcionamiento del país y la protección de los derechos y bienestar de los ciudadanos deberán aplicar medidas para prevenir, detectar y responder a los incidentes.

"Ahora bien, la simple adopción, implementación y despliegue de un estándar no resuelve la compleja dinámica de los ataques, pero sí ayudan a generar las bases y cimientos sobre los cuales se pueda desplegar un conjunto de controles y tecnologías por parte de la industria, que realizados sistemáticamente permiten ir mejorando progresivamente la resiliencia energética a nivel país y continental", acota la ejecutiva.

Para seguir avanzando, el director nacional de seguridad de Grupo Eulen Chile apunta que el principal desafío está en que la tecnología, las herramientas, las plataformas y las soluciones logren permear el conocimiento de los profesionales de la seguridad, y que "estos sean capaces de configurar soluciones personalizadas que potencien la eficacia de la seguridad, tanto física como electrónica".

US$ 10 MIL MILLONES

SERÁ EL COSTO GLOBAL DEL DELITO CIBERNÉTICO EN 2025, SEGÚN ESTIMACIONES DE CYBERSECURITY VENTURES.