

CNPIC participa como planificador en el primer ejercicio conjunto de ciberseguridad

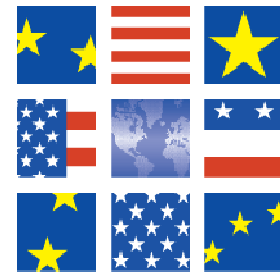
El pasado día 3 de noviembre de 2011 tuvo lugar en Bruselas el desarrollo de un ejercicio de ciberseguridad en el que participaron por primera vez los Estados Miembros de la Unión Europea y los Estados Unidos, con el soporte de la Agencia Europea de Seguridad de las Redes y la Información (ENISA) y el Departamento de Seguridad Interior de los EEUU (Department of Homeland Security – DHS).

El ejercicio, denominado como Cyber Atlantic 2011, tenía por objetivo la simulación de escenarios de ciber-crisis que permitiesen a los participantes explorar los modos en que la UE y los EEUU podrían coordinarse de cara a proveer los oportunos mecanismos de cooperación, en situaciones concretas de ciberataques deliberados dirigidos a sus infraestructuras críticas.

El Cyber Atlantic 2011 se ha desarrollado con la participación activa de cuatro organismos españoles. La delegación española, compuesta por instituciones con un rol importante en materia de ciberseguridad a nivel nacional, estuvo liderada por el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) del Ministerio del Interior, que representó a nuestro país como planificador del ejercicio, quedando completada por representaciones del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis (DISSC) de la Presidencia del Gobierno, el Centro de Respuesta a Incidentes de Seguridad para las Administraciones Públicas (CCN-CERT) del Centro Nacional de Inteligencia, y el Centro de Respuesta a Incidentes de Seguridad de INTECO (INTECO-CERT) del Ministerio de Industria, Turismo y Comercio.

El ciberejercicio contó con el apoyo de la Agencia Europea para la Seguridad de las Redes y la Información (ENISA) y del departamento estadounidense de Seguridad Nacional (DHS acrónimo del inglés Department of Homeland Security). En concreto, el ejercicio se dividió en la aplicación de dos escenarios diferenciados:

En el primer supuesto se recreó un ciberataque APT (Amenaza Persistente Avanzada) que, de forma secreta, trata de filtrar y publicar en la Red información confidencial perteneciente a agencias de seguridad de gobiernos de los distintos Estados miembros de la UE. En el ciber-ejercicio un grupo de hackers consiguieron, a través de técnicas



**CYBER
ATLANTIC
2011**

sofisticadas, acceder a información clasificada de estas agencias europeas. Los distintos Estados miembros debían colaborar conjuntamente en la mitigación de este incidente y, a su vez, coordinarse con EEUU que podía estar también afectado.

El segundo escenario se centró en un fallo en sistemas de supervisión y control (SCADA) en centrales de generación de energía eólica en varios Estados miembros de la UE, producido por un ataque cibernético. El hecho de que estos sistemas SCADA se utilicen en la gestión de múltiples infraestructuras críticas y que un porcentaje importante de estos sistemas sean de fabricantes americanos, hace fundamental una coordinación y colaboración internacional entre los Estados miembros y EE.UU., para mitigar este tipo de ciberataques.

Más de 20 Estados Miembros han participado en el ejercicio, 16 de ellos de forma activa como jugadores, siendo la Comisión Europea la encargada de proporcionar la dirección de alto nivel. Cyber Atlantic 2011 es parte del compromiso de cooperación en materia de ciberseguridad adquirido por la Unión Europea y los Estados Unidos en la cumbre de Lisboa del 20 de noviembre de 2010¹ y también uno de los resultados obtenidos de la reunión del G-6 y Estados Unidos celebrada pasado mes de febrero en Cracovia, en la que se abordó la puesta en marcha de nuevas medidas para luchar contra la ciberdelincuencia y la creación de una plataforma virtual. El entonces Secretario de Estado de Seguridad, Antonio Camacho, justificó en aquel momento la iniciativa en la necesidad de cambiar los métodos tradicionales de trabajo para garantizar la seguridad en la Red y, a la vez, poner en marcha un sistema global para hacer frente a una amenaza global. Para ello, el trabajo conjunto y el intercambio de información en tiempo real, como el que se ha trabajado en Cyber Atlantic 2011, es imprescindible.

El ejercicio se basó en las lecciones aprendidas en el primer ejercicio pan-europeo de ciberseguridad, denominado Cyber Europe 2010², que tuvo lugar en noviembre de 2010, donde España estuvo también representada a través del CNPIC.

El principal objetivo de este ciberejercicio fue el abordar las nuevas amenazas que conllevan las redes globales, puesto que la prosperidad y la seguridad de nuestras sociedades cada vez dependen en mayor medida de dichas redes. Actualmente todas las infraestructuras críticas que garantizan el funcionamiento cotidiano de los servicios esenciales (energía, comunicaciones, transportes, finanzas...) dependen de las redes informáticas, cuya seguridad es imposible garantizar de manera individual por cada país. Esta realidad hace que las medidas nacionales sean insuficientes, por lo que es

¹ Los objetivos de este acuerdo son “abordar las nuevas amenazas a las redes globales, sobre las que la seguridad y la prosperidad de nuestras sociedades libres dependen cada vez más”: Joint Statement, EU-US Summit, November 2010.

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/117897.pdf

² ENISA Cyber Europe 2010 exercise reports: <http://www.enisa.europa.eu/act/res/ce2010>

esencial impulsar mecanismos internacionales eficaces que faciliten el trabajo en la Red.

Las lecciones aprendidas de este ejercicio Cyber Atlantic 2011 servirán de base para el desarrollo de posibles futuros ciber-ejercicios entre la UE y los EEUU.

Centro Nacional para la Protección de Infraestructuras Críticas - www.cnpic.es