El mayor ejercicio de ciberseguridad jamás realizado, hoy en Europa.

@Enisa_EU #CyberSecurity #CyberEurope2014

Más de 200 organizaciones y 400 profesionales del sector de la ciberseguridad provenientes de 29 países europeos ponen a prueba su capacidad para responder a ciberataques en un ejercicio de simulación de un día entero de duración que ha organizado la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA). En Cyber Europe 2014, expertos tanto del sector público como del privado, entre los que se incluyen agencias de ciberseguridad, equipos de respuesta a emergencias informáticas nacionales, ministerios, compañías de telecomunicaciones, instituciones financieras y proveedores de servicios de Internet, ponen a prueba sus propios procedimientos y capacidades en un escenario simulado de ciberseguridad a gran escala.

#CyberEurope2014 es el ejercicio más complejo y de mayor envergadura jamás organizado en Europa. Se tratarán más de 200 ciberincidentes diferentes, como ataques de denegación de servicio a servicios en línea, informes de inteligencia y de medios de comunicación sobre operaciones de ciberataques, deformaciones de sitios Web (ataques que modifican la apariencia de un sitio Web), exfiltraciones de información sensible, ataques contra infraestructuras críticas, como redes de telecomunicaciones o energéticas, y la verificación de los procedimientos de cooperación y escalación de la UE. La realización del ejercicio está distribuida por varios centros de ejercicios de toda Europa bajo la coordinación de un centro de control de ejercicios.

La Vicepresidenta de la Comisión Europea @NeelieKroesEU afirmó: “La sofisticación y el volumen de los ciberataques aumentan cada día. Resultará imposible responder a ellos si los Estados trabajan cada uno por su cuenta, o si tan solo unos cuantos actúan de manera conjunta. Me complace que los Estados miembros de la UE y de la AELC estén trabajando con las instituciones de la UE bajo la coordinación de ENISA. Solo con este tipo de esfuerzos comunes seremos capaces de mantener protegidas la sociedad y la economía actuales”.

El profesor Udo Helmbrecht, Director Ejecutivo de ENISA, comentó: “Hace cinco años que no había procedimientos que pudieran guiar la cooperación entre la UE y sus Estados miembros durante una cibercrisis. Hoy disponemos de procedimientos colectivos para mitigar las cibercrisis a nivel europeo. El resultado del ejercicio de hoy nos dirá dónde nos encontramos e identificará los próximos pasos a dar para continuar mejorando”.

Entre otros aspectos, el ejercicio #CyberEurope2014 pondrá a prueba procedimientos de verificación para compartir información operativa sobre cibercrisis en Europa, mejorará las capacidades nacionales de respuesta a las cibercrisis y explorará los efectos de los intercambios de información múltiples y paralelos entre los sectores privado-público y privado-privado, tanto a nivel nacional como internacional. El ejercicio también pondrá a prueba los Procedimientos de Operación Estándar de la UE (EU-SOP, por sus siglas en inglés), un conjunto de directrices pensadas para compartir información operativa sobre cibercrisis.

Contexto

Según el informe Panorama de Amenazas (2013) de ENISA, los creadores de las amenazas han aumentado la sofisticación de sus ataques y herramientas. Si una cosa ha quedado clara es que la madurez en el campo de las ciberactividades no es cuestión exclusiva de unos cuantos países, sino que son varios los países que han desarrollado capacidades que pueden utilizarse para infiltrarse en todo tipo de objetivos, tanto gubernamentales como privados, con el fin de conseguir sus metas.

En 2013, los ataques a la red a nivel global se vieron incrementados en casi una cuarta parte, mientras que el número total de violaciones de datos fue un 61% más elevado que en 2012. Las ocho violaciones principales provocaron la pérdida de decenas de millones de datos y la exposición de 552 millones de identidades. Según estimaciones del sector, en 2013 la ciberdelincuencia y el espionaje fueron responsables de unas pérdidas de entre 300 billones y 1 trillón de dólares estadounidenses a nivel mundial.

El ejercicio

Este ejercicio simula crisis a gran escala relacionadas con las infraestructuras de información crítica. Una vez haya finalizado el ejercicio, expertos de ENISA presentarán un informe con las principales conclusiones.

#CyberEurope2014 es un ejercicio bianual de ciberseguridad a gran escala. ENISA lo organiza cada dos años y este año cuenta con la participación de 29 países (26 de la UE y 3 de la AELC), además de instituciones de la UE. Se lleva a cabo en 3 fases a lo largo de todo un año: la fase técnica, que implica la detección, la investigación, la atenuación y el intercambio de información sobre incidentes (finalizada en abril); la fase táctico-operativa, dedicada a las alertas, la evaluación de las crisis, la cooperación, la coordinación, los análisis tácticos y el intercambio de consejos e información a nivel operativo (actualmente y hasta 2015); y la fase estratégica, que examina la toma de decisiones, el impacto político y los asuntos públicos. Este ejercicio no afectará a las estructuras, los sistemas o los servicios de información crítica.

30/10/2014

www.enisa.europa.eu

En la Estrategia de Ciberseguridad de la UE y la propuesta de Directiva para un elevado nivel común de seguridad de las redes y de la información (NIS, por sus siglas en inglés), la Comisión europea ha reclamado el desarrollo de ejercicios periódicos y de planes nacionales de contingencia que permitan poner a prueba la capacidad de respuesta y de recuperación a gran escala de las redes en caso de desastre por incidentes de seguridad. El nuevo mandato de ENISA también destaca la importancia de los ejercicios de preparación en el campo de la ciberseguridad para mejorar la fiabilidad y la confianza en los servicios en línea en toda Europa. Los borradores de los procedimientos EU-SOPs se han puesto a prueba a lo largo de los últimos tres años, incluso con ocasión del CE2012.

Enlaces de utilidad

La ciberseguridad en la Agenda Digital

Ejercicios de cibercrisis de ENISA

Carpeta de información de ENISA sobre el CE2014

Nota de prensa sobre el Ejercicio de nivel técnico del CE2014: TLEx

Neelie Kroes – Siga a Neelie en Twitter

Contactos

Correo electrónico: comm-kroes@ec.europa.eu, c3e@enisa.europa.eu

Tel. +32.229.57361 Twitter: @RyanHeathEU, @enisa_eu