ABC | ESPAÑA

ESPAÑA

# Seis meses y 80 incidentes muy graves

## Al servicio del EstadoMedio centenar de expertos ayudan al Centro Criptológico Nacional, adscrito al CNI, a prevenir y combatir ataques a las administraciones y empresas que trabajan con información clasificada

Día 19/06/2011

La seguridad nacional ya no se juega en un campo de batalla, ni depende de la información sensible que espías más o menos intrépidos puedan obtener en los países en los que se despliegan. Internet ha cambiado el escenario para siempre; el espacio virtual no pertenece a nadie y sin embargo en él se ventilan intereses críticos para los Estados. La globalización alcanza aquí su máximo sentido. El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), está diseñado para conjurar esas amenazas, cuyos perfiles cambian casi a diario. Solo un dato: en lo que va de año, ha dado respuesta a unos 80 incidentes muy graves o críticos. En total, en ese periodo ha habido medio millar.

En el CCN lo tienen claro: «La tecnología plantea a diario nuevos retos de seguridad. Cada vez hay más redes informáticas empresariales, los móviles son capaces de conectarse a ellas... Son herramientas que mejoran la eficacia de las administraciones públicas y de las grandes compañías, pero a cambio los riesgos de ataques informáticos aumentan». El ejemplo es claro: hasta ahora hemos podido proteger un edificio de una agresión convencional, ¿pero podemos decir lo mismo de la información que ese inmueble alberga?

La magnitud del desafío se explica con algunas cifras. En 2008, el 14,9 de las vulnerabilidades detectadas en el ámbito de las administraciones fueron de nivel alto. Al año siguiente, alcanzaron el 21,2%, y en 2010 llegaron al 30,7. Cada año, se descubren unas 8.000. La amenaza, pues, crece. En el Centro Criptológico Nacional lo explican: «No hay que dramatizar. Los sistemas de detección han mejorado mucho».

«Cada vez hay más ciberataques —sostienen las mismas fuentes— porque tienen un bajo coste; las herramientas necesarias para realizarlos son de un manejo relativamente sencillo; resultan muy rentables y efectivas, ya que de la red se puede sacar mucha información susceptible de traducirse en beneficios económicos, y cuando se produce una agresión compleja es extremadamente difícil atribuir una autoría».

Las investigaciones y el trabajo de inteligencia indican que en España hay «hackers» de primer nivel, aunque rara vez atacan en nuestro país. De nuevo la ecuación riesgo-beneficio es decisiva: «Saben que aquí hay leyes investigadores capaces de descubrirlos. Lo habitual es que las agresiones tengan su

origen en terceros países, como Bielorrusia, Rusia, Ucrania, Brasil o China, por poner algún ejemplo. Allí es mucho más difícil que se les aplique una legislación que a veces ni siquiera existe».

La mayor parte de los ataques, hasta un 65, corresponde a la introducción de códigos dañinos en los sistemas informáticos, lo que se conoce como «troyanos». En sa categoría se incluyen aquellos que se utilizan para obtener información sensible de datos bancarios; virus diseñados para dañar equipos; programas espía que permiten acceder al corazón de las redes más delicadas de información, e incluso aquellos que buscan infectar ordenadores para convertirlos en «zombies»; es decir, para que sin que el usuario lo detecte la terminal quede a merced de las órdenes que le suministra un tercero.

En este contexto, la figura del «hacker», es decisiva. En el CC se destaca que los mejores se han profesionalizado y pueden jugar tanto en el bando de la ley —en ese caso es más preciso y evita connnotaciones peyorativas denominarlos expertos en seguridad informática—, como en el de los criminales. Más de medio centenar colaboran con el Centro aportando información, análisis, elaborando respuestas ante una crisis y alertando de vulnerabilidades.

Claro que también existe la otra cara de la moneda: no pocos «hacker» venden sus servicios a tramas criminales o incluso a servicios de inteligencia de Estados que quieren obtener información sensible de otros países. Es lo que se conoce como «ciberespionaje», que afecta no solo a las administraciones, sino también a empresas punteras.

Junto a este concepto se habla de la «ciberguerra», que no deja de ser un intento por parte de los países de aprovechar todas las posibilidades del «ciberespacio». «Pero el foco, de momento, se está poniendo en el aspecto defensivo», afirman las fuentes consultadas.

El tercer término peliagudo sería el de «ciberterrorismo». En el CCN prefieren hablar del «uso del ciberespacio por parte de terroristas» comunicaciones entre ellos, utilización de herramientas para obtener información de la red, el uso de Internet como medio de propaganda y también como herramienta de financiación. «Para que puedan perpetrar agresiones —sostienen en el Centro— hace falta una preparación técnica muy avanzada, que hasta ahora no se les ha detectado. De hecho, en este punto el nivel de amenaza actual está calificado de bajo o muy bajo». «Cuestión distinta —añaden— es que sean capaces de atacar sistemas de infraestructuras críticas que, no hay que olvidarlo, están en un 80 en manos del sector privado».

En España no hay cuantificación de las pérdidas causadas por los ataques, al contrario de lo que sucede en el Reino Unido. Allí, el CPNI calcula en 27.000 millones de libras los daños causados por la «ciberdelincuencia». «Aquí, a nuestra escala económica, las cifras pueden ser igual de mareantes», apuntan las fuentes.

El desafío es descomunal y la pregunta, por tanto, obvia. ¿Está España preparada para darle respuesta? El panorama es tranquilizador. El Centro Criptológico Nacional nació en 2002 y desde 2007 cuenta con un amplio reconocimiento internacional. Participa en los foros más avanzados y desde 2009 desarrolla uno de sus principales retos, la creación de un Sistema de Alerta Temprana, clave para dar una respuesta eficaz ante cualquier ataque. Entre sus misiones está la de avisar de vulnerabilidades, detectar ataques, prestar ayuda a quien se lo pide en dar respuesta a esas agresiones, ya sean administraciones o empresas que manejan información clasificada, y hacer un trabajo de inteligencia para anticiparse a los nuevos riesgos.

Para ello cuenta con profesionales muy solventes —su media de edad es 10 años menor que la del resto de agentes del CNI, incluidos científicos que publican trabajos en revistas internacionales; recibe ayuda desde el ámbito universitario y sectores empresariales; suscribe convenios con administraciones y colabora con servicios similares de países de nuestro entorno. Y en lo que se refiere al desarrollo normativo, se ha dado un paso más: la Estrategia Nacional de Seguridad prevé por primera vez un Estrategia Nacional de Ciberseguridad.

Por CRUZ MORCILLO y PABLO MUÑOZ