Un centenar de responsables de seguridad informática de las distintas administraciones públicas con presencia en la Comunidad Valenciana acudieron al encuentro del CCN-CERT y CSRIT-CV

Se presentan en Valencia los Equipos de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional y de la Comunitat Valenciana

- **Ambas instituciones han firmado recientemente un convenio marco de colaboración para impulsar los aspectos de seguridad dentro del desarrollo de la Sociedad de la Información, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos**

- **El incremento constante de amenazas y ataques sobre los sistemas y tecnologías de la información y las comunicaciones hacen indispensable estos servicios**

Valencia, 25 de noviembre de 2008.- El Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), y la Conselleria de Justicia y Administraciones Públicas de la Generalitat Valenciana han presentado hoy conjuntamente sus respectivos Equipos de Respuesta ante Incidentes de Seguridad de la Información. De un lado, el CERT gubernamental español, el CCN-CERT, y de otro, el Centro de Seguridad de la TIC de la Comunitat Valenciana, CSIRT-CV, primer equipo autonómico de estas características creado en España.

El acto contó, entre otras personalidades, con la participación del Secretario Autonómico de Administraciones Públicas de la Conselleria de Justicia y AAPP de la Generalitat, Rafael Peset, y el Subdirector Adjunto del Centro Criptológico Nacional, Luis Jiménez. Ambos coincidieron en señalar la necesidad de este tipo de servicios como respuesta al creciente número de incidentes de seguridad informática y a las graves repercusiones que estos pueden tener, tanto en el ámbito de la Administración como en el de las empresas y los ciudadanos.

En el transcurso del encuentro, al que acudieron casi un centenar de responsables de seguridad de las distintas administraciones con presencia en la Comunidad, se dieron a conocer los dos equipos creados para hacer frente a estos nuevos riesgos y amenazas, a nivel nacional (CCN-CERT) y autonómico (CSIRT-CV).

Así, el CCN-CERT, creado a principios del año 2007 por parte del CCN, tiene como objetivo contribuir a la mejora del nivel de seguridad de los sistemas de información de todas las administraciones públicas españolas (general, autonómica y local). Para ello, el CCN-CERT facilita a todas ellas un buen número de servicios entre los que destacan: soporte y coordinación para la resolución de cualquier ataque recibido; divulgación y recomendaciones sobre buenas prácticas en seguridad; formación a través de sus cursos STIC e información sobre posibles vulnerabilidades de los productos o servicios utilizados, así como de amenazas detectadas por su propio equipo.

Por su parte, el CSIRT-CV, Centro de Seguridad de las TIC de la Comunitat Valenciana, primero de estas características constituido por una autonomía

española, ha sido creado por la Conselleria de Justicia y Administraciones Públicas para hacer frente a estas mismas amenazas, no sólo en la AAPP sino también entre las empresas y los ciudadanos.

La consonancia en las líneas de trabajo del CCN-CERT y del CSIRT-CV ha hecho posible la firma de un Convenio Marco de Colaboración entre la Generalitat de la Comunitat Valenciana y el Centro Criptológico Nacional del Centro Nacional de Inteligencia. En virtud de dicho acuerdo, firmado recientemente, se fijan las bases de colaboración entre ambas instituciones para impulsar en España los aspectos de seguridad dentro del desarrollo de la Sociedad de la Información, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos.

Los ataques informáticos más comunes

En el transcurso del acto, un representante del CCN-CERT hizo además un breve resumen de los ataques más comunes que se están registrando a lo largo de todo el año 2008: robo de información, la infección de los sistemas Windows y Unix por medio de troyanos o rootkits (herramienta que sirve para ocultar actividades ilegítimas en un sistema), la utilización de botnets para realizar ataques de forma masiva, los ataques a servicios web, el phishing y el spam. De entre ellos, los más preocupantes a día de hoy son los troyanos (programa que aparentemente es útil o inocente pero que, en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos…) puesto que no son detectados por los anti-virus, tienen muy estudiado previamente su objetivo y suelen descubrirse no cuando han infectado a un equipo sino cuando ya han empezado a emitir información. Además, emplean un código malicioso o *exploit* para tomar el control de la máquina aprovechando vulnerabilidades muy recientes (en algunos casos cuando ni siquiera han sido detectadas por el propio fabricante).

MÁS INFORMACIÓN

Centro Criptológico Nacional
info@ccn-cert.cni.es
www.ccn-cert.cni.es

Centro de Seguridad TIC de la C.V.
csirtcv@gva.es
https://www.csirtcv.es
Tfno.: (+34) 96 398 53 00

TB·Security
Ana Claudia Rodríguez
(+34) 91 301 34 95
arodriguez@tb-security.com