Trofeos de la Seguridad TIC 2008

Más de 150 personas asistieron a la ceremonia de entrega de los "Trofeos de la Seguridad TIC 2008" de RED SEGURIDAD

El secretario de Estado, Alberto Saiz, presidió la III edición de los premios

A la izquierda, José Ramón Borredá, editor de RED SEGURIDAD, recibe a Alberto Saiz, secretario de Estado director del CNI, a su llegada a la celebración, junto con Alfonso Mur, presidente del Consejo Técnico Asesor de la revista (a la derecha).

SeMarket, el Centro Criptográfico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), Lexmark, S21sec e Hispasec Sistemas fueron los triunfadores de unos galardones muy competidos. El acto también contó con la presencia de Enrique Martínez, director general del Instituto Nacional de Tecnologías de la Comunicación (INTECO), así como autoridades de la Comunidad de Madrid, la Agencia Española de Protección de Datos (AEPD), el CCN y la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM).

Tx: Mercedes Oriol Vico.
Ft: Fermín Sánchez González.

EL PASADO 19 de noviembre, RED SEGURIDAD celebró, en el Hotel Meliá Castilla, la entrega de los "Trofeos de la Seguridad TIC", bajo la presidencia del secretario de Estado del Ministerio de Defensa y director del Centro Nacional de Inteligencia (CNI), Alberto Saiz. La tercera edición de estos premios se convirtió en todo un éxito, ya que al acto institucional asistieron más de 150 profesionales del sector, procedentes de empresas, organismos públicos y asociaciones. Otras autoridades que compartieron presidencia, junto con José Ramón Borredá, editor de la revista y presidente de Editorial Borrmart, y Alfonso Mur, presidente del Consejo Técnico Asesor (CTA) de RED SEGURIDAD, fueron: Enrique Martínez, director general del Instituto Nacional de Tecnologías de la Comunicación (INTECO); Fermín Montero, subdirector general de Innovación Tecnológica de la Comunidad de Madrid; Mª José Blanco, subdirectora general del Registro de Protección de Datos de la Agencia Española de Protección de Datos (AEPD); Emilio Aced, subdirector general de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM); Luis Jiménez, subdirector adjunto del Centro Criptológico Nacional (CCN); y Mercedes Pérez, directora del Gabinete del secretario de Estado.

Premiados de la tercera edición

Los ganadores de esta tercera edición han sido: la firma SeMarket, por su producto de control de acceso biométrico "BioSeLogOn"; el Centro Criptográfico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), por los servicios que ofrece desde su CERT; la empresa Lexmark, por los sistemas de seguridad implantados en sus dispositivos multifunción; la compañía S21sec, por sus planes de formación continua en tecnología de seguridad; e Hispasec Sistemas, por el fomento

"A día de hoy, más de 1.300 responsables de seguridad de toda la Administración están registrados en el CCN-CERT"

Alberto Saiz
Secretario de Estado y director del CNI

¿Qué supone para ustedes ganar el premio al servicio de seguridad TIC, por el Equipo de Respuesta ante Incidentes de Seguridad de la Información (CERT) del Centro Criptológico Nacional (CCN)?
Para nosotros es un reconocimiento a la labor emprendida hace ya más de tres años, cuando se empezó a fraguar la Capacidad de Respuesta ante incidentes de Seguridad de la Información (CCN-CERT). Entonces, y gracias al conocimiento adquirido sobre amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones durante toda su historia por el Centro Nacional de Inteligencia (CNI), y a través del Centro Criptológico Nacional (CCN), se decidió crear un nuevo servicio con el que contribuir, de forma activa, a la mejora del nivel de seguridad en los sistemas de información de las administraciones públicas españolas (general, autonómica y local).

Este premio, junto con la buena acogida que ha tenido entre los responsables de seguridad de toda la Administración, nos confirma que estamos en el camino adecuado y nos da nuevas fuerzas para afrontar, junto con el resto de organismos, los nuevos retos que tenemos ante nosotros.

¿Cuántos organismos están utilizando ya este servicio y se están beneficiando del CCN-CERT?
En realidad, podríamos decir que todas las administraciones públicas españolas y sus distintos organismos están utilizando, de una u otra manera, alguno de nuestros servicios e, incluso, y de forma colateral, todos los ciudadanos que acceden a nuestro portal (www.ccn-cert.cni.es). De hecho, mensualmente recibimos una media de 50.000 visitantes únicos que pueden acceder a una parte importante de la información publicada por el CCN-CERT, cuya principal función es reducir los riesgos de seguridad de cualquier sistema.

No obstante, y centrándonos en nuestra "comunidad" (en el ámbito de los CERT, se entiende por tal los miembros del grupo a los que se presta el servicio), a día de hoy, son más de 1.300 los responsables de seguridad de toda la Administración los que están registrados en la parte privada del portal, que no olvidemos que es nuestra principal herramienta y punto de contacto con todos ellos. A través de este registro reciben todo tipo de información de primera mano, no sólo sobre el modo de abordar cualquier incidente, sino también -y sobre todo- sobre cómo evitarlo a través de guías, herramientas y alertas de vulnerabilidades actualizadas diariamente. De este número, aproximadamente el 65 por ciento pertenece a la Administración General del Estado (AGE); el 23 por ciento, a la autonómica; el 18 por ciento, a la local; un tres por ciento a universidades; y un uno por ciento, a organizaciones internacionales con las que mantenemos una estrecha colaboración.

En cuanto a la gestión de incidentes, y dada la política del CCN-CERT de mantener la confidencialidad sobre cualquier información de la Administración solicitante de ayuda, no podemos ofrecer datos concretos, pero sí señalar que han sido numerosos los organismos que han recurrido a nuestro equipo para afrontar algún incidente en estos dos últimos años (particularmente de fraude, código malicioso, intentos de intrusión o ataques DoS y DDoS).

Otro de nuestros servicios más solicitado es la formación. El CCN ha ofertado desde el año 2006 cursos a más de 1.200 funcionarios, procedentes de 110 organismos diferentes y repartidos en los 18 cursos y 1.300 horas lectivas que lleva a cabo de forma presencial (a los que hay que sumar los cursos impartidos a distancia). De igual forma, en las jornadas y seminarios de concienciación y sensibilización, así como en las presentaciones del CCN-CERT realizadas por diversas autonomías (Madrid, Comunidad Valenciana, Aragón, Asturias, Cantabria, Castilla y León...), han sido más de 700 los responsables de seguridad que han asistido a las mismas.

Pero además, y conviene no olvidarlo, el CCN-CERT tiene un papel muy importante en el ámbito internacional. Al actuar como CERT gubernamental español está presente en las principales organizaciones internacionales en las que se aborda continuamente la forma y el modo de atajar cualquier posible ataque o incidente (ENISA, OTAN, FIRST, TERENA...). Esta participación nos lleva a colaborar activamente junto con otros equipos e instituciones en la resolución de incidentes transfronterizos en los que se nos pide ayuda y colaboración y que, por supuesto, siempre prestamos.

¿Qué aporta este servicio a la Administración?
Son numerosas las aportaciones y servicios del CCN-CERT puestos a disposición de toda la Administración. No obstante, yo destacaría las siguientes, en función del momento y la forma en que se actúe ante un incidente: servicios reactivos (gestión de incidentes; información sobre vulnerabilidades, alertas y avisos; o análisis de código dañino remitido por las diferentes administraciones), proactivos (boletines e informes restringidos, auditorías y evaluaciones de seguridad de los servicios web que así lo requieren; desarrollo de herramientas de seguridad y detección temprana de intrusiones) y de gestión (análisis de riesgos, sensibilización y formación).

En definitiva, el CCN-CERT mantiene entre sus metas el facilitar una gestión

de incidentes de seguridad centralizada; coordinar una respuesta a unos tipos de incidentes específicos; proporcionar asistencia técnica directa que se requiera y las referencias en configuraciones de seguridad; forzar a proveedores a una respuesta adecuada ante vulnerabilidades detectadas y establecer relaciones con otros CERT y con las Fuerzas y Cuerpos de Seguridad del Estado.

En un mundo interconectado, en el que la seguridad debería plantearse como una estrategia global, ¿no sería óptimo llegar a aunar todos los CERT de seguridad en uno solo que controlase todas las incidencias?

Un único CERT no puede afrontar por sí solo el número creciente de amenazas a los que, hoy en día, están expuestos los sistemas de información de un país o, en este caso, de toda la Administración Pública. No obstante, sí que es cierto que resulta imprescindible la colaboración no sólo de los CERT de un país, sino de los equipos de todo el mundo para afrontar unas amenazas que no tienen fronteras. Por este motivo, uno de nuestros objetivos es ofrecer información, formación y herramientas para que las distintas administraciones, particularmente las autonomías, puedan desarrollar sus propios CERT (u otros servicios de gestión de seguridad centralizada, llámense CSIRT, COS o de otra forma), permitiendo al CCN-CERT actuar de catalizador y coordinador de CERT a nivel gubernamental. Nuestra voluntad, además, es la de apoyar a todos ellos, colaborar en la medida de nuestras posibilidades a su formación (facilitando información, herramientas de seguridad...) y, llegado el caso, ayudarles en la resolución de incidentes e, incluso, fomentar su participación en foros internacionales.

Por poner un ejemplo, en países como Alemania o Reino Unido el número de CERT se eleva hasta los 19 y 17, respectivamente (incluidos equipos de organizaciones privadas).

¿De qué manera mantienen la colaboración o el cruce de información, tanto con servicios de seguridad TIC privados, como con otros públicos existentes?

Antes de nada, debo decir que para el desarrollo de las funciones establecidas en el Real Decreto de su constitución (RD 421/2004), el Centro Criptológico Nacional (CCN) debe establecer la coordinación oportuna con las Comisiones Nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las Tecnologías de la Información y de las Comunicaciones (TIC). Esto implica mantener un contacto permanente con diversas instituciones y organismos implicados en la seguridad de la información. Así, mantenemos relaciones con la Administración Pública, infraestructuras críticas (CNPIC) y sectores estratégicos, Fuerzas y Cuerpos de Seguridad del Estado, otros CERT, ISP, empresas de *hosting*, registradores, etc. En este sentido, formamos parte del Grupo de CERT españoles públicos y privados reconocidos (CSIRT.es) y del Foro ABUSES (equipos ABUSE de ISP españoles promovido por RedIRIS). Además, hemos venido firmando diversos acuerdos con distintos organismos con el fin de colaborar mutuamente (FEMP, INTECO, etc.).

En cuanto al ámbito internacional, somos miembros de pleno derecho del FIRST (principal organismo que aglutina a los CERT de todo el mundo), del *NATO Cyber Defense Workshops*, del *European Government CERT Group* (EGC), del Terena TF-CSIRT y del Grupo de Trabajo de CERT Nacionales de ENISA. Asimismo, pertenecemos al *AntiPhishing WG* y al Programa SCP de Microsoft.

¿Está la Administración española preparada para defenderse ante un posible ciberataque?

Desgraciadamente, ningún sistema está libre de sufrir algún ataque, e incluso la mejor infraestructura de seguridad de información no puede garantizar que una intrusión acabe por afectar a un equipo. Pese a ello, y pese a que somos conscientes de la existencia de estos riesgos y amenazas y de la necesidad de que todos los organismos tomen conciencia de ello, podemos decir que la Administración española está preparada para defenderse ante un posible ciberataque.

La iniciativa del CCN-CERT, junto con otras desarrolladas en los últimos años, sigue la línea trazada en materia de seguridad de las TIC por los países más avanzados y por las organizaciones internacionales OTAN y Unión Europea, con quienes colaboramos activamente y con quienes mantenemos una estrecha relación para actuar, tanto de forma preventiva como reactiva, ante cualquier hipotético ataque.

Para afrontar las amenazas que se producen a través de las TIC, ademas de tecnología, ¿qué claves son necesarias?

El principal obstáculo con el que nos enfrentamos a la hora de afrontar estas amenazas es, por paradójico que resulte, la falta de concienciación en materia de seguridad de los usuarios de las TIC. De hecho, la ingenuidad, los errores y omisiones del personal autorizado y bienintencionado -pero desconocedor de buenas prácticas de seguridad- y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información constituyen una fuente principal de amenazas, que todos, en mayor o menor medida, conocemos (robo, pérdida o extracción de dispositivos de almacenamiento; versiones descifradas de archivos confidenciales, claves de acceso públicas, etc.).

No hay que olvidar que a medida que las tecnologías empleadas para proteger la información se hacen más sofisticadas, los ataques centrados en explotar las debilidades de la persona se incrementan.

Por ello, consideramos que uno de los pilares básicos de la seguridad de la información es la formación y concienciación del personal. Para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación, es preciso tomar conciencia de los riesgos (con medidas procedimentales, organizativas y técnicas), utilizar herramientas de seguridad (medidas técnicas) y mantener inspecciones que acrediten el buen uso de estas prácticas y herramientas. ■

"Consideramos que uno de los pilares básicos de la seguridad de la información es la formación y la concienciación del personal"