Cyber Europe 2018 – Preparación para la próxima cibercrisis

ENISA, la agencia de ciberseguridad de la UE, ha organizado un ejercicio internacional de ciberseguridad

Imagine que es un día normal en el aeropuerto. De repente, las máquinas de facturación automática indican un fallo del sistema. Las aplicaciones de viaje de los móviles dejan de funcionar. En los mostradores de facturación, los empleados no pueden acceder a sus ordenadores. Los viajeros no pueden facturar equipaje ni atravesar los controles de seguridad. Se forman colas interminables en todas partes. Las pantallas del aeropuerto anuncian todos los vuelos como anulados. Por motivos desconocidos, la recogida del equipaje ha dejado de funcionar, y más de la mitad de los vuelos se queda en tierra.

Parece ser que un grupo de radicales ha tomado el control de los sistemas esenciales del aeropuerto mediante ataques digitales e híbridos. Ya han reivindicado el incidente y utilizan sus canales de propaganda para difundir un llamamiento a la acción y atraer a más personas a sus ideologías radicales.

Esta es la potente hipótesis a la que se enfrentaron más de 900 especialistas europeos en ciberseguridad de 30 países los días 6 y 7 de junio de 2018 durante el «Cyber Europe 2018» (CE2018), el ejercicio más avanzado de ciberseguridad en la UE hasta la fecha.

La ENISA había preparado estas jornadas en su sede en Atenas (Grecia), y los especialistas participaron desde su puesto de trabajo habitual o juntándose en células de crisis. La ENISA dirigió el ejercicio gracias a su plataforma de ejercicios de ciberseguridad, construyendo un «universo virtual» (entorno integrado) para ese mundo simulado, con material sobre el incidente, sitios web de noticias, canales de redes sociales, blogs de seguridad y sitios web de empresas de seguridad.

El Cyber Europe 2018, organizado por ENISA, la agencia de ciberseguridad de la UE, en colaboración con las autoridades y agencias de ciberseguridad de toda Europa, perseguía que los expertos europeos en ciberseguridad reforzaran sus capacidades de identificar y combatir amenazas a gran escala, y que comprendieran mejor el fenómeno de contagio de incidentes transfronterizos.

Y lo que es más importante, contribuyó a que las organizaciones pusieran a prueba sus planes de continuidad de las actividades y de gestión de crisis, incluida la comunicación a los medios en caso de crisis, reforzando al mismo tiempo la cooperación entre entidades públicas y privadas.

El ejercicio contenía incidentes técnicos y no técnicos, inspirados en la vida real, que exigían análisis de redes y de programas maliciosos, análisis forenses y esteganografía. Estos incidentes estaban concebidos para que provocaran crisis a todos los niveles posibles: en cada organización y a escala local, nacional y europea.

Mariya Gabriel, comisaria de Economía y Sociedad Digitales, ha afirmado: «La tecnología ofrece un sinfín de posibilidades en todos los sectores de nuestra economía, pero también presenta riesgos para las empresas y los ciudadanos. La Comisión y los Estados miembros tienen que cooperar y dotarse de los instrumentos necesarios para detectar los ciberataques y proteger las redes y los sistemas. Para eso se creó hace ocho años el ejercicio “Cyber Europe” de la ENISA, que se ha convertido en un importante ejercicio de ciberseguridad y acto emblemático de la UE, en el que confluyen cientos de especialistas en

ciberseguridad de toda Europa. Debemos aprovechar este éxito y seguir desarrollando los mecanismos de cooperación de la UE, en particular para hacer frente a ciberincidentes a gran escala».

El profesor Dr. Udo Helmbrecht, director ejecutivo de la ENISA, ha declarado: «En los últimos diez años, el sector de la aviación ha realizado un enorme salto tecnológico, sector en evolución constante. Ahora disponemos de facturación por internet, aplicaciones de navegación y control automatizado de equipajes. Con la tecnología inteligente ganamos tiempo, ahorramos dinero y se hace más fácil la vida de los viajeros. No obstante, al igual que la tecnología avanza, también lo hacen amenazas cibernéticas. Con ejercicios como "Cyber Europe 2018", nuestra agencia refuerza el nivel de ciberseguridad en la Unión. Países y organismos europeos que trabajan juntos como una única entidad: esa es la respuesta moderna a las amenazas cibernéticas sin fronteras. En nombre de la ENISA y su personal, felicito a todos los implicados en el Cyber Europe 2018».

En definitiva, los participantes pudieron mitigar los incidentes de manera oportuna y eficaz. Esto demuestra que el sector europeo de la ciberseguridad ha evolucionado en estos últimos años y que sus actores están mucho más preparados. La ENISA y los participantes procederán en breve al seguimiento del ejercicio y analizarán las acciones emprendidas, a fin de determinar qué ámbitos podrían mejorarse. Después, la ENISA publicará un informe final.

En síntesis

Países participantes: 30, Austria; Bélgica; Bulgaria; Croacia; Chipre; Chequia; Dinamarca; Estonia; Finlandia; Francia; Alemania; Grecia; Hungría; Irlanda; Italia; Letonia; Lituania; Luxemburgo; Malta; Países Bajos; Noruega; Polonia; Portugal; Eslovaquia; Rumania; Eslovenia; España; Suecia; Suiza; Reino Unido.

Organizaciones participantes: 300

Número de participantes: más de 900 profesionales de ciberseguridad

Número de tareas: 23 222

Sobre los ejercicios Cyber Europe

Los ejercicios de «Cyber Europe» son simulaciones de incidentes de ciberseguridad de gran envergadura que pueden llegar a generar crisis cibernéticas a escala de la UE. Permiten analizar incidentes de ciberseguridad avanzados y hacer frente a situaciones complejas de continuidad de las actividades y de gestión de crisis. La ENISA ya había organizado cuatro ejercicios paneuropeos en la materia: en 2010, 2012, 2014 y 2016.

La cooperación internacional entre todas las organizaciones involucradas es inherente al juego, en el que participa la mayor parte de los países europeos. Se trata de una experiencia de aprendizaje flexible: desde un analista solo hasta toda una organización, y con opciones de sumarse o de retirarse, los participantes pueden personalizar el ejercicio en función de sus necesidades.