LITORALPRESS

Fecha: 25-10-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Cómo fue el primer simulacro de ciberataque de infraestructuras críticas**

Pág. : 40
Cm2: 393,1
VPE: $ 3.483.149

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

DF DIARIO FINANCIERO

DF LAB
INNOVACIÓN, STARTUPS Y TRANSFORMACIÓN DIGITAL

Uno de los equipos de trabajo durante la simulación.

Cómo fue el primer simulacro de ciberataque de infraestructuras críticas

El Centro de Innovación UC y el Ejército realizaron una simulación de un ataque de ransomware a una institución financiera ficticia, en la que diversos actores asumieron roles para aprender a gestionar una crisis de ciberseguridad.

POR MARCO ZECCHETTO

La recien aprobada Ley Marco de Ciberseguridad crea la figura de infraestructuras críticas, aquellas que son esenciales para el funcionamiento del país, como electricidad, banca o telecomunicaciones.

En este contexto, el Laboratorio de Ciberdefensa para Infraestructuras Críticas (CiberLab), iniciativa del Centro de Innovación UC y el Ejército de Chile y representantes de los sectores público, privado y academia, realizó su primer ejercicio de simulación en tiempo real de un ciberataque, para desarrollar competencias en gestión de crisis y buenas prácticas en ciberseguridad.

En el ejercicio, que se realizó en la Escuela Militar, en Las Condes, participaron 100 personas de empresas, universidades y gobierno, quienes debieron enfrentar un ataque de *ransomware* (secuestro de archivos a cambio de un rescate) a una institución financiera de servicios esenciales ficticia.

Durante casi dos horas, cada asistente asumió un rol representando a las distintas áreas de la entidad, como gerencia general, legal, comunicaciones o informática, que participan en los equipos de gestión de crisis, donde tuvieron que tomar decisiones tanto a nivel estratégico como táctico.

El general de división, Rodrigo Marchessi, comandante de Operaciones Especiales del Ejército de Chile, dijo durante la actividad que "las Fuerzas Armadas, y el Ejército en particular, tiene y asume un rol importante en estas iniciativas. Somos responsables de implementar y operacionalizar las soluciones técnicas y estratégicas que resultan de estas colaboraciones".

En tanto, la subdirectora de Industrias del Futuro del Centro de Innovación UC, Rocío Ortiz, explicó que la idea del ejercicio surge de las necesidades de generar simulaciones, ya que "la misma Ley Marco de Ciberseguridad pide dentro de su normativa que se generen capacidades de forma transversal para poder enfrentarse a ciertos incidentes".

Comentó que este será el primero de una serie de ejercicios de simulación y prácticos, y que su propósito es enfrentar y diseñar un lineamiento de trabajo basado en el *framework* (marco) para respuesta de incidentes que establece el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, en inglés).

"La idea es entender cómo dentro de una crisis no hay solo roles técnicos, programadores o de ciberseguridad, sino que también hay comités de crisis a nivel comunicacional, legal, de tomadores de decisiones", dijo.

Ejercicio técnico

En paralelo, el Ciberlab en colaboración con DreamLab Technologies, Duoc UC y el Ejército de Chile, realizó un ejercicio virtual dirigido a equipos técnicos de respuesta en ciberseguridad, basado en el modelo *capture the flag* (CTF), un desafío de seguridad cibernética donde los competidores deben defender una vulnerabilidad en un sistema o aplicación.

Participaron 200 profesionales organizados en 80 equipos, quienes debieron enfrentar 10 desafíos y cuatro escenarios de infraestructura crítica simulados, entre ellos, una maqueta de un aeropuerto con tecnología operativa real, donde los equipos desplegaron sus habilidades y conocimientos.