Internet y nuevas tecnologías

Roberto Plá
Teniente coronel de Aviación
http://robertopla.net/

EVENTOS

CYBERCAMP 2014

Desde pequeños hemos oído a nuestros padres prevenirnos de los peligros que nos acechaban: "Mira antes de cruzar la calle", "abrígate no te resfríes", "no abras la puerta a extraños"…La experiencia convertía a nuestros mayores en guías adecuados para sortear los peligros. Sin embargo uno de los efectos de la revolución digital es que muchos padres ya no pueden advertir a sus hijos de determinados peligros, sencillamente, porque los desconocen. ¿Que podemos hacer para proteger a nuestros pequeños de los peligros que les acechan en el mundo moderno?. Hay que acompañarles en su descubrimiento de las nuevas tecnologías. No podemos desentendernos alegando que “no entendemos” o incluso esperar que sean ellos quienes nos expliquen el funcionamiento de las aplicaciones del teléfono o los peligros que conlleva la indiscreción. Aunque no seamos 'nativos digitales' como ellos, debemos seguir usando nuestro sentido común y nuestro criterio adulto para que sus descubrimientos en el maravilloso dominio de lo digital tengan un recorrido educativo que les ayude a formar un criterio y crecer en conocimiento y valores.

Participar en actividades de tipo cultural y formativo es un buen recurso, pero estas actividades no son muy frecuentes. Esta es una de las razones por la que Cybercamp se desarrolló en Madrid, a primeros del mes de diciembre con un éxito abrumador de público. Pocas veces pueden verse “talleres charlas” aptas para familias completas en el marco de un congreso internacional de seguridad del más alto nivel.

CyberCamp reunió a grandes figuras de carácter internacional con ponentes como Chema Alonso, Fermín J Serna, Richard Stallman, Joanna Rutkowska , Marc "Van Hauser" Heuse, Marion Marschalek y otros destacados hackers y expertos en ciberseguridad que participaron en 15 ponencias de primer nivel, 21 conferencias y mesas redondas especializadas, 17 talleres técnicos, 25 talleres para familias, un gran número de sesiones para emprendedores, proyectos lean, un nutrido Hackatón y variadas áreas de desarrollo en paralelo, además del Foro de Empleo.

En esta su primera edición, las cifras superaron con creces las expectativas marcadas por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), y el Instituto Nacional de Ciberseguridad (INCIBE), organizadores del evento.

Sin duda alguna uno de los principales aciertos de Cybercamp ha sido conjugar las actividades dirigidas a expertos con la presencia y participación de todo tipo de públicos, convirtiéndose en una auténtica fiesta de la cultura y la seguridad digital en la que han participado más de 5.800 asistentes.

Con el objetivo de fomentar el emprendimiento y premiar las ideas más innovadoras en ciberseguridad, INCIBE organizó, en colaboración con la Empresa Nacional de Innovación (ENISA), dos iniciativas clave: un certamen en el que participaron 16 proyectos, y un taller de habilidades para elegir al mejor proyecto emprendedor.

Como Mejor Proyecto en Ciberseguridad, los premiados fueron Enigmedia, Prot-On y SMiD y , que obtuvieron ayudas para su desarrollo por importes de 7.000, 5.000 y 3.000 euros respectivamente.

En cuanto al Mejor Proyecto Emprendedor en Ciberseguridad, el galardón fue para Virtual Security Box.

Otra de las iniciativas que se ha llevado a cabo en CyberCamp para descubrir a las futuras promesas del mundo de la ciberseguridad y potenciar su carrera en el sector, ha sido el concurso de “Retos de Ciberseguridad”.

El Foro de Empleo ha puesto en contacto a 20 entidades públicas y privadas con talentos y futuros profesionales de ciberseguridad. Empresas como Symantec, Telefónica, Indra o las Fuerzas y Cuerpos de Seguridad del Estado han recopilado más de 1.000 curriculums y han realizado 320 entrevistas a candidatos.

Una experiencia a cuya evolución habrá que estar atentos en las próximas ediciones.

http://delicious.com/rpla/raa840a

HACKING

ATAQUES A MINISTERIOS ESPANOLES

A mediados de diciembre, el diario "El País" se hizo eco de los ataques sufridos por organismos públicos españoles, entre los que se encuentran diversos ministerios, Ministros y se-

cretarios de Estado del Gobierno de España. Los intentos de infiltración procedieron de grupos coordinados de hasta 20 hackers probablemente con intereses mercenarios.

El software utilizado en los ataques se diseñó específicamente para esta operación y explota las vulnerabilidades de los sistemas operativos Android, Apple iOS y de Windows, el más usado tanto en los ordenadores de la administración como en el entorno familiar.

La mayor parte de estos ataques forman parte de lo que se conoce como “Amenazas Persistentes Avanzadas” o APT en su siglas inglesas (por Advanced Persistent Threat). Estos procesos APT implican la participación de un equipo de hackers coordinados durante un periodo de tiempo que puede ser bastante largo, utilizando sofisticadas técnicas para introducir malware explotando vulnerabilidades en los sistemas. Estos ataques tienen como finalidad la extracción de datos de un objetivo específico de forma continua.

En los últimos tiempos se han desarrollado sigilosos programas que resulta muy difícil detectar e incluso erradicar cuando han penetrado en un sistema.

Según la empresa Check Point, entre junio y diciembre de 2013, 1 de cada 3 organizaciones descargó al menos un archivo infectado con malware desconocido. Nuevas herramientas de ofuscación conocidas como “crypters” permitieron a los cibercriminales evadir la detección del software anti-malware.

El CNI detectó este año 13.000 incidentes, un 80% más que en 2013. El 11,6% de estos ataques alcanzaron un nivel de riesgo entre "muy alto" y "crítico". Un centenar de estos ataques fueron dirigidos contra el propio centro.

Naturalmente, estas noticias se refieren a ataques frustrados. De los que tienen éxito, normalmente no se tiene noticia.

http://delicious.com/rpla/raa840b
CIBERGUERRA

¿PUEDE UNA PELICULA PROVOCAR UNA CIBERGUERRA?

La ciberguerra se ha convertido en un tema popular. Cuanto más popular es un tema, más difícil es realizar análisis técnicos o científicos fiables sobre el mismo. Cuando esta popularidad afecta a una cuestión de naturaleza secreta o discreta, como pueden ser los medios y acciones que los países realizan para apoyar su política nacional o en materias de defensa, es seguro que de todo lo que se sabe y se publica, una gran parte es mentira y la otra no es verdad.

Las supuestas noticias sobre estos temas son frecuentemente bulos, señuelos, cortinas de humo o la parte sesgada de la verdad que al comunicador le interesa que se sepa. Sin duda alguna una de las leyes básicas de la guerra que la ciberguerra cumple a rajatabla es que "la primera víctima es la verdad".

Hubo un tiempo en el que los “casus belli” se podían incluir en una lista con un número discreto de lineas. El derecho internacional aún no ha incluido en esta lista los hechos que puedan ser considerados como "casus belli" en realción a las acciones en el dominio del ciberespacio o que puedan motivar una ciberguerra. El "Ius in bello", o prácticas aceptables en caso de ciberguerra, tampoco han sido desarrolladas y aún menos aceptadas por ningún contendiente.

Como conclusión, en las crónicas de ciberguerras que leemos en la prensa, todo parecido con la realidad es mera coincidencia. He intentado hacer un resumen breve del caso de la película de Sony que ha motivado escaramuzas varias, declaraciones contradictorias, amenazas más o menos creíbles e incluso anuncios de negociaciones entre las dos Coreas para su reunificación, pero después de repasarlo no creo que tenga demasiado sentido ni que sea mínimamente relevante. A cambio le propongo a los lectores que usen el conocido buscador que ya no resume noticias de la prensa española, para encontrar coincidencias de las palabras "Sony", "Corea" y "ciberguerra" e intente ordenarlas cronológicamente. El resultado es un relato tan inexacto del asunto como cualquiera que pueda ofrecerse en estas páginas o en otras. ■

http://delicious.com/rpla/raa840c

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto