Red CERT, garantía de seguridad en todo el mundo

SU OBJETIVO FUNDAMENTAL ES COORDINAR A LOS DIFERENTES CSIRT DE TODO EL MUNDO, COMPARTIENDO INFORMACIÓN SOBRE VULNERABILIDADES Y ATAQUES

CCN-CERT
Centro Criptológico Nacional

En el número anterior de esta revista se informaba sobre la presentación del Servicio de Respuesta a Incidentes de Seguridad para la Administración por parte del Centro Criptológico Nacional. La creación del CCN-CERT, que viene a suplir la ausencia de un CERT gubernamental a imagen y semejanza de los existentes en todos los países de nuestro entorno, posibilitará su presencia en los principales foros internacionales, en los que compartir objetivos, ideas e información sobre la seguridad de forma global.

En 1988, tan sólo existían unos 70.000 hosts interconectados y hasta ese momento la seguridad no había sido un aspecto a tener en cuenta. Sin embargo, el 2 de noviembre de 1988 aparece el *Gusano de Morris*, creado por el estudiante predoctoral, graduado en Harvard, Robert Tappan Morris, de 23 años. El gusano usaba un defecto del sistema operativo Unix para reproducirse hasta bloquear el ordenador. En pocas horas el 10% de los ordenadores conectados dejaron de funcionar correctamente, lo que supuso un coste de 15 millones de dólares. Las copias del virus llegaban a través del correo electrónico que, una vez instalado, realizaba copias repetidas de sí mismo mientras intentaba propagarse, logrando que muchas veces los ordenadores se quedasen sin recursos.

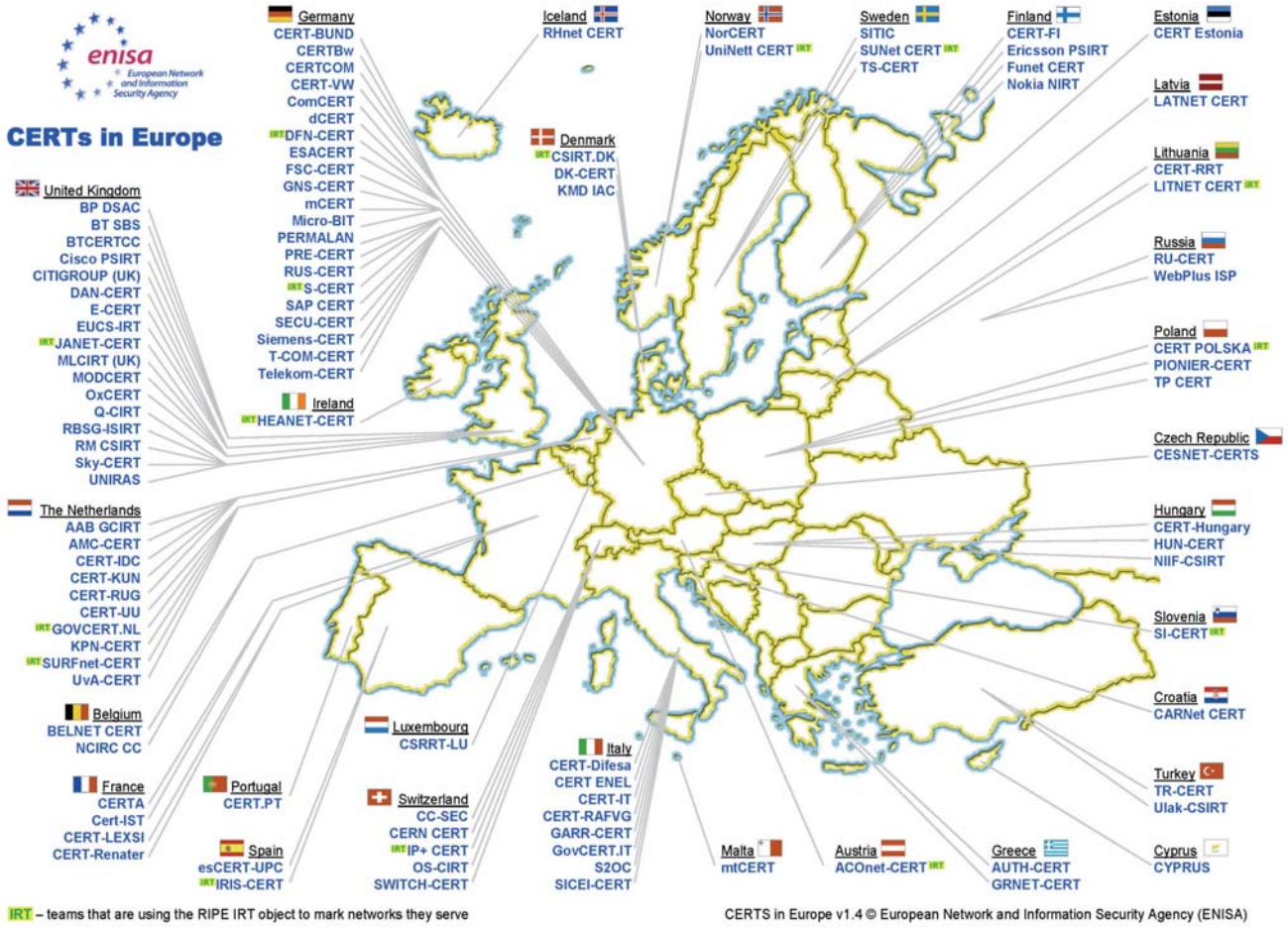
> Resulta fundamental que cualquier equipo de respuesta a incidentes se mantenga en contacto con otros equipos del resto del mundo en caso de ataque y se asegure de qué fuentes de información son fiables

Aunque sus abogados aseguraban que Morris *"intentaba ayudar a la seguridad de Internet cuando su programa se salió de su control por accidente", la fiscalía argumentó que el gusano "no se trató de un error, sino de un ataque contra el gobierno de los Estados Unidos"*. Finalmente Morris fue condenado a tres años de libertad condicional, una multa de 10.000 dólares y 400 horas de servicio a la comunidad.

Una de las principales consecuencias de este virus fue que el Departamento de Defensa norteamericano comenzó a tener en cuenta la seguridad informática y encargó a la Universidad *Carnegie Mellon*, en Pittsburgh, la creación de un equipo capaz de hacer frente a este nuevo tipo de amenazas. El resultado fue la constitución del denominado Computer Emergency Response Team (CERT); es decir, Equipo de Respuesta a Incidentes de Seguridad Informática (www.cert.org)

Bajo estas mismas siglas comenzaron a formarse otros grupos en distintas universidades norteamericanas encargados de estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas.

A su vez, empezó a hablarse de CSIRT *(Computer Security and Incident Response Team)* para completar el concepto de CERT y ofrecer, como valor añadido, los servicios preventivos y de gestión de



seguridad. Hoy en día se emplean de forma similar ambos términos.

Poco tiempo después, a principios de la década de los noventa, la idea se trasladó a Europa y, gracias al apoyo del programa técnico **TERENA** (www.terena.org), empezaron a crearse los primeros CERT en el Viejo Continente. De hecho, en la actualidad TERENA continúa siendo el principal foro europeo de CERT en el que se colabora, innova y comparte información con el fin de *"promover y participar en el desarrollo de unas infraestructuras de información y telecomunicaciones de alta calidad en beneficio de la investigación y la educación"*, tal y como recogen sus estatutos. Asimismo, auspicia un task force para promover la cooperación entre CSIRT en Europa.

Situación en España

A finales de 1994 se formó el primer Equipo de estas características en nuestro país, en concreto, en la Universidad Politécnica de Cataluña. Se trata del **esCERT-UPC** (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas), surgido como primer centro español dedicado a asesorar, prevenir y resolver incidencias de seguridad en entornos telemáticos. Este equipo, totalmente operativo en la actualidad, ofrece un servicio de respuesta a incidentes, así como formación, auditoría, consultoría e implantación de soluciones en estos entornos.

Conviene reseñar, asimismo, que de esCERT-UPC surgió en el año 2000, como spin-off, la empresa InetSecur que, en 2005 se unió a SecurityXperts, formando TB-Security (contratista principal de la capacidad inicial del CCN-CERT, Equipo Gubernamental y tercero en constituirse en nuestro país).

Un año después, en 1995 se formó **el Iris-CERT**, servicio de seguridad de RedIRIS (red académica y de investigación nacional que desde enero de 1994 hasta 2003 fue

gestionada por el Consejo Superior de Investigaciones Científicas y, a partir de enero de 2004, pasó a integrarse como un departamento con autonomía e identidad propias en el seno de la Entidad Pública empresarial **Red.es**, adscrita al Ministerio de Industria, Turismo y Comercio). La finalidad de este equipo es la detección de problemas que afecten a la seguridad de las redes de centros de RedIRIS, así como la actuación coordinada con dichos centros para poner solución a estos problemas. También se realiza una labor preventiva, avisando con tiempo de problemas potenciales, ofreciendo asesoramiento a los centros, organizando actividades de acuerdo con los mismos, y ofreciendo servicios complementarios.

En los años siguientes, tanto esCERT-UPC como Iris-CERT, pasaron a formar parte de foros internacionales como TF-CSIRT, Trusted Introducer o FIRST y participaron en varios proyectos de desarrollo. Asimismo, en el año 2000 Iris-CERT, promovió y moderó el **Foro ABUSES**, cuyo principal objetivo es crear un entorno de confianza entre técnicos para el intercambio de información, experiencias y coordinación sobre los problemas de inseguridad en la Red. Dicho foro está enfocado a técnicos y profesionales de ISP que gestionan o están interesados en solucionar incidentes y quejas de tipo abuse en Internet.

Por último, y ya en el año 2004, empezó a fraguarse lo que sería el CERT gubernamental español, a raíz del Real Decreto 421/2004, que regula la actividad del Centro Criptológico Nacional (CCN), dependiente del CNI. Así, y tras dos años de intenso trabajo, a principios de este 2007, se presentó el **CCN-CERT**, cuyo principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las Administraciones Públicas (tanto la administración general, como la autonómica y local).

De igual modo, el Instituto Nacional de Tecnologías de la Comunicación (**INTECO**), está formando el CERT para el mundo de la pequeña y mediana empresa y los ciudadanos.

Ámbito internacional

La continua proliferación de CERT en todo el mundo y en todos los ámbitos de la sociedad (administración, universidad, investigación, empresa, etc.) ha ido tejiendo en los últimos años una tupida malla de seguridad informática que, necesariamente, ha de estar interconectada, dado que, si existe algún sector globalizado, con ausencia absoluta de fronteras, este es, sin lugar a dudas, el de Internet. Por ello, es imprescindible compartir objetivos, ideas e información sobre la seguridad de forma global. Del mismo modo, resulta fundamental que cualquier equipo de respuesta a incidentes se mantenga en contacto con otros equipos del resto del mundo en caso de ataque y se asegure de qué fuentes de información son fiables. De ahí, la importancia de los distintos foros internacionales existentes, tanto de ámbito europeo (TERENA), como mundial (FIRST).

El primero y más importante por su representatividad mundial es el FIRST *(Forum of Incident Response and Security Teams)*. Desde su creación en noviembre de 1990, este foro ha pasado de contar con nueve equipos de seguridad de EEUU y uno europeo, a los más de 180 miembros que lo componen en la actualidad, procedentes del ámbito gubernamental, económico, educativo, empresarial y financiero (a él pertenecen o están a punto de pertenecer los tres CERT existentes por el momento en España, incluido el de reciente incorporación: CCN-CERT).

> El CCN-CERT participará como Gold Sponsor en el 19º Congreso Anual del FIRST, que este año se celebra en Sevilla, entre los días 17 y 22 de junio

Su objetivo fundamental es coordinar a los diferentes CSIRT de todo el mundo, compartiendo información sobre vulnerabilidades y ataques a nivel global y divulgando medidas tecnológicas que mitiguen el riesgo de ataques a sistemas y usuarios conectados a Internet, que dan servicio a sus respectivas comunidades. También se encuentra entre sus cometidos, el fomentar la creación de nuevos equipos de coordinación de emergencias, tanto de ámbito nacional como a nivel corporativo.

Otra de sus actividades es la organización de un Congreso Anual que, precisamente, este año, en su decimonovena edición, tendrá lugar en Sevilla, entre los días 17 y 22 de junio. Este encuentro, en el que el CCN-CERT participará como *Gold Sponsor*, reunirá a los principales Equipos de Respuesta a Incidentes del mundo.

La protección de la información privada y personal; la prevención del fraude, robo y pérdidas accidentales, así como la conservación del prestigio de la comunidad son las tres ideas básicas sobre las que girará el encuentro de este año.

Por último, conviene reseñar, que prácticamente la mitad de los CERT existentes en el mundo se sitúan en Europa. Así, países como Alemania (con 21 CERT), Reino Unido (17) u Holanda (10) encabezan la lista por número de equipos destinados a asistir a sus respectivas comunidades. Incluso, compañías como Nokia, Ericsson o Siemens, cuentan con su propio CERT.