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 y León, presenta en Valladolid 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**

***14 de octubre de 2008*.** La sede de la Consejería de Administración Autonómica de la Junta de Castilla y León, en Valladolid, 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 está dirigido a los responsables de seguridad de la información de las tres administraciones públicas con presencia en Castilla y León (general, autonómica y local).

El acto ha contado con la presencia del Director General de Innovación y Modernización Administrativa de la Junta, Antonio Francisco Pérez Fernández, y del Jefe de Políticas y Servicios para la Seguridad de las TIC del CCN, Javier Candau.

En el transcurso del acto, 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 (*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

Los representantes del CCN-CERT hicieron 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. 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, 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).

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