El papel de un CERT gubernamental

SU EXISTENCIA Y COORDINACIÓN SE HA CONVERTIDO EN UNA HERRAMIENTA INDISPENSABLE PARA LA SEGURIDAD NACIONAL

CCN-CERT
Centro Criptológico Nacional

Dentro de las distintas tipologías de CERTs se encuentran los Equipos de Respuesta a Incidentes de Seguridad gubernamentales. Su existencia y coordinación se ha convertido en una herramienta indispensable para la seguridad nacional y, por ende, la mundial.

Nadie duda en estos momentos de la trascendencia e importancia de la seguridad de los sistemas y redes de información de los que depende, en gran medida, nuestra sociedad actual. Unos sistemas que tienen ante sí una lista interminable de amenazas y potenciales delitos que les afectan y que pueden provenir de muy diferentes frentes: hackers (intrusos que penetran en redes corporativas con diferentes fines), ciberdelincuentes, terroristas, mafias, servicios secretos e, incluso, usuarios internos malintencionados o "despistados".

La comunidad internacional, consciente de esta situación, ha ido reaccionando en los últimos años creando estructuras operativas que protegieran el espacio cibernético en todas sus manifestaciones y ámbitos. Aquí es donde entran en juego los denominados CERTs *(Computer Emergency Response Team)* o CSIRTs *(Computer Security and Incident Response Team)*, organizaciones enfocadas a asegurar que la gestión de sistemas de información se realiza de forma adecuada para resistir los ataques en sistemas interconectados, limitar el daño y asegurar la continuidad de los servicios críticos a pesar de ataques exitosos, accidentes o fallos.

No hay que olvidar que incluso la mejor infraestructura de seguridad de información no puede garantizar que una intrusión no acabe por afectar a un equipo. De hecho, cuando se produce cualquier incidente de seguridad en un ordenador es crítico para una organización contar con un protocolo eficaz de respuesta. En este sentido, la velocidad con la cual se reconozca, analice y responda a un incidente limitará el daño y bajará el coste de la recuperación.

El primer CERT *(véase artículo anterior en esta misma revista)* perteneciente al *Software Engineering Institute* (SEI) de la *Carnegie Mellon University*, fue creado en 1988 a raíz del ataque del gusano Morris que afectó a un 10% de los sistemas de Internet. Otras universidades norteamericanas siguieron el ejemplo y pronto la creación de este tipo de equipos se extendió a otros organismos, tanto públicos como privados, y a otros países de todo el mundo.

Distintas tipologías de CSIRTs

En la actualidad, por tanto, existen más de 250 CSIRTs en todos los ámbitos de la sociedad, de muy distintas formas y tamaños. Algunos equipos apoyan a un país entero (por ejemplo el Centro de Coordinación de Equipo de Respuesta de Emergencia de Japón -JPCERT/CC-); otros pueden proporcionar la ayuda a una región particular, como APCERT hace para el área de Asia-Pacífico; o dar servicio a una universidad u organización comercial, etc.

En términos generales, los CSIRTs se clasifican atendiendo a la comunidad o al tipo de ámbito al que se enfocarán los servicios que se presten. En la actualidad se distinguen los siguientes "sectores":

- **Sector académico:** prestan servicios a centros académicos y educativos, como universidades o centros de investigación, y a sus campos virtuales. El grupo atendido

por estos CSIRTs está formado por el personal y los estudiantes de las universidades. Un ejemplo de ello son: IRIS-CERT (de Red.es) o esCERT-UPC (Universidad Politécnica de Cataluña).

- **Comercial:** prestan servicios comerciales a un grupo de clientes que pagan por ello. Suele pertenecer a una consultora de seguridad y, por lo general, se contratan diversos servicios como monitorización de sistemas, formación, etc. Un ejemplo de ello es la actividad de TB-Security.
- **Infraestructuras críticas:** se centran principalmente en la protección de la información crítica y de la información y las infraestructuras críticas (entendiendo como tal a aquella infraestructura o servicio cuya incapacitación o destrucción puede tener un grave impacto en la seguridad nacional y en el bienestar económico y/o social de un país). Entre estas infraestructuras podrían citarse: sistemas de control aéreo, banca y finanzas, Gobierno central, defensa civil, telecomunicaciones, prensa, servicios de rescate, energía/educación, salud pública, industria, servicios de información, seguros, justicia, defensa, monumentos nacionales, plantas nucleares, agua, fuentes de gasóleo, gasolina, policía, sistema postal, basuras, seguridad social, transporte, hacienda.

Países con CERTs que sirven a infraestructuras críticas (CI) podemos encontrar a: Australia, Austria, Canadá, Finlandia, Francia, Alemania, India, Corea, Estados Unidos, Malasia, Holanda, Nueva Zelanda, Noruega, Reino Unido, Rusia, Singapur o Suiza.

- **Gubernamental:** su objetivo es asegurar la infraestructura IT de un Gobierno y la disponibilidad de los servicios gubernamentales ofrecidos a la población. La comunidad a la que está dirigido son las administraciones y sus distintos organismos. Es el caso del recientemente creado CCN-CERT en España (se analiza en el siguiente apartado).
- **Interno:** únicamente prestan servicios a la organización a la que pertenecen, lo que describe más su funcionamiento que su pertenencia a un sector. Numerosas organizaciones de telecomunicaciones y bancos, por ejemplo, cuentan con sus propios equipos.
- **Información y comunicaciones:** sector financiero, transporte, electricidad. Un ejemplo, es el sistema de monitorización propios de la Corporación Catalana de Radio y Televisión (CTTV) y sus planes de contingencia y sistemas de gestión de incidencias propios.
- **Militar:** responsable de la infraestructura TI para la defensa nacional. Su comunidad suele ser una institución relacionada con los estamentos militares. Un ejemplo podría ser el NATO Computer Incident Response Capability (NCIRC) que da servicio a 32 redes y que proporciona servicios técnicos y de apoyo a los servicios legales para responder a los incidentes de seguridad informática dentro de la OTAN.
- **Nacional:** se considera un punto de contacto de seguridad del país y ofrece su servicio a toda la nación. Este tipo de CISRTs no suele tener una comunidad directa, pues se limita a desempeñar un papel de intermediario o de coordinación del resto de equipos. Un ejemplo el es Centro de Coordinación de Japón (JPCERT/CC).
- **PYME:** se trata de un CERT organizado por sí mismo que presta servicios a las empresas del ramo o a un grupo de usuarios similar. Un ejemplo es el recientemente creado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO) para PYMES.
- **De soporte:** se centran en productos específicos. Suelen tener por objetivo desarrollar y facilitar soluciones para eliminar vulnerabilidades y mitigar posibles efectos negativos.

Hay que reseñar, asimismo, que cabe la posibilidad de que varios CERTs compartan una parte de sus comunidades. Se hace imprescindible, por lo tanto, que exista una estrecha colaboración entre CERTs de un mismo entorno, con distribución de tareas y gestión de incidentes compartida.

> Información sobre vulnerabilidades; investigación, formación y divulgación de las mejores prácticas; y el soporte ante incidentes y vulnerabilidades son tres funciones principales del CERT

CCN-CERT

En el caso de España, el CERT gubernamental, CCN-CERT, comenzó a fraguarse en el año 2004 al crearse el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia (R.D. 421/2004). Asimismo, el Plan AVANZA 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas (Ministerio de Industria, Turismo y Comercio), en su Anexo I, menciona el desarrollo de una red de centros de seguridad cuyo principal objetivo sea crear una infraestructura básica de centros de alerta y respuesta ante incidentes de seguridad que atienda a las demandas específicas de los

diferentes segmentos de la sociedad. Sectores críticos, agencias gubernamentales, Administración Pública, PYMEs, Grandes Corporaciones y ciudadanos recibirán el adecuado asesoramiento por parte de estos centros.

En este sentido, se habla de la creación de centros de seguridad y de establecer los procedimientos y protocolos que permitan coordinar sus funciones y actuaciones. En este mismo texto se adelanta la creación de un CERT para la Administración/Gubernamental, un CERT para PYMEs y una unidad de lucha contra la violación de la privacidad (lucha contra el spam, el phishing y otros fraudes).

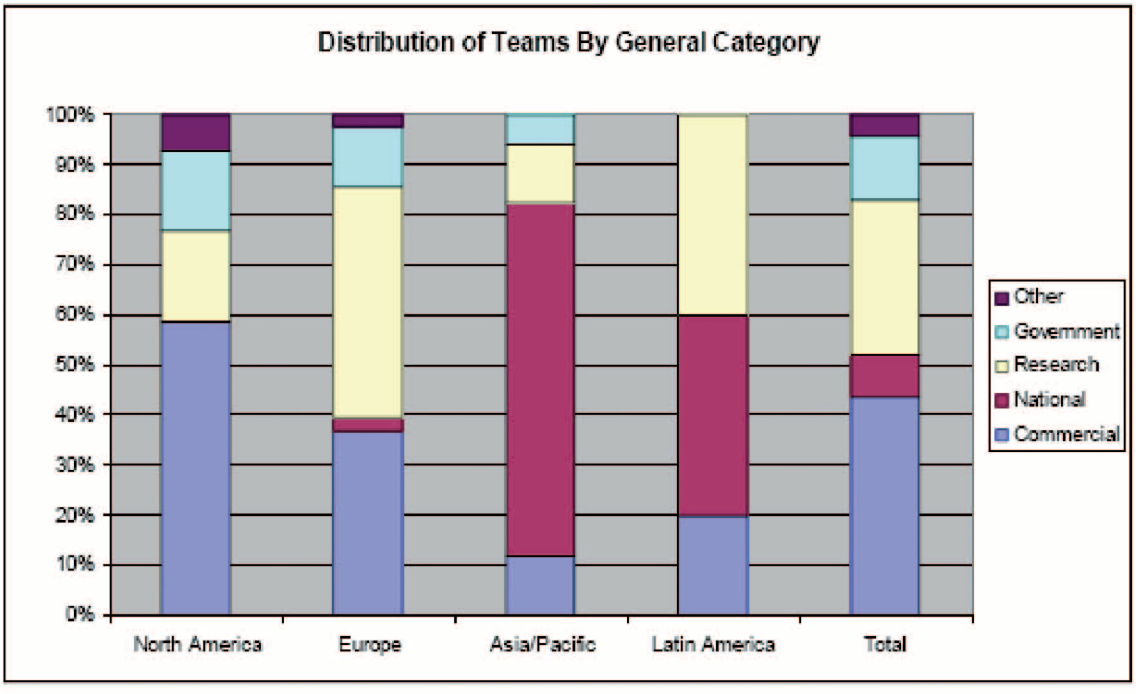
De esta forma, en el año 2006 empezó a gestarse la creación del CCN-CERT (presentado a principios de este 2007), el CERT gubernamental español cuya principal misión es ser el centro de alerta nacional que ayude a todas las Administraciones Públicas a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir.

Tres son sus grandes líneas de actuación: información sobre vulnerabilidades; investigación, formación y divulgación de las mejores prácticas para la seguridad de las tecnologías de la información y las comunicaciones; y el soporte ante incidentes y vulnerabilidades, mediante servicios de apoyo técnico y coordinación entre todas las administraciones españolas.

Desde su creación, el CCN-CERT está desarrollando una intensa labor de acercamiento a los responsables TIC de todos los organismos estatales (generales, autonómicos y locales) y ha intensificado su presencia en los foros internacionales. Buena prueba de ello es su ingreso en la principal organización del mundo de este tipo de equipos, el FIRST *(Forum of Incident Response Teams)*, así como en el último encuentro celebrado en Madrid organizado por el CERT CC (CERT *Coordination Center, Carnegie Mellon University*) y destinado a todos los CSIRTs de responsabilidad nacional.

En dicho encuentro estuvieron invitados los 38 CSIRTs existentes con responsabilidad nacional y sirvió para debatir los principales desafíos a los que se enfrentan este tipo de equipos en un mundo cada día más interconectado, con un número de incidentes en continuo crecimiento y con una gran diversidad de comunidades de usuarios que hacen necesario contar con un apoyo global en cuestiones de seguridad de la información.

Alemania, Argentina, Australia, Bélgica, Brasil, Brunei, Canadá, Chile, China, Corea del Sur, Dinamarca, El Salvador, Eslovenia, España, Estados Unidos, Filipinas, Finlandia, Francia, Holanda, Hong Kong, Hungría, India, Indonesia, Japón, Lituania, Malasia, Méjico, Nueva Zelanda, Noruega, Polonia, Qatar, Rusia, Singapur, Suecia, Tailandia, Turquía, Reino Unido y Vietnam son los países que estuvieron presentes en Madrid.



Fuente: *"State of the Practice of Computer Security Incident Response Teams (CSIRTs)"*. Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek