CCN-CERT presenta su informe Ciberamenazas 2012 y Tendencias 2013 y tres guías CCN-STIC

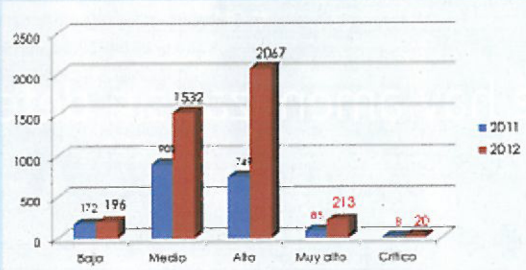
El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, **CCN-CERT**, adscrito al Centro Nacional de Inteligencia (CNI), ha dado a conocer su informe "**Ciberamenazas 2012 y Tendencias 2013**", en el que se hace balance del panorama internacional y nacional en el marco de los ciberincidentes.

Según dicho informe, durante el año 2012 se incrementaron en un 150% el número de incidentes catalogados con un riesgo muy alto o crítico por el propio CERT gubernamental –donde destacan especialmente las llamadas APTs o Amenazas Persistentes Avanzadas–, habiéndose pasado de los 93 incidentes de este nivel registrados en 2011 a los 233 contabilizados en 2012.

A lo largo de sus 170 páginas, el informe hace un balance de los actores implicados en los ciberincidentes (los propios Estados, las grupos de "hacktivistas", investigadores de ciberseguridad y los actores internos de las organizaciones), así como de las principales amenazas detectadas a lo largo de 2012, siendo el ciberespionaje y la infección por *malware* los riesgos más altos para los organismos públicos. Mientras, para las organizaciones privadas, las fuentes más importantes de riesgos son el espionaje industrial digital, la infección por código dañino, el *spam*, y el fraude de identidad. En cuanto a los ciudadanos, el principal problema sigue siendo el fraude de identidad.

Las vulnerabilidades (la insuficiente seguridad de los sitios web y de los sistemas operativos para dispositivos móviles, entre otros), las herramientas tecnológicas utilizadas por los atacantes y la resiliencia o capacidad para mantener unos niveles mínimos de servicio y recuperarse con rapidez tras un incidente son otros de los capítulos de este Informe.

Según se señala en el documento, donde se recogen algunos de los principales incidentes ocurridos durante el año pasado, "*los atacantes siguen manteniendo la iniciativa y la capacidad para causar enormes daños. A pesar de la existencia de medidas de seguridad, los métodos, procedimientos y herramientas tendentes a mejorar la defensa ante los ciberataques siguen, en muchos casos, sin estar debidamente implantados*". Además, recoge que "*los ataques dirigidos son comúnmente utilizados con fines de espionaje industrial, de cara a obtener acceso a la información confidencial contenida en un sistema de información. Se trata de los ataques más difíciles de combatir*".



Evolución de los incidentes registrados por el CCN-CERT, por nivel de criticidad

Tendencias para 2013

De cara a este año 2013, el CCN-CERT, a partir de análisis y prospectivas propios e informes provenientes de diferentes fuentes y expertos consultados, considera que las APT seguirán constituyendo las herramientas más significativas para el ciberespionaje empresarial y gubernamental.

De igual modo, se espera un crecimiento del *malware* para dispositivos móviles, así como ataques de ingeniería social y el uso económico de las redes sociales, con un aumento de los ataques de *malware* que persigan la sustracción de las credenciales de pago usadas en estas redes. Otras tendencias observadas por el CCN-CERT son los ataques contra servicios web, la consolidación del *ransomware* (caballos de Troya diseñados para cifrar los datos del disco duro del usuario o bloquearle el acceso al sistema, exigiéndole dinero a cambio de recuperar la información y/o el sistema), la expansión de *botnets* y *malware* de precisión, o el crecimiento del *activismo*.

Guías CCN-STIC

Por otro lado, el CCN-CERT ha hecho públicas sus **Guías de la Serie CCN-STIC 450** sobre seguridad en dispositivos móviles: *Guía CCN-STIC 453 Seguridad en Android*, *CCN-STIC 454 (iPad)* y *CCN-STIC 455 (iPhone)*, donde recoge información necesaria para la evaluación y análisis de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los dispositivos móviles en la actualidad.

Adicionalmente, esta serie presenta una lista de recomendaciones de seguridad generales cuyo objetivo es proteger los dispositivos móviles, sus comunicaciones y la información y datos que gestionan y almacenan.

Las Guías de Seguridad en dispositivos móviles android, iPad e iPhone pueden descargarse desde el portal del CCN-CERT (www.ccn-cert.cni.es) y son actualizadas continuamente según la versión del fabricante.

AENOR publica la norma UNE 71506 para el análisis forense de las evidencias electrónicas

Aenor ha hecho pública la **Norma UNE 71506:2013 Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas**, cuyo objeto es establecer una metodología para la preservación, adquisición, documentación, análisis y presentación de evidencias electrónicas.

La Norma UNE 71506, elaborada por el Comité Técnico de Normalización de Aenor AEN/CTN 71 Tecnologías de la Información, define el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas, complementando todos aquellos otros procesos que conforman dicho sistema de gestión de las evidencias electrónicas, según se describe en las partes de la Norma UNE 71505, cuya familia de normas ha sido asimismo publicada.

Se pretende que esta norma proporcione respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades, ya que la obtención de evidencias electrónicas fiables y robustas ayuda a atribuir correctamente dichos hechos, pudiendo discernir si su causa tiene como origen un carácter intencional o negligente.

Con dicha información se consigue ubicar de forma acertada los instrumentos, acciones, fines y demás parámetros concernientes a dichas conductas.

La Norma UNE 71506:2013 es de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a los equipos de respuesta a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.