MINISTERIO
DE DEFENSA

CNI-CCN
centro nacional de inteligencia
centro criptológico nacional

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional detecta un incremento constante de este tipo de incidentes

La infección por código dañino fue uno de los principales incidentes gestionados por el CCN-CERT en 2008

- **El CERT gubernamental español ha colaborado con organismos nacionales e internacionales en la resolución de todo tipo de incidentes, manteniendo siempre la confidencialidad sobre la información del solicitante de ayuda.**

- **Más de 1.300 responsables de seguridad TIC de las distintas administraciones públicas españolas se registran en la parte privada de su portal, www.ccn-cert.cni.es, desde la que se coordina y da soporte a cualquier incidente o vulnerabilidad.**

Madrid, 9 de marzo de 2009. El fraude online (principalmente el phishing) y la infección por código dañino (virus, gusanos, troyanos, spyware, etc.), con un 24,14% y un 20,69%, respectivamente, fueron las dos tipologías de incidentes, que más tuvieron que ser gestionadas por el Equipo de Respuesta ante Incidentes de Seguridad de la Información, del Centro Criptológico Nacional, CCN-CERT, durante el pasado año (*ver Fig.1*).

Tras estas dos modalidades, se situaron los incidentes por intentos de intrusión (explotación de vulnerabilidades conocidas, cross-site scripting, inyección SQL, inyección de ficheros remoto, intentos de login, etc.) con un 17,44% del total; seguido de la ausencia de disponibilidad (ataques DoS y DDoS, sabotaje, fallos en el hardware o en el software o errores humanos), con el 17,14%. Entre estos incidentes gestionados por el CERT gubernamental español, también se encontraron los de contenidos abusivos (spam) y los de robo de información (escaneos a aplicaciones Web, sniffing o ingeniería social)

Los incidentes gestionados durante el año 2008 fueron localizados por el propio Equipo o bien notificados por otros organismos solicitantes de ayuda, tanto a nivel nacional como internacional. En este sentido, la política del CCN-CERT es mantener siempre la confidencialidad sobre cualquier información específica de la Administración solicitante de ayuda.

La gestión de estos incidentes no se limita al establecimiento de la capacidad de reacción sino que proporciona la base para la prevención de incidentes futuros (tanto si los incidentes tienen su origen dentro o fuera del Organismo, como si son provocados por un agresor, indirectamente a través de un agente o incluso si se producen por causas fortuitas).

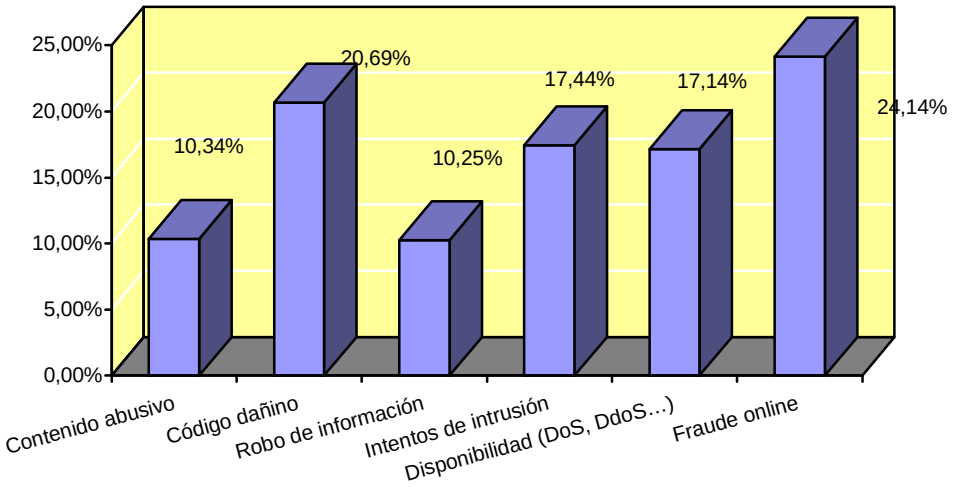

Figura 1: Porcentaje de incidentes gestionados por el CCN-CERT durante 2008

Incremento de vulnerabilidades y código dañino

La actividad del CCN-CERT no sólo se centra en la gestión de incidentes, sino que el Equipo realiza una fuerte labor proactiva recopilando y registrando información sobre vulnerabilidades y código dañino, basadas tanto en el trabajo de sus propios analistas como en las contribuciones procedentes de muy diversas fuentes de reconocido prestigio, nacionales e internacionales (*Ver Fig. 2*). De esta forma, en los últimos cuatro años, el número de vulnerabilidades se ha duplicado (pasando de 2.998 a 6.100); mientras que el código dañino ha seguido la tendencia contraria (de 16.705 a 9.687). No obstante, estas cifras pueden resultar engañosas puesto que muchos especimenes de código dañino pueden permanecer actuando sin ser detectados por los diferentes programas de seguridad.

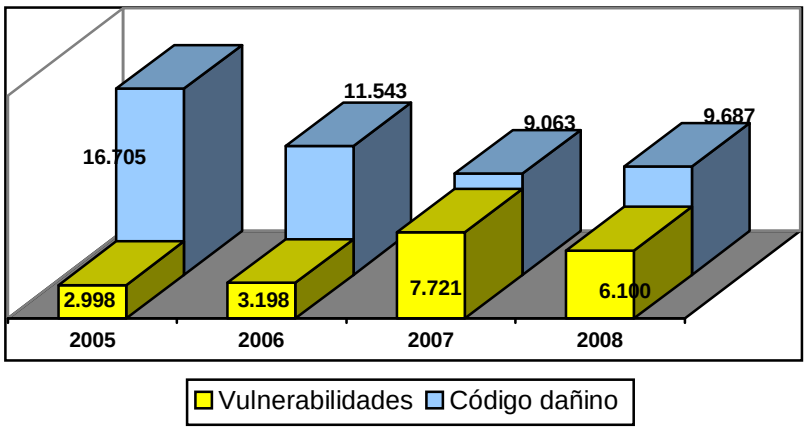

Figura 2: Evolución de vulnerabilidades y código dañino registrados

Portal www.ccn-cert.cni.es

La principal herramienta desarrollada por el CCN-CERT para coordinar y dar soporte a todos los responsables de seguridad TIC de las distintas administraciones públicas españolas es el portal: www.ccn-cert.cni.es. A través de este sitio web, se puede acceder a la mayor parte de los servicios ofrecidos por el CERT gubernamental español.

A 31 de diciembre de 2008, más de 1.300 responsables de seguridad de toda la Administración pública (general, autonómica y local) se habían registrado en su parte restringida, desde la cual reciben todo tipo de información de primera mano, no sólo sobre el modo de abordar cualquier incidente, sino también, y sobre todo, sobre cómo evitarlo a través de guías, informes y herramientas de seguridad. De este número, aproximadamente el 61% pertenece a la Administración General del Estado, el 18% a la autonómica, el 14% a la local, un 4% a Universidades y un 1% a organizaciones internacionales con las que se mantiene una estrecha colaboración.

MÁS INFORMACIÓN

Ana Claudia Rodríguez
TB-Security
(+34) 934 054 232
arodriguez@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