Centros de alerta temprana sobre seguridad informática en España

La seguridad en Internet resulta cada vez más problemática. Muy recientemente se ha producido un ataque, posiblemente ciberdelincuente, a una entidad que gestiona registros de dominios .es con modalidades y características nuevas.

Pero no solamente los ataques novedosos son preocupantes, sino también los tradicionales de tipo virus en su surtido variado: troyanos, botnets, rootkits, denegación de servicio, etc.

En la actualidad se consideran, en muchas legislaciones, como ciberdelincuentes no solo a los denominados "crackers" y piratas, sino también a los denominados "hackers". No son figuras iguales y hemos de tener en cuenta que cuando surgió Internet, los "hackers" no eran considerados ni ciberdelincuentes ni siquiera peligrosos, ya que eran y son expertos que normalmente se dedican a probar la seguridad en Internet avisando a los interesados de los peligros y debilidades detectados. La denigración de los "hackers" ha venido formulándose principalmente por las empresas cuyos productos resultan inseguros y los "hackers" lo ponen en evidencia publicándolo en Internet, con consecuencias negativas de tipo comercial y de imagen. Estas empresas, que muchas veces contratan a "hackers" para verificar la seguridad de sus propios productos, son las que consideran que les perjudica esta publicidad y en algunos países han conseguido que los "hackers" sean considerados ciberdelincuentes.

En la actualidad, dada la difusión de Internet, en una serie de países se han venido creando, por organizaciones privadas y públicas, pero no por las administraciones públicas, entes dedicados a detectar los diversos tipos de ataques de la ciberdelicuencia. Estos entes que se denominan genéricamente C.E.R.T (Computer Emergency Response Team) y también C.S.I.R.T (Computer Security Incident Response Team), son en realidad centros de alerta temprana que pueden facilitar medidas de protección frente a los mencionados ataques.

En España tenemos ya varios de estos centros, el primero fue creado por la UPC, el CERT-UPC, después se creó el CERT de Red Iris y hace pocas semanas se anuncio la creación del CERT-CNI (Centro Nacional de Inteligencia). También INTECO, el Instituto Nacional de Tecnologías de la Comunicación del Ministerio de Industria, Comercio y Turismo va a crear otro CERT, y parece ser que los gobiernos autonómicos también serían proclives a crear sus propios CERT, con lo cual en nuestro país llegaríamos fácilmente a superar la cifra de 20 CERTs.

La creación de estos centros de respuesta a los ataques en Internet es importante para la seguridad de los usuarios nacionales de Internet, tanto empresariales y de las administraciones publicas como usuarios particulares.

Pero a ATI le resulta preocupante que esta proliferación de CERTs se realice sin la debida colaboración y coordinación entre ellos. Los esfuerzos en detección de ataques y en toma de contramedidas de protección de los usuarios no pueden dilapidarse con duplicidades costosas (aunque solo sean las de carácter administrativo y de cargos directivos) e inútiles que lo único que hacen es reinventar la rueda. Los profesionales especialistas en esta materia son escasos, apreciándose la necesidad de establecer mecanismos de colaboración y cooperación formales entre los diversos CERTs españoles y europeos, con el fin de que su eficacia sea realmente sobresaliente, y de paso evitar que los usuarios resulten confundidos con un conjunto variado de alertas de diversas procedencias.

en resumen El arco iris

Llorenç Pagés Casas
Coordinación Editorial de ***Novática***