Llega Crypt4you, formación 'online' y gratuita sobre criptografía y Seguridad

Hace más de un año, dos de los más reconocidos expertos españoles en criptografía, Jorge Ramió (profesor titular de la Universidad Politécnica de Madrid -UPM- y miembro del Consejo Técnico Asesor de RED SEGURIDAD) y Alfonso Muñoz (doctor de Telecomunicaciones por la UPM), lanzaron Intypedia, un exitoso proyecto de Enciclopedia de la Seguridad de la Información y cuya última lección se publicará este mes. Pero, en su afán de continuar mejorando al servicio de la divulgación, presentan un nuevo formato de enseñanza *online*, gratuita y colaborativa: el Aula Virtual de Criptografía y Seguridad de la Información Crypt4you (www.crypt4you.com), un proyecto de innovación educativa sin ánimo de lucro que nace dentro de la Red Temática de Criptografía y Seguridad de la Información (Criptored), en la UPM. La voluntad de este proyecto es abrir las puertas de la universidad a toda la sociedad y poner la criptografía y la Seguridad de la Información a disposición de todos los interesados.

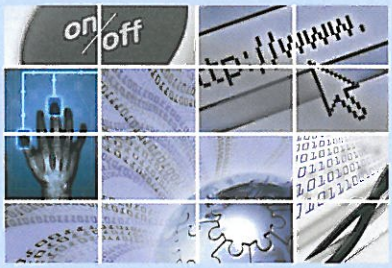
Del mismo modo que en Intypedia, los autores de los cursos serán preferiblemente investigadores y profesores universitarios miembros de Criptored. Una de las características distintivas de Crypt4you es la publicación y entrega de lecciones en formato *eLearning* todos los días 1 y 15 de cada mes. El primer curso es "El algoritmo RSA", del profesor Jorge Ramió, y está compuesto por 10 lecciones que se publican desde el pasado 15 de marzo y hasta el 1 de agosto de 2012. Las lecciones contemplan un conjunto de ejercicios y prácticas, un test de evaluación personal; con la última lección de cada curso se publicará un examen final. Además, se invita a los alumnos que sigan estos cursos con participación activa a través de las redes sociales Facebook y Twitter de Crypt4you.

Aumentan los ataques de nivel crítico a la Administración

El CCN-CERT revela que el *hacktivismo* continuará al alza en 2012 y recomienda disponer de una Estategia Nacional de Ciberseguridad como la mejor forma de combatirlo.

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional (CCN-CERT), adscrito al Centro Nacional de Inteligencia, (CNI), dio a conocer su resumen de amenazas de 2011 y las predicciones de seguridad de cara al presente ejercicio, recogidas en su informe "Ciberamenazas 2011 y tendencias 2012".

Según este análisis, aumentaron los ataques dirigidos contra la Administración Pública española, registrados por los distintos sistemas de detección del CCN, pero lo más preocupante es que se eleva el nivel de criticidad (durante 2011 se registraron 93 incidentes catalogados con nivel de severidad "muy alto" o "crítico"). La introducción de código dañino en los sistemas, las intrusiones mediante ataques a páginas, así como el contacto con IP maliciosas, son algunos de los incidentes más recurrentes sufridos por nuestras administraciones. También se hace eco el CCN-CERT del avance del ciberespionaje, cuyo origen hay que buscarlo tanto en las empresas como en los propios Estados; de la evolución del *hacktivismo* y la colaboración entre el mundo tecnológico y el físico; y de la evolución del troyano bancario ZeuS, entre otros.



De cara a este año 2012, este organismo considera, entre otros puntos, que los *hacktivistas* aumentarán aún más su protagonismo; continuarán los ataques contra autoridades de certificación; se detectarán nuevas familias de *malware* y se potenciará la figura del intermediario (encargada de encontrar clientes que compren datos previamente robados). De igual modo, el informe alerta sobre los peligros en las redes sociales, los dispositivos móviles, los servicios *cloud* y los ataques distribuidos de denegación de servicio (DDoS). Finalmente, el estudio resalta la necesidad de impulsar la Estrategia Nacional de Ciberseguridad en España -que todavía se encuentra en periodo de desarrollo- con la que articular una respuesta adecuada, similar al resto de países de nuestro entorno. ■

El Consejo de Europa insta a los países miembros a proteger los derechos humanos en buscadores y RRSS

El Consejo de Europa ha decidido 'mojarse' en un asunto espinoso: ha aprobado dos recomendaciones en las que solicita a sus 47 Estados miembros que protejan los derechos humanos en los motores de búsqueda y las redes sociales (RRSS), especialmente los derechos relacionados con la libertad de expresión, el acceso a la información, la libertad de asociación y el derecho a la vida privada. Esto se traduce en un mandato para que cada país trabaje estrechamente con los proveedores de los motores de búsqueda, con el objetivo de mejorar la transparencia en la forma en que proporcionan acceso a la información, en particular, sobre el criterio que se utiliza para seleccionar, clasificar o eliminar resultados de las búsquedas. En cuanto a las redes sociales, la recomendación se orienta a que fomenten seriamente la concienciación de los usuarios respecto a sus derechos.

Estas iniciativas indican que, por fin, la Unión Europea toma conciencia de cómo las TIC y su uso obligan a revisar el concepto tradicional del derecho. Muestra de ello es que el *hacking* de sistemas será considerado como un delito que podría ser penado con hasta dos años de cárcel, en virtud de una propuesta del Parlamento Europeo, que obtuvo 50 votos a favor, uno en contra y tres abstenciones. Asimismo, la posesión y distribución de *software* pirata también pasará a constituir delito y las empresas serían responsables si cometen ataques en su beneficio.