La ciberseguridad en los sectores estratégicos nacionales

CCN-CERT

Centro de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional, perteneciente al CNI

El uso de Internet y de las nuevas tecnologías está implantado completamente en la vida cotidiana de nuestro país. Los ciudadanos españoles, sus administraciones públicas y sus empresas utilizan este entorno global denominado 'ciberespacio' de forma habitual, lo que plantea numerosas posibilidades, pero también un gran número de riesgos y amenazas. Esta dependencia de las tecnologías de la información y la comunicación (TIC) en todos los ámbitos, incluidos los sectores estratégicos esenciales para la seguridad nacional y para el conjunto de la economía del país, hace imprescindible una apuesta decidida por la ciberseguridad, como la mantenida por el Centro Criptológico Nacional, y su Capacidad de Respuesta a Incidentes, CCN-CERT. La estabilidad y prosperidad de España dependerá en buena medida de la seguridad y confiabilidad del ciberespacio.

> CCN-CERT tiene responsabilidad en ciberataques sobre sistemas de la Administración y de empresas de sectores estratégicos

Durante el pasado año 2012, el CCN-CERT gestionó más de 4.000 incidentes de ciberseguridad (casi el doble que en 2011), registrados por los distintos sistemas de detección de los que dispone. De ellos, 230 fueron catalogados con una criticidad de 'muy alto' o 'críticos' y no solo en los sistemas de las administraciones públicas (algunas empresas estratégicas también fueron blanco de estos ciberataques). La introducción de código dañino en los sistemas (con niveles muy bajos de detección por parte de las compañías antivirus), las intrusiones mediante ataques a páginas web con el fin de robar información, así como el contacto con IP maliciosas, fueron algunos de los incidentes más recurrentes sufridos por nuestras administraciones. Unas administraciones que, no lo olvidemos, dependen del uso de Internet y de las nuevas tecnologías tanto para su funcionamiento interno como para los servicios que prestan a la población (el 95 por ciento de los servicios públicos ya están operativos a través de Internet). Así, la información que almacenan en sus sistemas y estos mismos servicios constituyen un activo básico para el correcto funcionamiento de nuestra sociedad.

Estas amenazas, extensibles al ámbito empresarial y a los sectores estratégicos del país (entendiendo como tal aquellos que son esenciales para la seguridad nacional o para el conjunto de la economía), se incrementan día a día y las perspectivas de su disminución son muy escasas. Antes al contrario, la rentabilidad que se obtiene (económica, política o de otro tipo), la relativa facilidad y bajo coste de las herramientas utilizadas, así como la dificultad de saber quién está detrás de un ataque y desde dónde se está efectuando son factores que en nada ayudan a la hora de contener las ciberamenazas.

Sectores estratégicos

Hace poco más de diez años, se publicaba en el Boletín Oficial del Estado la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI). En ella, en su artículo 4, entre otros puntos, se señalaban como funciones del Centro: "Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España". Además, debía "coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las

misiones del Centro. De igual modo, incluía como una de las funciones del CNI el velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

Posteriormente, se publicó el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN). En él se manifiesta que la elaboración, conservación y utilización de determinada información por parte de la Administración es necesaria para garantizar su funcionamiento eficaz al servicio de los intereses nacionales. Señala, además, la necesidad de contar con un organismo que, partiendo del conocimiento de la tecnología y la amenaza, proporcionara una garantía razonable sobre la seguridad de productos y sistemas. Este organismo es el CCN que, en 2006, constituyó su Capacidad de Respuesta a Incidentes, CCN-CERT, como CERT gubernamental/nacional.

El CCN-CERT, cuyas funciones quedan recogidas en las citadas Ley 11/2002 y RD 421/2004, así como en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos.

Su misión, de hecho, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las administraciones públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas.

Cómo estar infectado

El trabajo del CCN-CERT desde su creación ha ido encaminado a una defensa preventiva frente a los ciberataques. Todo su esfuerzo se ha desarrollado (y lo seguirá haciendo en el futuro) a incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas, haciendo énfasis en las administraciones públicas, las infraestructuras críticas, las capacidades militares y de Defensa, y otros sistemas de interés nacional.

En este sentido, es fundamental un cambio en la mentalidad de la detección de los ataques, tanto entre las empresas como entre la Administración. Trabajar como si se estuviese infectado, crear y potenciar equipos de vigilancia, políticas de seguridad más estrictas e intercambio de información entre el sector público y privado son algunos de los aspectos que deberían tenerse en cuenta a la hora de hacer frente a las ciberamenazas. La estabilidad y prosperidad de España dependerá en buena medida de ello. ■