El CCN-CERT, en su calidad de CERT Gubernamental español, reúne en Madrid a los principales expertos en ciberseguridad del país

Más de 500 asistentes confirman el éxito de las VI Jornadas STIC CCN-CERT centradas en la defensa frente a las APT y la colaboración público-privada

La gestión de incidentes, los agentes implicados en el ciberespionaje, la persistencia de un APT, su funcionamiento y cómo reaccionar ante este tipo de amenazas que ponen en peligro la información más valiosa de las AAPP y de las empresas, fueron algunos de los temas abordados en las VI Jornadas STIC CCN-CERT, que bajo el lema "*La gestión de la ciberseguridad en las Administraciones Públicas*", se celebraron los pasados 11 y 12 de diciembre de 2012 en el Auditorio de la Fábrica Nacional de la Moneda y Timbre, en Madrid. El contenido de lo presentado, la afluencia de público –con más de 500 asistentes– y la calidad y conocimiento de los ponentes avalaron estas jornadas, inauguradas por el Secretario de Estado-Director del CNI, Félix Sanz, acompañado en el acto por el Presidente de la entidad antifriona, Jaime Sánchez Revenga.

Jaime Sánchez Revenga (FNMT) y Félix Sanz (CNI), durante el acto inaugural.

Participantes en el debate, moderado por José de la Peña (SIC).

Si hay algo que preocupa al Centro Criptológico Nacional, **CCN**, y su Capacidad de Respuesta a Incidentes, **CCN-CERT**, es la proliferación de ataques dirigidos o APTs y el robo de información sensible que afectan de modo creciente a la Administración Pública y a las empresas estratégicas españolas. Por este motivo, las VI Jornadas STIC CCN-CERT centraron buena parte de su contenido en este tipo de amenazas, catalogadas como críticas, cada vez más frecuentes y más difíciles de detectar. Lo atinado de su contenido concitó la nutrida asistencia de responsables de la protección de los sistemas TIC de la Administración y de las empresas pertenecientes a los sectores designados como estratégicos.

La colaboración público-privada, a escena

El evento, que reunió a significados expertos en materia de ciberseguridad del país, abordó también un debate de gran actualidad, conducido por el director de **SIC**, **José de la Peña**, centrado en las pautas de colaboración entre los CERTs, las organizaciones usuarias y los MSSP, así como el intercambio de información entre las partes, particularmente en ataques complejos como las APTs.

El animado y clarificador debate evidenció los diversos enfoques y sensibilidades de las compañías y organismos participantes: **CCN-CERT (Carlos Abad)**, **CESICAT (Tomás Roy)**, **Ecija (Israel Córdoba)**, **Grupo BBVA (Carlos Pérez)**, **INTECO (Marcos Gómez)**, y **Telefónica (Carlos Olea)**. Durante el transcurso de la mesa redonda, los panelistas pusieron sobre el tapete los ámbitos más viables y factibles para la colaboración público-privada (CPP), si bien afloraron también opiniones bastante divergentes en lo relativo a la colisión de atribuciones y ámbitos de actuación competencial a la hora de su delimitación y alcance. En todo caso, la totalidad de los participantes subrayó el propósito constructivo de encauzar esta necesidad dando pasos viables, para lo cual enumeraron diferentes ejemplos concretos que reflejan históricamente la decidida voluntad de cooperación en este asunto tan crítico.

La evolución del ENS

Las acciones realizadas para facilitar la aplicación del **Esquema Nacional de Seguridad**, **ENS**, y su nivel de cumplimento, así como una serie de ponencias sobre los desafíos que plantean las nuevas tecnologías y sus diferentes usos (nube, redes sociales, ciberactivismo, Bluetooth, dispositivos móviles…) completaron el programa de este evento.

Particularmente, y en lo que concierne al ENS en 2013, se mencionó el seguimiento mensual del estado de cumplimiento que realizará la Comisión Permanente del Consejo Superior de Administración Electrónica y el seguimiento trimestral por la Comisión de Subsecretarios, al tiempo que se informó de la creación del Comité de Seguridad de la Información de las AAPP. También se evidenciaron dos acciones: la primera, a realizar durante el primer trimestre del presente, que consistirá en la elaboración de un informe del estado de la seguridad en la AGE y en las CCAA; y la segunda, centrada en el emprendimiento de acciones para modificar el Real Decreto del ENS, en concreto su Artículo 35 y el Anexo II, entre otros.

Además de con la **Revista SIC**, las jornadas contaron con la colaboración especial y el patrocinio de compañías de referencia en materia de ciberseguridad: **TB-Security-Incita, Corero, Autek, Deloitte, HP, Innotec, Tecnobit, AlienVault, Ecija, IBM, Ingenia, Isdefe, Realsec, S2 Grupo, S21sec** y **Safenet**.