Su Informe de Actividades 2011-2012 repasa también su labor de concienciación e I+D y los logros de su Organismo de Certificación

El CCN-CERT gestionó 6.256 incidentes entre 2011 y 2012, 325 de ellos críticos

El Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia (CNI), ha hecho pública su Memoria de actividades 2011-2012, donde recoge el trabajo y esfuerzo realizado por el organismo en los dos últimos años en su cometido de garantizar la seguridad TIC en las diferentes entidades de la Administración Pública y en los sistemas que procesan, almacenan o tramitan información clasificada. En los dos últimos años, el organismo ha publicado alrededor de 200 Guías CCN-STIC y potenciado su labor formativa y de sensibilización sobre ciberseguridad gracias a las Jornadas STIC CCN-CERT y SAT-INET y los diferentes cursos impartidos. Del mismo modo, también ha hecho progresos en la acreditación de sistemas y productos; su apuesta en I+D, con nuevos servicios, como el sistema CARMEN para la detección de APT; y su actividad realizada en torno al Esquema Nacional de Seguridad (ENS).

El documento empieza haciendo un repaso al panorama de la ciberseguridad, donde examina lo que considera las principales amenazas (ciberespionaje, ciberdelito, ataques contra servicios web, la acción de grupos *hacktivistas*, vulnerabilidades y *exploits*, *cloud computing*, telefonía móvil y *O-Day*); para luego adentrarse en tres grandes bloques: el que se refiere a la actividad más específica del CCN (donde se analiza su ámbito de actuación y funciones, se expone un catálogo de las diferentes guías e informes publicados, se presenta la herramienta PILAR de Análisis de Riesgos, y se comentan las metas alcanzadas en I+D y en relación al Esquema Nacional de Seguridad), el centrado en el CCN-CERT, y el relativo al Organismo de Certificación (OC). Finalmente, en la Memoria de Actividades 2011-2012 se recoge también una relación de los diferentes acuerdos y colaboraciones suscritos por el organismo, tanto a nivel nacional como internacional.

En esencia, la idea ha sido, y seguirá siendo, tal y como prologa en el informe el Secretario de Estado Director del CNI y Director del CCN, **Félix Sanz Roldán**, contribuir *"a la mejora de la ciberseguridad en España, articulando la respuesta y gestión de los ciberincidentes en torno al CERT Gubernamental/nacional, y promoviendo y certificando los productos y sistemas utilizados. Todo ello, impulsando la colaboración internacional y la necesaria implicación de organismos y empresas"*.

El CCN-CERT

Junto a sus servicios tradicionales de gestión de Incidentes (donde se contabilizaron en dos años 6.256, de los que 325 se consideraron de riesgo muy alto o crítico), elaboración de alertas, avisos y vulnerabilidades (donde se registraron 22.500 vulnerabilidades y 245.000 muestras de código dañino) o auditorías web a distintos organismos de la Administración, el Informe hace hincapié en sus Sistemas de Alerta Temprana (SAT), tanto de la Red SARA como de Internet, para la detección rápida de incidentes y anomalías, y en el sistema CARMEN (Centro de Análisis de Registros y Minería de Datos), especialmente indicado para detectar APTs).

Concretamente, a finales de 2012, el SAT-SARA operaba en 51 organismos públicos, y en él se notificaron ese año un total de 430 incidentes, frente a los 322 del ejercicio anterior. El SAT de Internet, por su parte, en sus cuatro años de existencia, está ya presente en 38 organismos públicos.

El Organismo de Certificación (OC)

Por otra parte, el informe del CCN resalta el papel que cumple su Organismo de Certificación (OC), con sus tres tipologías de certificación: funcional, criptológica y Tempest.

Sobre la primera de ellas, que opera con diversas normas de evaluación de la seguridad TIC, como la conocida como *Common Criteria for Information Technology Security Evaluation*, durante los años 2011 y 2012 se iniciaron 81 expedientes de certificación de productos o sistemas STIC (entre nuevas solicitudes y mantenimiento o revisión de vigencia de los certificados ya existentes) y se publicaron 49 resoluciones de certificación que habían pasado satisfactoriamente el proceso de evaluación.

Guías e informes

Dentro del capítulo dedicado a normas, instrucciones, guías y recomendaciones para optimizar el grado de ciberseguridad en nuestro país, y aparte de la actividad centrada en informes sobre análisis forense, ingeniería inversa de código dañino y auditoría, cabe destacar que a finales de 2012 existían 197 documentos enmarcados dentro de la serie CCN-STIC, 73 de las cuales habían sido elaboradas o actualizadas en los dos últimos años. Algunas de las más populares son la *Guía CCN-STIC 804 de Medidas de Implantación del ENS*, con cerca de 28.000 descargas web; o la *Guía CCN-STIC 480 de Seguridad en Sistemas SCADA*, con 12.120 descargas.

Aquí, y dentro del impulso al desarrollo e implantación del ENS, también es de interés comentar el convenio firmado en julio de 2011, entre el CNI, el Mº de Política Territorial y Administración Pública (hoy de Hacienda y Administraciones Públicas) y el Instituto Nacional de Administración Pública (INAP), por el que el que el organismo se comprometía a elaborar y proporcionar una serie de guías CCN-STIC, colaborar en la formación del personal y proporcionar seguridad a la Intranet Administrativa. A finales de 2012, este compromiso se había materializado en 22 guías de la serie 800, 14 de ellas nuevas.

Formación y cursos

En el área de formación, a las tradicionales Jornadas STIC CCN-CERT (500 asistentes en la VI edición de 2012) y del Sistema de Alerta Temprana de Internet (SAT-INET), que en febrero de 2013 llegó a su tercera edición, se unieron también otras jornadas de concienciación sobre ciberseguridad y el ENS, además de la participación en los dos últimos años en más de 110 mesas redondas o jornadas del sector. Paralelamente, cabe resaltar que los cursos presenciales han convocado a más de 2.340 alumnos, y el formato *on-line* a un total de 1.887.

I+D

Finalmente, en el apartado de investigación y desarrollo, y aparte de la presentación, durante 2012, de la versión 5.2 de la herramienta PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos), el CCN ha participado y/o llevado la dirección técnica de los siguientes proyectos: el sistema de cifrado *Criptosistema EP430GN*; el programa *Criptoper Scap Procif*, cifrador de voz y datos con protocolo de interoperabilidad SCIP para transmitir información nacional clasificada (primer producto de cifra nacional adquirido por la OTAN); y los proyectos TMSDef, de Terminal móvil tipo PDA, de demostrador de cifrador IP táctico y de cifrador personal interoperable SCIP multipropósito, entre otros.