Responsables de seguridad TIC de la Administración y gestores de Infraestructuras Críticas, asisten al evento inaugurado por la Secretaria General del CNI, Elena Sánchez

Más de 400 asistentes en las V Jornadas STIC CCN-CERT, celebradas bajo el lema: *La Ciberseguridad, un reto para las Administraciones Públicas*

- **La Gestión de Incidentes y la coordinación entre todos los Equipos de Respuesta públicos, la implantación del Esquema Nacional de Seguridad (ENS) y la protección de las Infraestructuras Críticas de los ciberataques, fueron los principales temas que vertebraron las ponencias y los debates de las Jornadas**

- **El CERT Gubernamental español ofreció un breve resumen de los últimos servicios incorporados, entre los que destacaron el desarrollo de 14 guías para la implantación del ENS, un piloto de la herramienta CARMEN enfocada a detectar anomalías en el tráfico de navegación o la incorporación de nuevas funcionalidades en su Sistema de Alerta Temprana, en el que ya están implantadas más de 65 sondas (entre la red SARA e Internet)**

Madrid, 22 de diciembre de 2011. Más de cuatrocientas personas asistieron a las V Jornadas STIC CCN-CERT organizadas por la Capacidad de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT), adscrito al Centro Nacional de Inteligencia (CNI) y celebradas en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), en Madrid, durante los días 13 y 14 de diciembre.

Las jornadas, celebradas bajo el lema ***"La ciberseguridad: un reto para las Administraciones Públicas"***, fueron inauguradas por la Secretaria General del CNI, Elena Sánchez Blanco, que resaltó el éxito de esta convocatoria que durante cinco años consecutivos, *se ha convertido en un referente en materia de seguridad de la información en nuestro país, y un punto de encuentro ineludible para todos los responsables de seguridad de la Administración pública*. Blanco prosiguió su intervención asegurando que *la experiencia de más de cinco años del **CCN-CERT** encargado de velar por la seguridad de los sistemas de toda la Administración, ratifica la necesidad de contar con una visión global* frente a las ciberamenazas *que incluya medidas tanto preventivas como reactivas, capaces de reaccionar ante el constante incremento de incidentes y, sobre todo, que prevengan su propagación y atajen su impacto de la forma más rápida posible. Para ello, resulta fundamental potenciar las capacidades de monitorización y alerta temprana, fortalecer la gestión y respuesta a incidentes e impulsar las políticas comunes de seguridad*.

La Secretaria General se congratuló de que alguna de estas medidas se hayan ido adoptando en los últimos años, citando la propia creación del **CCN-CER**T, en el año 2006 y de su Sistema de Alerta Temprana, en 2009, así como la regulación del Esquema Nacional de Seguridad, o de la Ley de Infraestructuras Críticas, de este mismo año 2011.

Programa variado

Cuatro fueron los módulos en los que se dividieron las jornadas: dos enfocados a la Gestión de Incidentes y los otros dos a la Implantación del Esquema Nacional de Seguridad y a las Infraestructuras Críticas (IC). Este último apartado, y como novedad frente a otros años, contó con la presencia entre los asistentes de organizaciones privadas, gestoras y/o

propietarias de IC (particularmente de los sectores energético y de transporte), así como del Centro Nacional de Protección de Infraestructuras Criticas (CNPIC), perteneciente al Ministerio del Interior.

En el primero y segundo de los módulos se abordaron la gestión de incidentes del propio CCN-CERT así como las Amenazas Persistentes Avanzadas (APT). "Persistencia APT: Ocultación en las comunicaciones"; "Vulnerabilidades en aplicaciones web basadas en el DNIe en las AAPP"; "Persistencia APT en los sistemas de la organización"; "Ataque a iPhone" y "Estrategias de monitorización del uso de Internet para alerta temprana" fueron las conferencias que conformaron esta primera sesión, que concluyó con una mesa redonda sobre el panorama en la gestión de incidentes en las AAPP y la necesidad de coordinación entre todos los CERTs públicos españoles (Andalucía-CERT, CCN-CERT, CESICAT, CSIRT-CV, INTECO-CERT e IRIS-CERT).

El día 14 tuvo lugar la segunda sesión, en la que se presentaron las novedades del CCN-CERT, se analizó el ENS y la seguridad en el intercambio de información y se abordó la problemática de las vulnerabilidades SCADA. "Retos en la implantación del ENS"; "Métricas en el ENS"; "Cloud Computing y el ENS"; "El DNIe es seguro pero… ¿se usa de forma segura?"; "Actualización sobre Infraestructuras Críticas (CNPIC)"; "Ataque a protocolos de comunicaciones en Infraestructura Crítica"; "Lecciones aprendidas tras un ataque DDoS"; "Ataque de una arquitectura SCADA para boicotear un proceso industrial" y "DNS Distribución de malware y compromiso de información" fueron el resto de ponencias que configuraron el programa de la segunda sesión y que se publicarán en la parte restringida del portal del CCN-CERT (www.ccn-cert.cni.es).

Novedades del CCN-CERT

El responsable del CERT Gubernamental español ofreció un breve resumen de los últimos servicios incorporados por este equipo durante el año 2011 y puestos a disposición de todo el personal de la Administración en su portal www.ccn-cert.cni.es. La ampliación y actualización de la sección del Esquema Nacional de Seguridad (con 14 guías de implantación, programas de apoyo y documentación sobre el mismo), la nueva sección sobre Infraestructuras Críticas, las Series CCN-STIC (con 156 guías que recogen normas, instrucciones y recomendaciones), Cursos STIC, Cursos On-line de Seguridad de la Información, Sistema MultiAntivirus o la Herramienta PILAR, son algunas de los servicios ofrecidos por el CCN-CERT. Muchos de ellos se ubican en la parte restringida del portal (son ya 3.385 los responsables de seguridad de las distintas administraciones que están inscritos en esta área). También se presentó el piloto de la herramienta CARMEN enfocada a detectar anomalías en el tráfico de navegación.

De igual forma, el CCN-CERT realizó una breve exposición de los principales incidentes y amenazas detectadas por este Equipo provenientes de sus Sistemas de Alerta Temprana, cuyo fin es la detección rápida de eventos sospechosos y anomalías dentro del ámbito de la Administración (tanto dentro de la red SARA como en los accesos a Internet de los organismos suscritos al servicio, 38 en el caso de la Intranet Administrativa y 25 en Internet).

MÁS INFORMACIÓN

Clara Baonza
cbaonza@tb-security.com
TB·Security
(+34) 91 301 34 95
cbaonza@tb-security.com

Centro Criptológico Nacional
Avda. del Padre Huidobro, Km. 8,500
28023 Madrid
www.ccn-cert.cni.es
info@ccn-cert.cni.es