MINISTERIO
DE DEFENSA

CNI-CCN
centro nacional de inteligencia
centro criptológico nacional

El Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia, fue el anfitrión del evento

Éxito en la IX Conferencia de la OTAN sobre Ciber Defensa celebrada en Barcelona

- **El encuentro contó con la participación de más de 180 representantes de los 26 países miembros de la Organización**
- **Durante tres jornadas (del 16 al 18 de abril) se debatieron las principales novedades con respecto a la ciberseguridad**

Madrid, 21 de abril de 2008.- España, a través del Centro Criptológico Nacional (CCN), fue el anfitrión del IX encuentro del grupo de trabajo de Capacidad de Respuesta a Incidentes de Seguridad TIC de la OTAN (NCIRC), celebrado en Barcelona del 16 al 18 de abril pasados. El encuentro fue un éxito de asistencia, al acoger a más de 180 especialistas en seguridad procedentes de los 26 países miembros de la Organización, así como representantes de la industria, quienes analizaron durante estos tres días los principales avances realizados en materia de ciberdefensa.

Las reuniones se estructuraron en tres jornadas, de las cuales, la primera de ellas se centró principalmente en los avances realizados en nuestro país en la seguridad de sus sistemas de información y comunicaciones. Así, y dentro de su marco legislativo, se presentó al CCN como el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. Como resultado de sus funciones, en el mercado español se encuentran diversos productos/tecnologías de seguridad desarrollados y/o certificados por el CCN.

También se habló del CCN-CERT (Equipo de Respuesta a Incidentes de Seguridad de la Información del CCN), el CERT gubernamental español orientado a toda la Administración Pública y puesto en marcha hace un año y medio. Desde entonces el CCN-CERT ha prestado sus ayuda a los diferentes organismos que lo han requerido y ha mantenido una amplia variedad de servicios dirigidos hacia su comunidad, entre los que destaca su portal (www.ccn-cert.cni.es), en el que pueden encontrarse guías de configuración (Guías CCN-STIC) y herramientas de seguridad, avisos de vulnerabilidades o noticias del sector, entre otros.

El CCN-CERT ingresó el año pasado en las dos principales organizaciones existentes en el mundo dentro de este campo: FIRST y Trusted Introducer y mantiene una

relación activa con varias organizaciones nacionales o internacionales, tanto públicas como privadas.

El entorno para el análisis de riesgos y la herramienta PILAR (desarrollada y financiada por el CCN) o las actividades del CNPIC (Centro para la Protección de Infraestructuras Críticas del Ministerio del Interior), fueron otros de los temas tratados, además de los sistemas de seguridad multinivel, las comunicaciones seguras mediante PDA, los Sistemas de Alerta Temprana del Gobierno Español, las características de seguridad del eDNI o las plataformas de firma electrónica.

El primer día finalizó con una serie de presentaciones impartidas por la industria, en las que se profundizó en los sistemas de defensa ante ataques DDoS, las mejores prácticas en la respuesta de incidentes o los modelos y estrategias de mitigación.

Cómo evitar ciberataques

Durante la segunda y tercera jornada se celebraron sesiones de expertos en las que se debatió cómo hacer frente a ciberataques similares a los ocurridos en Estonia en mayo de 2007, cuando se produjeron agresiones de denegación de servicio contra portales web del gobierno estonio.

El primer grupo de trabajo se centró en cuál sería la mejor manera de organizar un CERT nacional para optimizar su efectividad y, aunque se aceptaron las peculiaridades de cada uno de estos centros, se destacó la necesidad de mantener un modelo común con el resto de CERTs de los países de la OTAN, con los que compartir objetivos, ideas e información sobre la seguridad de forma global, así como procesos y herramientas de trabajo.

Además, se apuntó la importancia de la existencia de un CERT por país que sea el punto de contacto con el resto de CERTs de la OTAN, vinculados a través del Centro de Coordinación de la organización, el OTAN Cyber Defence Cordination Center. Según los expertos, esta entidad debe actuar sólo y únicamente en situaciones de crisis, y sus principales funciones pasan por dictaminar directrices y coordinar al grupo, entre otras.

El segundo de los grupos de trabajo llevaba por título "¿Qué esperan los CERTs del Equipo de Reacción Rápida (RRT) de la OTAN?". Como respuesta, se mencionaron diversos servicios, tales como la asistencia para la coordinación en caso de ataques (mediante un equipo de expertos en el terreno o de forma remota, u otro tipo de recursos); la vinculación entre los diferentes CERTs de la OTAN; o bien un servicio de análisis *post-mortem*. Los países integrantes de la OTAN, por su parte, pondrán a disposición del RRT tanto su experiencia en gestión de incidentes como los conocimientos de sus expertos, así como el soporte político y tecnológico necesario.

Entre el listado de recomendaciones se dio especial relevancia a las comunicaciones seguras, a la cooperación con organizaciones internacionales o bien a la elaboración de un catálogo global en la que se incluyan los servicios actualizados que los expertos pueden aportar al RRT.

Por último, el tercer grupo de trabajo estableció las posibles aportaciones de un proveedor de servicios de Internet (ISP) a los CERTs: implantación de mecanismos de defensa sugeridos por el propio CERT, definición del uso legal de los servicios "in SLA" (Service Level Agreements) o contribuir con datos útiles para el centro. La industria, por su parte, podría definir modelos o realizar monitorizaciones de sistemas o redes, así como proveer personal técnico experto para los CERTs.

A su vez, las aportaciones de los CERT Nacionales (NCERT) podrían consistir en definir y catalogar las infraestructuras nacionales; colaborar con otros CERTs

nacionales o internacionales, mantener una relación operacional con ISP nacionales y otros actores relevantes de la industria, asistir y asesorar a otras organizaciones, etcétera.

Sobre CCN-CERT

El Equipo de Respuesta ante Incidentes de Seguridad de la Información, CCN-CERT, fue creado por el Centro Criptológico Nacional, con el fin de contribuir a la mejora del nivel de seguridad de los sistemas de información de las administraciones públicas españolas (central, autonómica y local).

Este Equipo tiene como misión ser el centro de alerta nacional que ayude a la Administración a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir. Del mismo modo, asesora a todas las Administraciones en la implantación de medidas tecnológicas que mitiguen el riesgo de sufrir cualquier ataque, proporciona asistencia técnica, facilita cursos de formación y proporciona información sobre vulnerabilidades, alertas y avisos de amenazas a los sistemas de información.

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
info@ccn-cert.cni.es
www.ccn-cert.cni.es