El principal objetivo del CCN-CERT es contribuir a la mejora del nivel de seguridad informática de la Administración pública española

El Centro Criptológico Nacional, en colaboración con la Junta de Castilla-La Mancha, presenta en Toledo su servicio de Respuesta a Incidentes de Seguridad de la Información (CCN-CERT)

- **El incremento constante de vulnerabilidades y amenazas sobre los sistemas y tecnologías de la información y comunicaciones hacen indispensable este servicio.**

- **Colaborar con todas las administraciones para prevenir incidentes y, llegado el caso, responder de forma rápida y eficiente ante cualquier ataque, fundamentos del CCN-CERT**

***30 de septiembre de 2009*.** La sede de la Consejería de Industria, Energía y Medio Ambiente de Castilla-La Mancha, en Toledo, ha sido el lugar escogido para la presentación hoy del Equipo de Respuesta ante Incidentes de Seguridad (CCN-CERT) del Centro Criptológico Nacional (CCN), organismo dependiente del Centro Nacional de Inteligencia (CNI). El evento ha sido organizado por el CCN y dicha Consejería y ha contado con la asistencia de alrededor de cincuenta responsables de seguridad de la información de las tres administraciones públicas con presencia en la región (general, autonómica y local).

El acto ha contado con la presencia de la Directora General para la Sociedad de la Información y las Telecomunicaciones, Agustina Piedrabuena Moraleda, y del Subdirector Adjunto del CCN, Luis Jiménez.

En el transcurso de la Jornada se presentaron algunos de los recursos más importantes puestos a disposición de todas las administraciones públicas por parte del CCN-CERT, con los que poder mejorar la seguridad de los sistemas y, de esta forma, garantizar su funcionamiento eficaz al servicio del ciudadano. Soporte y coordinación en la resolución de incidentes (*phishing, spam*, ataques a servicios web, captura de datos personales, denegación de servicio, destrucción de información….); información sobre vulnerabilidades, alertas y avisos de nuevas amenazas detectadas por el Centro; análisis de código dañino, análisis de riesgos, cursos de formación para el personal TIC de toda la Administración o evaluación y certificación de productos son algunos de las herramientas facilitadas por este Equipo.

Por su parte, representantes de la Consejería de Industria, Energía y Medio Ambiente hicieron un breve recorrido por las distintas actuaciones que se están desarrollando desde la Dirección General para la Sociedad de la Información y las Telecomunicaciones de la Junta en materia de seguridad de la información.

Tendencias 2009

Para terminar el acto, el coordinador del CCN-CERT ofreció una charla sobre los ataques más comunes que se están registrando a lo largo de todo el año 2009 y sobre la importancia de la sensibilización del personal encargado de los sistemas de seguridad. El robo de información, la infección de los sistemas Windows y Unix por medio de troyanos o rootkits (programa que oculta actividades ilegítimas en un sistema y que, una vez instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo), la utilización de botnets para realizar ataques de forma masiva, los ataques a servicios web, el phishing y el spam, fueron algunos de los aspectos abordados en la Jornada.

Portal www.ccn-cert.cni.es

La principal herramienta para dar soporte a estos servicios lo constituye el portal que ha desarrollado el CCN-CERT: www.ccn-cert.cni.es. A través de esta página web se ofrece información actualizada diariamente sobre amenazas, vulnerabilidades, guías de configuración de las diferentes tecnologías, herramientas de seguridad, cursos de formación o indicaciones para mejores prácticas de seguridad.

Además, existe una parte de acceso restringido dirigida únicamente a personal de la Administración, que exige el registro previo. Así, y una vez autorizada su alta, se puede realizar la descarga de documentos, herramientas de seguridad, metodologías o técnicas con las que contar ante un posible incidente.

Gracias a este registro, el CCN-CERT pretende conseguir una comunicación directa con su *comunidad* para poder actuar adecuada y rápidamente ante cualquier hipotético ataque.

MÁS INFORMACIÓN

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

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