MINISTERIO
DE DEFENSA

GOBIERNO
DE ARAGON
Departamento de Ciencia,
Tecnología y Universidad

CCN-CERT

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 el Gobierno de Aragón, presenta en Zaragoza 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**

***Madrid, 8 de julio de 2008*.** La sede del Departamento de Tecnología, Ciencia y Universidad del Gobierno de Aragón, en Zaragoza, ha sido el lugar escogido para la presentación hoy del Equipo de Respuesta ante Incidentes de Seguridad (CCN-CERT) del Centro Criptológico Nacional (CCN), dependiente del CNI. El evento ha sido organizado por el CCN y dicho Departamento y está dirigido a los responsables de seguridad de la información de las tres administraciones públicas con presencia en Aragón (general, autonómica y local).

El acto ha contado con la presencia del Director General de Tecnologías para la Sociedad de la Información del Gobierno de Aragón, Miguel Ángel Pérez Costero, y del Subdirector Adjunto del CCN, Luís Jiménez.

En el transcurso del acto, Jiménez presentó 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 (*phising, 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.

Tendencias 2008

En el transcurso del acto, el Subdirector Adjunto del CCN hizo un breve resumen de los ataques más comunes que se prevén para 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. Una vez que ha sido 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. De entre ellos, y según Jiménez, los más preocupantes a día de hoy son los troyanos.

Con el fin de ofrecer una solución eficaz frente a estos ataques, se formó a principios del 2007 el CCN-CERT. Este equipo constituye el CERT gubernamental español, a imagen y semejanza de los existentes en otros países (Alemania, Reino Unido, Holanda, Italia, Suiza, etc.). Además, participa en los principales foros de seguridad europeos y mundiales, en los que comparte información y objetivos y en los que se debate sobre los nuevos avances en materia de ciberseguridad.

Portal www.ccn-cert.cni.es

La principal herramienta para dar soporte a estos servicio lo constituye el portal que ha desarrollado el CCN: 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.

De hecho, y dado el carácter crítico de algunos de los aspectos recogidos en el portal, 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
Lorena Fernández Martín
lfernandez@tb-security.com
TB·Security
91 301 34 95

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