La compartición ágil, confiable y de calidad, protagonista de la IX JORNADA STIC CCN-CERT, que registró 1.400 asistentes

Con el lema "Detección e Intercambio, factores clave", el **Centro Criptológico Nacional** (CCN) celebró los pasados 10 y 11 de diciembre la novena edición de las Jornadas STIC CCN-CERT que, este año, congregó a cerca de 1.400 profesionales en Madrid, entre los cuales se encontraban representados cerca de 400 organismos públicos y más de 200 empresas.

Desde la sesión de inauguración, que corrió a cargo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, **Víctor Calvo Sotelo**, el Jefe del Estado Mayor de la Defensa, **Fernando García Sánchez** y el Secretario de Estado y Director General del Centro Nacional de Inteligencia, **Félix Sanz**, el seminario se convirtió en un espacio de debate y reflexión sobre los riesgos asociados a las nuevas tecnologías y, en especial, sobre la capacidad de respuesta que posee en este sentido nuestro país. Desde esta perspectiva, el CCN reflexionó sobre los desafíos a los que se enfrenta el CERT Gubernamental Nacional y, en general, el conjunto de los agentes involucrados en la ciberseguridad de España, concerniendo tanto a organizaciones públicas, como a empresas privadas y ciudadanos. Dichos retos pasan por la detección como primer factor clave en la contención de los ciberataques y la mejora continua en el intercambio de información en la materia. En este sentido, el CCN alegó, no en vano, que en 2015 se registraron 18.653 incidentes de seguridad, de los cuales, la gran mayoría se catalogaron con un nivel de riesgo alto o muy alto. Dicha cifra correspondía nada menos que a un 44% de incremento en el número de incidentes respecto a 2014.

Ante dicha escalada de ataques cibernéticos, el CCN aprovechó para presentar algunas novedades en su cartera de servicios. Entre ellas, se destacó, por un lado, el marco técnico conocido como REYES, cuyo gran reto para este año es depurar este sistema con el objetivo de que se convierta en un sistema más ágil en el que exista una mayor confianza y reciprocidad a la hora de intercambiar dicha información. Y, por otro, la actualización a la versión 2.0 del Servicio de Alerta Temprana (SAT) cuya finalidad es permitir analizar en tiempo real una mayor cantidad de información de forma simultánea sobre de los riesgos e incidentes existentes en el tráfico que fluye entre la red interna del Organismo.

La realidad actual

Tras las sesiones iniciales, el evento contó con varias sesiones simultáneas en las que se abordaron los temas más candentes del panorama de la ciberseguridad actual, como son el ciberespionaje, el cibercrimen en Rusia, las amenazas persistentes avanzadas (APTs), las nuevas vulnerabilidades en los sistemas operativos Android e iOS, la seguridad en Internet de las Cosas, los ciberataques detectados en los nuevos sistemas de pago, los peligros cibernéticos en los sistemas de información de las Ciudades Inteligentes. Al tiempo se realizó una muy completa presentación de la actualización del Esquema Nacional de Seguridad (ENS).

Llamada a la acción

Luis Jiménez, subdirector adjunto del CCN –convertido actualmente en una Subdirección del CNI– se encargó de clausurar dos días intensos de unas jornadas que finalizaron con un mensaje claro: la necesidad de empezar a cimentar las bases para la construcción de nuevas iniciativas y fórmulas de coordinación y cooperación público-privada, especialmente, a través del intercambio fiel de información con el objetivo de conseguir una seguridad cibernética más eficaz y eficiente en España.

MESA REDONDA

¿Qué está dispuesto a compartir el sector industrial de ciberseguridad privada con las estructuras oficiales de cibervigilancia?

La importancia que tiene el tipo de información que deberían intercambiar las administraciones públicas y los proveedores de productos y servicios de seguridad para mejorar la protección ante potenciales ataques fue el *leitmotiv* de la segunda mesa redonda que se celebró en la recta final de las jornadas. Bajo la batuta de **Luis Fernández**, Editor de la revista SIC, el debate contó con la participación de **Jorge Uyá** (InnoTec System), **Héctor Sánchez** (Microsoft), **José Miguel Rosell** (S2 Grupo), **Javier Santos** (KPMG), **Tony Hadzima** (Palo Alto) y **David Fernández** (Symantec). Los participantes destacaron la importancia de compartir información respetando la privacidad y sensibilidad de la misma, así como favorecer la agilidad y la calidad de dichos datos, por encima de la cantidad. Asimismo, los ponentes coincidieron en la idoneidad de crear de una regulación que estimule, ampare y obligue a compartir este tipo de información y que garantice su trazabilidad, establecimiento un marco formal del que todos los implicados puedan beneficiarse.

MESA REDONDA

Futuro desarrollo reglamentario de la Ley de Seguridad Privada en la contratación pública de servicios de ciberseguridad

Con una breve introducción de **José de la Peña**, Director de la revista SIC, como moderador, comenzaba esta mesa redonda que contó con la participación de **Esteban Gándara** (CNP), **Nacho García** (HPE), **Óscar Pastor** (Isdefe), **Román Ramírez** (Rooted CON), y **Concha Hortigüela** (GISS) para debatir sobre el posible desarrollo normativo previsto en la Ley de Seguridad Privada –en la que se considera la seguridad informática no como una actividad de seguridad privada sino como una actividad compatible con la misma– y su incidencia en la contratación pública de servicios de ciberseguridad.

Gándara, Comisario Jefe de la Unidad Central de Seguridad Privada de la Policía Nacional, abrió la sesión dando una breve explicación sobre el estado de esta futura reglamentación, que se encuentra en fases preliminares de su gestación. Tras su exposición, no exenta de polémica, el resto de los ponentes reflexionaron en torno a las implicaciones que esta futura Ley podría tener en sus respectivas áreas como representantes tanto de organismos públicos como de la empresa privada y del universo *hacker*, sin llegarse a establecerse una conclusión unísona y dejando abierto un nuevo debate a futuro.