La creación del CCN-CERT por parte del Centro Criptológico Nacional pretende contribuir a la mejora del nivel de seguridad en las AAPP

Las amenazas y vulnerabilidades sobre los Sistemas de Información se incrementaron un 55% entre 2004 y 2006

- **Las amenazas son cada vez más complejas y difíciles de detectar**

- **Las distintas AAPP deben considerar el desarrollo, adquisición, conservación y utilización segura de las TIC como algo imprescindible que garantice el funcionamiento eficaz del servicio al ciudadano y de los intereses nacionales**

Madrid, 24 de abril de 2007. Las amenazas y vulnerabilidades registradas por el CCN-CERT se incrementaron en un 55% en los dos últimos años. Así, de las 1.329 publicadas en 2004 (obviamente, no todas explotadas) se pasó a 2.057 en 2006, lo que representa un incremento del 54,7%. Si bien es cierto que en 2006 se observa un leve descenso en el número de amenazas y/o vulnerabilidades registradas frente a 2005 (2.213), basta un vistazo a la serie de datos de los últimos cuatro años (ver figura 1) para observar que el ritmo de crecimiento de las mismas que afectan a los Sistemas de Información ha sido prácticamente exponencial en este período de tiempo.

Respecto a los tipos de riesgos que estas vulnerabilidades implican para nuestros Sistemas de Información, según publica el CERT® *Coordination Center*[1], la mayoría de las amenazas recibidas cuando se está conectado constituyen casos de cibercrimen. La situación actual de este cibercrimen se caracteriza por:

- Los tipos de amenazas evolucionan continuamente (virus, *phishing, defacement,* etc.*)*.
- Los sistemas de información para misiones críticas de las organizaciones se están integrando cada vez más con Internet.
- El daño y la velocidad de los ataques se incrementan continuamente.
- El software continua teniendo vulnerabilidades intrínsecas “desde la caja”.
- Existe un amplio consenso en considerar que el cibercrimen es una debilidad crítica de las naciones occidentales

El registro de vulnerabilidades [2] y amenazas[3] (recogidas en el portal www.ccn-

[1] CERT® es una marca de servicios registrada por la Carnegie Mellon University

[2] Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema.

[3] Cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un Sistema de las TIC resultando en una pérdida de confidencialidad,

cert.cni.es) se alimenta diariamente con la lectura sistemática de noticias sobre ataques a todo tipo contra Organismos y Entidades. Términos como *spam, virus, phising, troyano, malware, spyware, pharming, fraude on-line, hacker o keylogger* han pasado a formar parte del lenguaje común de muchos de nosotros y se encuentran en titulares de la prensa diaria tan inquietantes como algunos de los recogidos en este portal:

- *"El robo informático es una nueva unidad de negocio para la mafia",*
- *"Piratas informáticos chinos roban información militar secreta en Taiwán",*
- *"La Agencia Tributaria advierte de un intento de Phishing",*
- *"La policía británica desbarata un plan de Al Qaeda para bloquear Internet en todo el país",*
- *"Una niña de seis años instala un keylogger en un ordenador del Parlamento británico",*
- *"Posible robo de datos al Ministerio de Economía de Rumanía".*

Dado que las amenazas cada vez son más complejas y, a veces, difíciles de detectar, se hace necesaria una **formación del personal** responsable de las TIC en todas las Organizaciones (incluidas, por supuesto, todas las Administraciones Públicas) para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información (STIC). Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: **disponibilidad, integridad y confidencialidad**. En algunos entornos, especialmente en los dedicados a la Administración Electrónica, interesan, además, otros aspectos muy importantes de las transacciones on-line como son la autenticidad o la trazabilidad.

La Administración en su conjunto no puede ser ajena a este escenario y debe considerar el desarrollo, la adquisición, conservación y utilización segura de las TIC como algo imprescindible que garantice el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. Sobre todo, teniendo en cuenta los nuevos **retos** a los que se enfrenta, procedentes de muy diversas fuentes: **Servicios de Inteligencia, Grupos Organizados, Terroristas, Hackers, Grupos Criminales, Empleados deshonestos,** etc.

Se hace imprescindible, por tanto, tomar conciencia de los riesgos a través de medidas a todos los niveles (legislativas, organizativas y técnicas) así como de la implentación de herramientas técnicas de seguridad (anti-virus, firewalls, software para autenticación de usuarios o para cifrado de la información) y del empleo de productos certificados, de inspecciones o auditorías de seguridad, etc.

Del mismo modo, resulta esencial la gestión de incidentes a través de Centros de Respuesta a Incidentes o CERT (*Computer Emergency Response Team*), dedicado s a la implantación y gestión de medidas tecnológicas que prevenga, primero, y mitiguen llegado el caso el riesgo derivado de los ataques a los que están expuestos los sistemas de la comunidad a la que proporcionan el servicio.

La creación por parte del Centro Criptológico Nacional del Equipo de Respuesta a Incidentes de Seguridad de la Información (CCN-CERT) viene a cubrir esta necesidad y a contribuir a la mejora del nivel de seguridad de los sistemas de información en las Administraciones Públicas Españolas.

---

integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio Sistema.

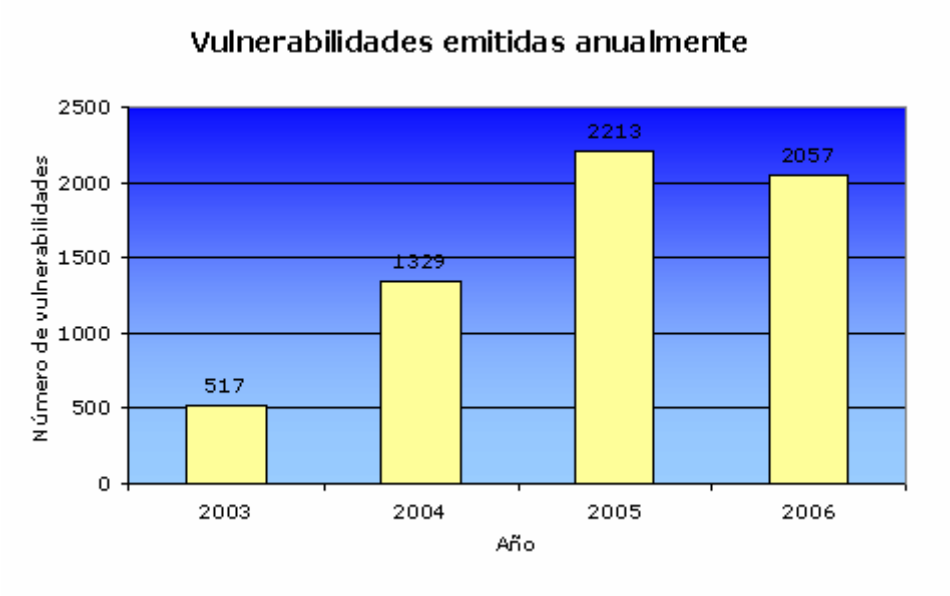

Figura 1.

MÁS INFORMACIÓN

Clara Baonza Díaz
TB-Security
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