Próxima meta para combatir la ola global de ciberataques: crear un marco común europeo de defensa

Líderes de la Eurocámara, del Mando Conjunto del Ciberespacio, del mundo empresarial y académico han definido durante la segunda jornada de DES las claves para blindarse ante los nuevos conflictos en la era digital

José Andrés Jiménez, Jefe del Departamento TIC en el Congreso de los Diputados, ha avanzado que el gobierno está construyendo, a corto plazo, una estrategia de gestión cibernética, ya que la actual es poco "madura"

Madrid, 12 de junio de 2024. – El potencial de las tecnologías exponenciales ha abierto la ventana a nuevas oportunidades de negocio y de desarrollo, si bien también ha inducido al surgimiento de riesgos inéditos siendo los ciberataques los máximos protagonistas. En 2023 los gestionados por el Centro Criptológico Nacional subieron un 94% respecto a 2022, impactando también en el ámbito material y el bienestar de las personas. "*Las guerras físicas y cibernéticas ya no están separadas. El ciberespacio no tiene fronteras, sólo un campo de juego en el que cualquiera con conexión a Internet es un jugador*", ha indicado **Enrique Pérez de Tena,** jefe de sección de RRII y de cooperación del Mando Conjunto del Ciberespacio, durante su participación en la segunda jornada de **DES – Digital Enterprise Show**.

Este miércoles, el evento ha analizado las claves de cara a gestionar de forma eficaz una crisis cibernética con el foco puesto en la estrategia de reputación, la respuesta operativa y las tácticas de comunicación. Además, ha explorado cómo los gobiernos deben afrontar los conflictos que van más allá de la presencialidad y mejorar las estrategias de defensa. "*Es necesario que la normativa de la UE se prepare para las nuevas formas de guerra"*, ha apuntado **Timea Lapsanszki**, asesora política de Asuntos Exteriores y Defensa en el Parlamento Europeo.

En líneas similares se ha expresado **Manuel Antonio Fernández-Villacañas**, profesor y Director del Máster en Inteligencia Económica para la Gestión de la Seguridad en la UNIR, que ha afirmado que el mundo VUCA (volátil, incierto y complejo) ha evolucionado hacia el mundo BANI (frágil, ansiosos, no lineales e incomprensibles), donde la desinformación tiene un peso importante. "*Las formas de guerra ocurren todo el tiempo a nivel internacional. La '3ª Guerra Mundial 5.0' es muy diferente a los conflictos anteriores*", por lo que ha considerado que necesitamos herramientas adaptaras para contrarrestarla. Paralelamente, ha abogado por promover la colaboración público-privada, la inteligencia financiera y la ciberinteligencia a fin de disponer de nuevos guerreros económicos. Igualmente, "*necesitamos una defensa europea común mediante la creación de unas fuerzas armadas y un plan de defensa comunitario a nivel coyuntural"*.

En la misma línea se ha dirigido **Rosa Kariger**, Global Security Analysis & Prospective en Iberdrola, que ha asegurado que "*no existe un regulador común de la UE en el ciberespacio que proteja o haga frente a múltiples ciberataques*" por lo que resulta vital contar con una coordinación europea. *"La UE tiene un papel importante para garantizar que podamos operar en un ciberespacio más seguro y democrático*", ha dicho.

Gobiernos inmaduros para la gestión de la cibercrisis

"*Los gobiernos están muy acostumbrados a administrar crisis de reputación. Pero, ¿gestionan también las cibercrisis? La respuesta es que no*". Así de tajante se ha mostrado **Iván Monforte**, responsable de Comunicación, Ecosistema y Cultura de Ciberseguridad en la Agencia de Ciberseguridad de Cataluña, durante su intervención en DES. Monforte ha recordado cómo en marzo de 2023, el segundo hospital más grande de Cataluña sufrió un ciberataque de ransomware que obligó a desviar a las ambulancias a centros sanitarios cercanos.

En este contexto, ha revelado la importancia de no lidiar solo la incidencia a nivel de ciberseguridad, sino también de notoriedad. "*Hay que gestionarlo entre el CEO y el equipo de comunicación, que puede entender cómo actuarán los medios y cómo se publicará la información sobre la ofensiva*". El representante del organismo catalán ha considerado esencial actuar con celeridad a fin de obtener liderazgo: "*Tienes que analizar el 'storytelling' del grupo de hackers y publicar tu propia historia más rápido que ellos. Si no, tienes que luchar contra su falso relato y convencer a la gente de que crea el tuyo*".

De la misma opinión se ha mostrado **José Andrés Jiménez**, Jefe del Departamento de Asesoramiento Técnico TIC en el Congreso de los Diputados, que ha reconocido que "*el gobierno español no tiene una estrategia de gestión de cibercrisis muy madura. El panorama está cambiando mucho ahora. Ya no son sólo los hackers, también hay actores patrocinados por el Estado que pueden causar incidentes cibernéticos. Es necesario contrarrestar su narrativa, ya que son activos en las redes sociales*".

En este aspecto, ha señalado que el ejecutivo español está construyendo, a corto plazo, una estrategia de gestión cibernética. *"No tenemos los medios para mantener una defensa a largo plazo contra el equivalente de un ejército extranjero a las puertas. Así que necesitan ayuda de instituciones como la Agencia Catalana de Ciberseguridad*", ha indicado.

Un plan B tecnológico y opción analógica como protección

Ante la creciente escalada de ciberataques, **Rosa Kariger**, Global Security Analysis & Prospective en Iberdrola, ha abierto el debate sobre la necesidad de contar con un plan B para securizar la información y sistemas de las empresas, en especial en un momento importante de migración de los servicios e información a la nube. Por su parte, **Jesús Mérida**, Chief Information Security Officer de Iberia, ha valorado como solución distintas actuaciones que llevan a cabo muchas empresas. "*Están realizando backups en tecnologías muy diversas que no se puedan ver afectadas por la misma tecnología, o tener incluso parte de sus servicios e información en recursos físicos que aseguren su mantenimiento ante cualquier suceso".*

Registro de prensa: Completa el siguiente formulario con tus datos para solicitar tu pase

***

Sobre DES | Digital Enterprise Show (11-13 junio 2024, FYCMA, Málaga): DES – Digital Enterprise Show es un evento de Nebext – Next Business Exhibitions en colaboración con el Ayuntamiento de Málaga y la Junta de Andalucía. En siete ediciones, se ha convertido en el mayor evento profesional europeo sobre tecnologías exponenciales y uno de los referentes mundiales que ofrece a la alta dirección de las empresas las últimas soluciones y productos para acompañar a las grandes corporaciones, a Pymes y a las Administraciones Públicas europeas hacia la transformación digital. Durante 3 días, combinamos tecnología e innovación con liderazgo digital, soluciones tecnológicas para mejorar la experiencia de cliente y del empleado, optimización de los procesos operacionales y la identificación de nuevos modelos de negocio, servicios y productos de todas las industrias.