España y su Administración como blanco de las ciberamenazas globales

Nuestro país, y más concretamente las Administraciones Públicas y sus máximos órganos de Gobierno, está siendo uno de los más castigados por los agentes de las ciberamenazas, especialmente en materia de ciberespionaje y ciberdelincuencia organizada. A ello se une el hacktivismo que, aunque con intenciones más modestas, ponen en peligro en numerosas ocasiones la prestación de servicios y el normal funcionamiento de la Administración. Ante esta situación el CERT Gubernamental Nacional ofrece una primera línea de contención frente a los ciberataques ofreciendo todos sus servicios a las distintas administraciones y actuando como nodo de coordinación e intercambio de información a nivel público estatal.

JAVIER CANDAU
Jefe de Área de Ciberseguridad del Centro Criptológico Nacional

Durante el año pasado, el CCN-CERT, del Centro Criptológico Nacional, gestionó un total de 12.916 incidentes en las Administraciones Públicas y en empresas y organizaciones de interés estratégico para el país; es decir, aquellas entidades que por su actividad o conocimiento son esenciales para la seguridad nacional y para el conjunto de la economía española. Esta cifra representa un incremento del 78% con respecto al año 2013 y de más del 150% en relación al año 2012. De estos incidentes de 2014, el 11% fueron catalogados por el equipo de expertos del CERT Gubernamental Nacional con un nivel de riesgo entre muy alto y crítico; es decir, se tiene constancia de que el ataque afectó a los sistemas de la organización y a su información sensible. Estas cifras nos indican que los sistemas y comunicaciones más críticas de nuestro país, entre ellas las de la Administración, reciben una media de cuatro ataques diarios.

La introducción de código dañino en los sistemas (con niveles muy bajos de detección por parte de las empresas antivirus), las intrusiones mediante ataques a páginas web con el fin de robar información, así como el contacto con IPs maliciosas, fueron algunos los incidentes más recurrentes sufridos por nuestra Administración. 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 (recordemos que los trámites que los ciudadanos y las empresas realizaron con la Administración General del Estado en 2013 superaron los 480 millones, de los cuales, el 76,5% se llevaron a cabo por vía electrónica, según los datos del Sistema de Información Administrativa -SIA-). Así, la información que almacenan

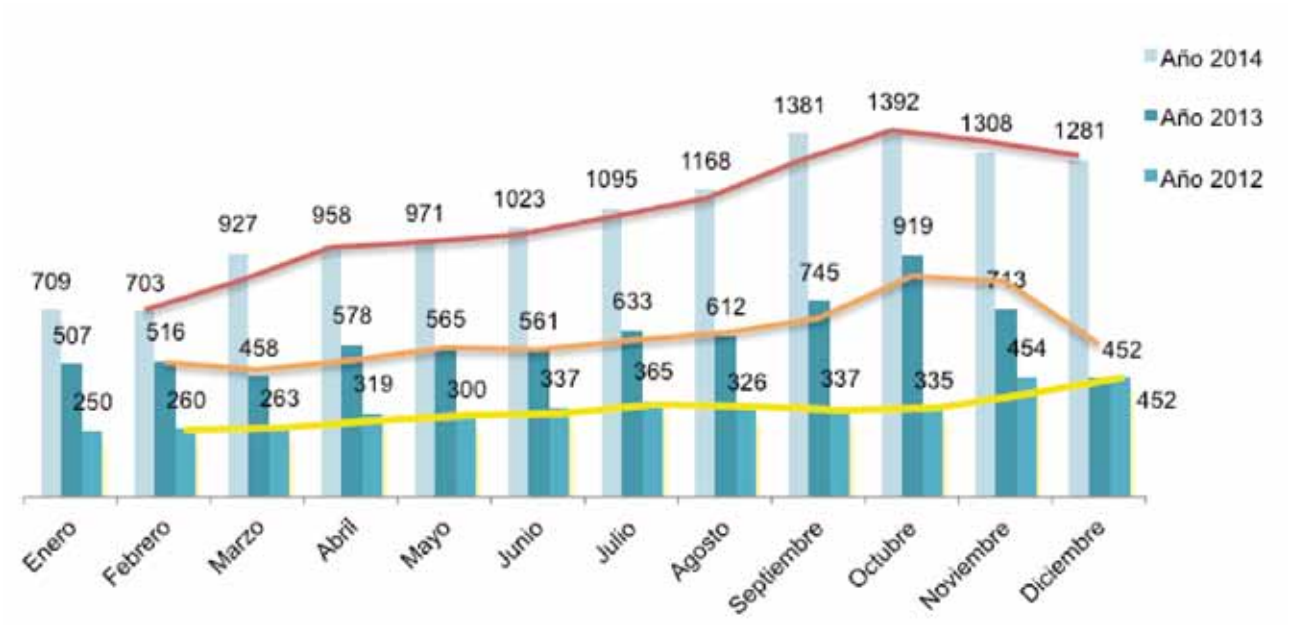

FIGURA 1. Evolución de los incidentes gestionados por el CCN-CERT

en sus sistemas y estos mismos servicios constituyen un activo básico para el correcto funcionamiento de nuestra sociedad.

Principales objetivos

En función del origen de la amenaza (véase Figura 2), los objetivos buscados en los ciberataques a las distintas administraciones públicas son diferentes. El principal y más peligroso objetivo detectado por el CCN-CERT es, sin duda, el robo de información de alto valor que permite al atacante una mejora de su situación geopolítica o económica (con el fin de alcanzar rápidamente una capacidad científico tecnológica de la que no se dispone, como forma de presión, etc.) o, cada vez más habitual, como forma de negocio para grupos perfectamente organizados que subastan la información conseguida al mejor postor.

En este sentido, todos los ministerios (especialmente aquellos que fijan la acción de gobierno como Presidencia, Asuntos Exteriores, Defensa, Interior o Economía), las Fuerzas Armadas y la industria de la Defensa están en permanente riesgo en relación con el robo de información que, en este sector, tiene un valor estratégico y económico de singular magnitud.

Además, el CERT Gubernamental Nacional viene observando cómo las amenazas que, originariamente, se dirigían solamente a instituciones públicas, se centran en individuos, incluyendo altos cargos, personajes notorios o responsables políticos. Y si no se consigue acceder directamente al objetivo, se ataca a los elementos más débiles de la cadena, como podrían ser los proveedores, clientes o contratistas o cualquier sujeto que pueda estar en contacto con el blanco.

CCN-CERT, primera línea de defensa

El CCN-CERT, como CERT Gubernamental Nacional, y tal y como recogen distintas leyes, tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y

Los sistemas y comunicaciones más críticos de este país, entre ellos los de la Administración, reciben una media de cuatro ataques cada día en los que hay constancia de que se ha accedido a información sensible

Origen de la amenaza	Objetivo en la Administración
Estados	Ciberespionaje
	Cibercapacidades ofensivas
Grupos terroristas	Interrupción de Sistemas / Toma de control
Profesionales del ciberdelito	Sustracción, publicación o venta de información
	Manipulación de información
	Interrupción de sistemas
	Toma de control de sistemas
Cibervándalos y script kiddies	Sustracción de información
	Interrupción de sistemas
Hacktivistas	Sustracción y publicación de la información sustraída
	Desfiguraciones
	Interrupción de sistemas
	Toma de control de sistemas
Actores internos	Sustracción, publicación o venta de información
	Interrupción de sistemas
Ciberinvestigadores	Recibir y publicar información

FIGURA 2. Objetivos de los ataques al sector público

organizaciones de interés estratégico para el país.

Por ello, su labor desde el año 2006 en el que se constituyó en el seno del Centro Criptológico Nacional, ha sido precisamente intentar reducir los riesgos y las amenazas provenientes del ciberespacio, potenciando las acciones, no sólo defensivas, sino primordialmente preventivas, correctivas y de contención. A través de su equipo de expertos destinados a investigar sobre técnicas empleadas, funcionamiento de los ataques, soluciones y procedimientos más adecuados para hacerlos frente, el CCN-CERT ofrece todos sus servicios a las Administraciones Públicas **(1)** .

El Servicio de Alerta Temprana (SAT), tanto en Internet como en la red SARA, en la que están incluidos más de 70 organismos públicos de las distintas administraciones (General, Autonómica y Local); así como el desarrollo de diferentes herramientas como CARMEN (detección de APTs), LUCIA (Listado de Coordinación de Incidentes y Amenazas), INES (Informe Nacional del Estado de Seguridad), CLARA (nueva herramienta para cumplir con el ENS) o MARTA (Motor de Análisis Remoto de Troyanos Avanzados) son algunos de estos servicios puestos a disposición de toda la Administración.

Destaca también su estrecha colaboración con la Secretaria de Estado de Administraciones Públicas, puesta de manifiesto en el desarrollo, implantación y seguimiento del Esquema Nacional de Seguridad (ENS), en la formación de su personal a través de los Cursos STIC (presenciales y online) en coordinación con el Instituto Nacional de Administración Pública (INAP) y en la difusión de normas, instrucciones, guías y recomendaciones (cuenta con más de 200 Guías CCN-STIC en este sentido) sobre múltiples aspectos de seguridad.

Todo ello, conscientes de que dada la influencia de los sistemas de información en la economía y en los servicios públicos, la estabilidad y prosperidad de España dependerá en buena medida de la seguridad y confiabilidad del ciberespacio. Por ello, las AAPP, y con ellas el CCN-CERT, deben involucrarse activamente en un proceso de mejora continua respecto de la protección de sus sistemas TIC, actuando como estandarte y ejemplo de la correcta gestión de la ciberseguridad ante toda la sociedad.*

NOTAS

(1) Todos sus servicios así como la forma de contactar con el CCN-CERT están disponibles en su portal web: *https://www.ccn-cert.cni.es/*