

CIBERSEGURIDAD

### Así se protege España del ciberespionaje

► España, en el punto de mira de los 'hackers'



Las instalaciones del Centro Nacional de Inteligencia, donde se encuentra el CCN, en el distrito madrileño de Moncloa-Aravaca.

JAVIER G. FERNÁNDEZ MADRID  @JGF92

Actualizado: 10/01/2017 00:30 horas

El Centro Criptológico Nacional, dependiente del CNI, es el encargado de velar por la seguridad de las comunicaciones de la Administración, así como de analizar y dar respuesta a los incidentes cibernéticos.

La sombra de una intervención rusa en las pasadas elecciones del 20 de noviembre en Estados Unidos, favoreciendo supuestamente al candidato republicano Donald Trump, ha despertado los peores fantasmas de la Guerra Fría y dejado una inquietante pregunta en el aire: ¿Puede un pirata informático a sueldo de un gobierno extranjero vulnerar las defensas cibernéticas de la primera potencia mundial y adulterar algo tan sensible como unos comicios? Mientras en EEUU tratan de dar respuesta a esta cuestión, en España el Centro Criptológico Nacional (CCN) trabaja para evitar que los *hackers* influyan en el correcto funcionamiento del Estado.

Dependiente del Centro Nacional de Inteligencia (CNI), este organismo es el encargado de garantizar la seguridad de las comunicaciones y proveer de dispositivos cifrados a los diferentes organismos de la Administración, formar al personal en materia de ciberseguridad y detectar y analizar los incidentes cibernéticos. A cargo de este equipo de expertos -el CCN no detalla cuántas personas lo integran- se encuentra Javier Candau, jefe del Departamento de Ciberseguridad del CCN.

Candau: "Tenemos mejores herramientas de detección y podemos disputarle el partido a los atacantes"

"Nuestro trabajo consiste en proteger la información de la Administración y garantizar al Gobierno unas comunicaciones lo más seguras posibles", explica a EXPANSIÓN desde la sede del organismo, ubicado en el distrito madrileño de Moncloa-Aravaca, a pocos kilómetros de la Casa de Campo y camuflado entre viviendas unifamiliares y parques infantiles. Un edificio de tonos pastel y aspecto funcional en el que, antes de entrar, y después de haber pasado varios controles de seguridad, te exigen que guardes en una taquilla cualquier dispositivo electrónico que lleves encima. "Es para evitar que interfiera con nuestras señales", aseguran. Además del CCN, este complejo gubernamental alberga la sede del CNI, el hogar de los espías españoles.

## SEGURIDAD

Escándalos recientes como el protagonizado por Hillary Clinton por el uso de un servidor privado durante su etapa como secretaria de Estado, han puesto en el foco la integridad de las comunicaciones y las prácticas, más o menos responsables, de los políticos a la hora de gestionar información sensible para el país. Cuestionado acerca de cómo evitar que sucesos así se repitan en España, Candau asegura **haber puesto en manos de ministros y secretarios de Estado "los medios y la formación necesaria para evitar estos incidentes"**, aunque, añade, **"si se relajan los procedimientos podemos encontrarnos con un problema"**.

Desde su creación hace ya una década, el Centro Criptológico Nacional ha gestionado unos 66.000 ciberincidentes, ha elaborado más de 80.000 reglas de detección de intrusiones y realizado 135 auditorías de seguridad. Un periodo, explica el responsable de ciberseguridad del CCN, en el que las amenazas han evolucionado muchísimo. Casi tanto como las capacidades de los defensores para detectar las grietas por las que se cuelan los hackers. "El *malware* ha dejado de ser tan rentable, ahora lo que más abundan son los ataques dirigidos. Hoy, tenemos mejores herramientas de detección que antes y podemos disputarle el partido a los atacantes".

"Desde su creación en 2006, el CCN ha gestionado más de 66.000 incidentes de seguridad"

Según el documento Ciberamenazas 2015 / Tendencias 2016, elaborado por el CCN, el ciberespionaje es la mayor amenaza cibernética hoy en día. **"El ciberespionaje y los ataques de denegación de servicios es lo que más nos preocupa"**, confirma Candau, que señala a las "empresas financieras, de salud, tecnológicas, de Defensa y la Administración Pública" como las más amenazadas.

## ATAQUES EXTRANJEROS

Según las conclusiones del informe, [el 90% de los ciberataques clasificados como críticos, los de mayor gravedad, sufridos por organismos públicos o empresas españolas de interés estratégico, proceden de Gobiernos extranjeros](#). Una estadística que refleja el complejo mapa geopolítico actual en el que, como destaca el jefe de Ciberseguridad del organismo, "cualquier conflicto en el mundo físico se refleja en el ciberespacio". Pese a que resulta muy complicado obtener pruebas para demostrar quién está detrás de estos ataques, desde el CCN apuntan a China, Rusia, Europa del Este y Estados Unidos como el origen geográfico de buena parte de los incidentes.

En este sentido, llama la atención la creciente influencia que están ganando en la Red el denominado ciberyihadismo. Por el momento, la actividad de estos grupos se limita a los ataques DDoS (denegación de servicios), la diseminación de propaganda y el reclutamiento y radicalización de nuevos combatientes. Tareas, en su mayoría, que no requieren de grandes conocimientos técnicos pero que, como alerta Candau, irán a más. **"Motivaciones no les faltan y en los próximos años se van a incrementar sus capacidades. Aunque ahora mismo estén jugando en segunda división, eso no quiere decir que no puedan realizar con éxito algún ataque más sofisticado en caso de recibir apoyo de un gobierno extranjero"**.

Candau: "En los próximos años se van a incrementar las capacidades de los ciberyihadistas"

De cara al 2017, el experto del CCN vaticina un incremento en el número de incidentes entre los que destacan "más ataques de denegación de servicios a través del Internet de las Cosas y muchos casos de ransomware, que van a tener a las instituciones como objetivo".

## "Necesitamos invertir más en ciberseguridad"

Después de casi una década de crisis económica, y los consiguientes recortes que ha aplicado la Administración, la ciberseguridad española necesita de más inversiones para seguir por delante de los cibercriminales. Así lo reclama Javier Candau, jefe de Ciberseguridad del Centro Criptológico Nacional (CCN): **"Una legislación tan avanzada como la española la tienen muy pocos países en Europa, pero aun así necesitamos invertir más en sistemas de ciberseguridad"**. Y añade: "Ahora mismo podemos comparar sin miedo nuestras capacidades con la de otros países de nuestro tamaño de la Unión Europea". Este ejercicio, el presupuesto del Centro Nacional de Inteligencia (CNI), del que depende el CCN, se ha incrementado un 7,87%, recuperando así los niveles de 2010, después de años de reducciones y estancamiento. Unas restricciones presupuestarias que impiden al organismo captar a los talentos más demandados que, normalmente, se inclinan por los jugosos sueldos que les ofrece el sector privado. Por ello, explica Candau, "preferimos ir a las universidades en busca del talento y luego fidelizarles".

Fuente: <http://www.expansion.com/economia-digital/innovacion/2017/01/10/586a8176e2704e10488b4601.html>