Fortaleciendo la seguridad cibernética de los Sistema de Emergencia en América Latina

En el marco del 17 Congreso Internacional de Centros de Atención de Llamadas de Emergencia, organizado por NENA México, el jueves 24 de octubre, Budge Currier, de *Emergency Technology Consulting*, realizó una presentación sobre ataques cibernéticos a los 9-1-1. Su intervención estuvo enfocada en tres aristas: prevención, preparación y contención.

Este tema es particularmente relevante para los Sistemas de Emergencia de América Latina porque, según la primera y segunda edición de la publicación PSAPs: Edición América Latina de la OEA y EENA, 11 de 20 Sistemas o Centros de Emergencia (lo cual representa un 55% del total), no cuentan con procesos establecidos o certificaciones para asegurar la ciberseguridad.

Dada esta brecha, es importante avanzar en la implementación de regulaciones, medidas y procesos para el fortalecimiento de la seguridad cibernética de los Sistemas o Centros de Emergencia de la región. La ponencia de Currier ofrece algunos elementos interesantes para avanzar en ese sentido.

En primer lugar, Currier compartió algunas buenas prácticas en materia de ciberseguridad:

- Evitar redes planas e inseguras.
- Adoptar una red de infraestructura de clave privada.
- Mantener los sistemas actualizados para minimizar el riesgo
- Corroborar que los registros de seguridad estén habilitados y activados (mensual y anual).
- Identificar cuáles son las amenazas a los sistemas críticos.
- Contratar los servicios de una consultora externa para que lleve a cabo un análisis de las redes y los sistemas. Este análisis conlleva no solo una prueba de penetración sino también una habilitación para que puedan entrar a la arquitectura del sistema e identificar sus vulnerabilidades.
- Identificar quiénes pueden brindar ayuda en caso de un ciber incidente. Tener la información de contacto de estas personas y establecer una relación profesional para que luego sea fácil contactarlas.
- Priorizar los riesgos y comenzar con su mitigación.

También brindó algunas sugerencias sobre cómo prepararse para un ciber ataque:

- Aprender de otros Centros que tienen sistemas y redes similares.
- Llevar a cabo ejercicios de simulación, con diferentes tipos de escenarios. Convocar al personal de informática del Centro, así como también a los proveedores de tecnología con los que se trabaja.
- Nombrar a un jefe/director de incidentes para ciberataques. Esta persona debe tener un perfil en informática y experiencia trabajando con tecnología.
- Designar a una persona para que maneje la comunicación con los medios de comunicación, las autoridades y el público.
- Tener relaciones bien establecidas con personas y personal clave que pueda brindar apoyo ante un ciber ataque.
- Elaborar un plan de respuesta.

En lo que respecta a cómo responder ante un ciber ataque, Currier mencionó los siguientes puntos:

- Identificar el tipo y la dimensión del ataque
- Determinar el curso de acción. Si se debe cerrar el sistema, ¿quién tiene la autoridad para hacerlo?
- ¿Qué autoridades e instituciones deben ser notificadas? Tener en cuenta que el ciber ataque pudo haber afectado a otras instituciones y no solo al Sistema de Emergencias.
- Comunicar al público acerca del incidente (número y medios/canales alternativos para comunicarse con el 911)