9th NATO WORKSHOP

Últimos avances en ciberseguridad

LA NECESIDAD DE PROGRESAR EN LA SEGURIDAD DE LA RED ES CADA DÍA MÁS PERENTORIA. ASÍ SE DESTACÓ EN EL IX ENCUENTRO SOBRE CIBERDEFENSA DE LA OTAN, ORGANIZADO POR EL CCN-CERT EN BARCELONA

CCN-CERT
Centro Criptológico Nacional

¿Quién hubiera pronosticado, hace poco más de una década, el formidable impacto de Internet? Su uso generalizado en la actualidad ha coronado a la red de redes como uno de los inventos más transcendentales de los últimos tiempos. Aunque, como todo gran hallazgo, arrastra luces y sombras. Entre los inconvenientes más sonados destaca, sin duda, el ciberterrorismo, que se materializa en ataques cada vez más frecuentes y más peligrosos, máxime si tenemos en cuenta que la sociedad actual depende a todos los niveles de las tecnologías de la información.

Recientemente -y demostrando la creciente preocupación de las instituciones mundiales por la CiberDefensa-, la OTAN ha anunciado la formación de un centro de investigación contra el ciberterrorismo, del que formará parte España, junto con otros seis países de la Alianza.

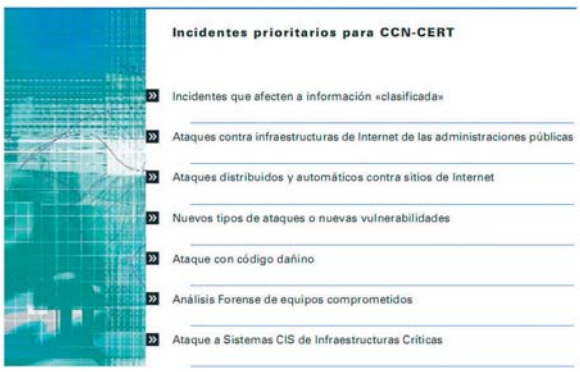
Y fue precisamente en nuestro país, en Barcelona, donde el grupo de trabajo del Equipo de Respuesta a Incidentes de Seguridad TIC de la OTAN (NCIRC) celebró el IX Encuentro sobre CiberDefensa, en el que más de 180 especialistas, de los 26 países miembros de la Alianza, trataron los principales avances realizados en la materia. En esta ocasión, España actuó de país anfitrión del evento a través del Equipo de Respuesta a Incidentes de Seguridad de la Información (CCN-CERT), dependiente del Centro Criptológico Nacional (CCN).

> Parte del éxito del CCN radica en la colaboración con los organismos europeos y mundiales

En el transcurso de las Jornadas, el CCN-CERT, el CERT gubernamental español creado hace año y medio, expuso gráficamente los últimos avances realizados en nuestro país en seguridad de los sistemas de información y las comunicaciones, tanto por parte de la Administración, como de las empresas que colaboran con ella.

Entre estos avances se sitúa la última versión de la herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos) que sigue la metodología MAGERIT, estándar de la Administración Central del Estado y reconocida por la OTAN. Esta herramienta, facilitada a todas las administraciones por parte del CCN, soporta el análisis y la gestión de riesgos de los sistemas de información y ha sido traducida a tres idiomas: inglés, francés e italiano. Próximamente, además, los usuarios también dispondrán de la herramienta en alemán, portugués, húngaro y polaco.

Otra de las bazas de este Equipo para favorecer la seguridad en la Administración, tal y como se mencionó en Barcelona, son los cursos dirigidos a sus responsables TIC. Resultan de especial interés los cursos Informativos y de Concienciación en Seguridad, los de Seguridad (entornos Windows,



Nueva versión del portal www.ccn-cert.cni.es

entornos Linux, bases de datos e infraestructura en red), los relativos a la Gestión de Seguridad (Common Criteria, gestión STIC y especialidades criptológicas) y los de Especialización en Seguridad (búsqueda de evidencias y control de integridad, entornos UNIX, entornos Windows, entornos Linux, redes inalámbricas, cortafuegos, detección de intrusos, herramientas de seguridad e inspecciones de seguridad).

Todos los recursos mencionados, junto con las "Series CCN-STIC" (documentos con normas, instrucciones, guías y recomendaciones de seguridad) están disponibles para las administraciones públicas en el portal (www.ccn-cert.cni.es).

e-DNI y Protección de Infraestructuras Críticas

Además de estas acciones, el CCN ha colaborado con el Cuerpo Nacional de Policía en el proyecto de desarrollo del DNI electrónico (e-DNI), perfeccionando las medidas de seguridad que debe cumplir el e-DNI y las aplicaciones que lo empleen. Algunas de las medidas introducidas: un chip criptográfico, el uso de tintas invisibles y policromáticas, la inclusión de hologramas, el uso de tecnología láser para la impresión de la fotografía -que protege de la falsificación- así como su integración en el fondo impreso de la tarjeta.

De igual forma, el CCN apoya al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) -cuya creación fue aprobada por el Gobierno en noviembre de 2007- en la prevención y gestión de incidentes relacionados con la seguridad de más de 3.500 instalaciones (vías de transporte, centrales eléctricas o redes de abastecimiento de agua y alimentos).

Las Infraestructuras Críticas se refieren al conjunto de recursos, servicios, tecnologías de la información y redes que, en el caso de sufrir un ataque informático, causarían un gran impacto en la seguridad -tanto física como económica- de los ciudadanos o en el buen funcionamiento del Gobierno. Entre éstas se incluyen el sector energético, nuclear, económico, químico, espacial, de las tecnologías de la información, de transportes, de abastecimiento, de sanidad y de investigación.

Colaboración con organismos y entidades

Una importante parte del éxito del CCN también radica en la colaboración con los organismos europeos y mundiales. A nivel internacional, el CCN-CERT pertenece al *Forum of Incident Response and Security Teams* (FIRST), foro internacional que se creó en 1990 y que aglutina a 189 miembros en la actualidad. El objetivo fundamental de este Organismo consiste en coordinar a los diferentes CERTs de todo el mundo, compartiendo información sobre vulnerabilidades y ataques globales y divulgando medidas tecnológicas de mitigación.

A nivel europeo, CCN-CERT está integrado en TERENA *(Trans-European Research and Education Networking Association)*, principal foro de Respuesta a Incidentes de Seguridad de la Información, y trabaja con los demás CERTs europeos a través del grupo EGC *(European Government CERTs)*.

Además del diálogo continuo con instituciones tanto nacionales como internacionales, el CCN mantiene un estrecho vínculo con el sector empresarial, un vínculo que incide en su capacidad para estar al tanto de las últimas innovaciones de la industria como: sistemas de seguridad multinivel; comunicaciones seguras mediante PDA; plataforma de firma electrónica; sistemas de alerta temprana; sistema multiantivirus o técnicas de análisis de *malware*.

A través de todas estas actividades, el CCN-CERT orienta sus esfuerzos, energías y recursos para continuar afrontando de manera eficaz los retos que plantea la Sociedad de la Información, contribuyendo así a la mejora de la seguridad de las tecnologías de la información en la Administración y, por ende, de todos los ciudadanos.