Unidos somos más Fuertes: ENISA lanza el informe concluyente de Cyber Europe 2014

ENISA lanza hoy la edición pública del informe concluyente del ejercicio de ciberseguridad paneuropea Cyber Europe 2014 (CE2014). Este informe, aprobado por los Estados miembros, ofrece una visión de alto nivel acerca del complejo ejercicio de ciberseguridad que se llevó a cabo en 2014.

El objetivo principal de Cyber Europe 2014 era formar a los Estados miembros para cooperar en un escenario de cibercrisis. El ejercicio, dividido en tres fases, proporcionó oportunidades para evaluar la efectividad de la cooperación y los procedimientos escalables durante los ciberincidentes transfronterizos que afectan a la seguridad de los servicios vitales y la infraestructura, mientras que se someten a prueba las capacidades nacionales y planes de contingencia que involucran a organizaciones del sector público y privado.

El ejercicio, que ENISA organiza con carácter semestral, se planificó de manera conjunta con representantes de los países involucrados y requirió seis (6) reuniones de planificación en Europa. Este ejercicio, que reunió a más de **1.500 participantes** de **29 Estados miembros de la UE y la AELC**, cubrió **por primera vez las tres (3) fases** de respuesta a un ciberincidente (técnica, operativa y estratégica), desembocando cada una en la etapa posterior. Resumen de aspectos esenciales:

- Fase 1 – Nivel técnico (28-30 de abril de 2014, **49 horas**): Detección, análisis y mitigación de incidentes, intercambio de información.
- Fase 2 – Nivel operativo (30 de octubre de 2014, **10 horas**): Alerta, cooperación, mitigación de crisis a corto plazo y desarrollo de un planteamiento común.
- Fase 3 – Nivel estratégico – **Sometido a prueba por primera vez** - (25 de febrero de 2015): Toma de decisiones basada en un planteamiento común de la situación, debates políticos de alto nivel sobre la mitigación de crisis estratégicas a largo plazo.

El informe muestra que la habilidad común para atenuar los incidentes de ciberseguridad a gran escala en Europa ha progresado de manera significativa desde 2010, cuando se realizó el primer ejercicio Cyber Europe. La transmisión de datos en tiempo real entre los países está demostrando su utilidad a la hora de tomar decisiones con rapidez. Los **Procedimientos Estándar Operativos** de la UE (UE-SOPs) se emplean para respaldar estas actividades de cooperación y facilitan a los Estados miembros directrices que estos pueden utilizar para afrontar incidentes de ciberseguridad a gran escala. Estas actividades seguirán mejorándose considerando el contexto en evolución de la política de ciberseguridad en Europa.

La cooperación destacó como elemento clave que contribuye a aumentar el entendimiento, construir confianza y elaborar una respuesta más rápida. La **Plataforma Cibernética de Ejercicio** (CEP por sus siglas en inglés) desarrollada por ENISA para planificar, dirigir y evaluar los ejercicios ha demostrado ser una herramienta muy útil. ENISA continúa desarrollando la CEP en la actualidad con el fin de albergar futuros ciberejercicios y situaciones técnicas. El noventa y ocho por ciento (98%) de los participantes de la fase técnica mostraron interés para tomar parte en el siguiente ejercicio.

El Director Ejecutivo de ENISA, Udo Helmbrecht, *afirmó: "Las lecciones aprendidas de Cyber Europe 2014 son numerosas y aportan la base para un trabajo innovador en el ámbito de la cooperación en cibercrisis, un campo emergente que la UE y ENISA están dirigiendo. Estamos comprometidos a implementar el plan de acción con el apoyo de los Estados miembros para continuar mejorando la preparación ante una crisis cibernética, tanto a escala nacional como comunitaria."*

El escenario

El escenario de Cyber Europe 2014 se centró en la propuesta de regulación europea vinculada a los **recursos energéticos.** Durante la fase técnica del ejercicio, los Estados miembros y las instituciones europeas tuvieron que lidiar con **ciberincidentes** como la **exfiltración de información**, inteligencia de fuente abierta y análisis de ***malware*** de teléfonos móviles para **rechazar** ataques **de servicio** y **continuas amenazas avanzadas**. La fase operativa de Cyber Europe 2014 está relacionada con la escalada de la situación que condujo a una serie de **ataques cibernéticos a gran escala** en diversas infraestructuras fundamentales y numerosos servicios online. Finalmente, la fase estratégica de Cyber Europe 2014 intensificó más la crisis con varias infraestructuras energéticas seriamente afectadas en medio de un duro invierno, tecnologías críticas vulneradas y una opinión pública cada vez más preocupada.

Para acceder al informe completo

Para echar un rápido vistazo a Cyber Europe, visualice el siguiente vídeo de ENISA:

https://www.enisa.europa.eu/media/news-items/preparing-for-the-unknown-a-peek-into-cyber-europe

Para entrevistas y solicitudes de prensa:

Ponerse en contacto con la **Cooperación de Crisis Cibernéticas**: c3@enisa.europa.eu