redseguridad.com

“El ciberespionaje persigue información de altísimo valor y debe considerarse una amenaza crítica”

ENTREVISTA

JAVIER CANDAU, JEFE DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN)

“El ciberespionaje persigue información de altísimo valor y debe considerarse una amenaza crítica”

15/06/2015

Desde su puesta en marcha, el CERT del Centro Criptológico Nacional (CCN) ha contribuido a mitigar los ciberataques dirigidos a administraciones, organismos y empresas estratégicas para el normal desarrollo del país. Según Javier Candau, responsable de Ciberseguridad del CCN, dichas acciones pretenden, en la mayoría de los casos, captar información que “puede llegar a ser esencial para la seguridad nacional o el conjunto de la economía”.

El CERT del Centro Criptológico Nacional (CCN) inició su andadura en 2006. De las actuaciones que ha llevado a cabo, ¿cuáles destacaría, por su relevancia, para contribuir a la mejora de la ciberseguridad en España?

Sin lugar a dudas, su principal contribución ha sido la gestión de los ciberincidentes que han afectado a sistemas clasificados de las administraciones públicas y de empresas y organizaciones de interés estratégico para el país. Su papel como centro de alerta y respuesta nacional, que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y afronta de forma activa las ciberamenazas, puede calificarse de clave en la defensa de nuestros sistemas. Adecuándonos a los nuevos desafíos, hemos potenciando las acciones no sólo defensivas, sino primordialmente preventivas, correctivas y de contención para hacer frente, por ejemplo, a los 33.000 ciberincidentes gestionados en los últimos cinco años.Además, hemos contribuido al desarrollo de la Estrategia de Ciberseguridad Nacional y a la implantación del Esquema Nacional de Seguridad, así como a la formación de personal experto a través de guías y cursos, la concienciación y sensibilización en la materia mediante jornadas, conferencias y charlas, la aplicación de políticas y procedimientos y el empleo de tecnologías de seguridad adecuadas.

¿Con qué medios cuenta el CCN-CERT para dar respuesta a los ciberataques destinados a comprometer la seguridad nacional?

Dispone de un equipo multidisciplinar de expertos altamente cualificados en seguridad de la información y las telecomunicaciones. Gracias a él, hemos sido capaces de configurar un Centro de Operaciones eficaz dedicado a la implantación y gobierno de medidas preventivas, reactivas y de gestión. Contamos, además, con el fuerte respaldo del CCN, que es, no lo olvidemos, el organismo de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información. Y también tenemos el apoyo del Centro Nacional de Inteligencia (CNI).En 2014, tras EEUU y Reino Unido, nuestro país fue el tercero que más ciberincidentes registró.

¿Por qué somos tan apetecibles para los ciberterroristas?

Como cualquier estado occidental, donde el volumen de las aplicaciones TIC es muy elevado y los dispositivos de todo tipo (ordenadores, smartphones, tablets, etc.) son muy utilizados, el riesgo de ciberataques se incrementa. En definitiva, nuestra dependencia cibernética aumenta los riesgos y las amenazas.En cuanto a los ataques, son múltiples: ciberespionaje (originado en los propios estados o en empresas que buscan una ventaja competitiva), ciberdelito (procedente de delincuencia organizada cuyo fin es fundamentalmente económico), hacktivismo (como medio para acercarse a sus objetivos ideológicos), ciberterrorismo (persigue influir en la toma de decisiones políticas), cibervandalismo (búsqueda de desafíos), actuaciones internas (ansían venganza o beneficios económicos o ideológicos), ciberinvestigación (para desvelar debilidades), etc.

En el caso del ciberespionaje, ¿supone una amenaza real para España y su tejido empresarial?

Sí, una de las principales. En este tipo de ataques se busca información de altísimo valor (propiedad intelectual, datos referentes a la seguridad nacional, secretos comerciales, códigos fuente, información sobre I+D, mercados y clientes, sistemas financieros, etc.) para el atacante o un tercero, que ofrecería un alto precio por ella. Esa información puede llegar a ser esencial para la seguridad nacional o el conjunto de la economía del país. Por lo tanto, el ciberespionaje debe considerarse una amenaza crítica.

¿Cuántos ciberincidentes tuvo que gestionar el CCN-CERT el año pasado? ¿Cuáles son sus principales objetivos?

Durante 2014, se gestionaron unos 13.000 ciberincidentes, un 80 por ciento más que el año anterior. De ellos, el 11,6 por ciento fue catalogado con un nivel de peligrosidad de entre muy alto y crítico; es decir, se tuvo constancia de que el ataque afectó a los sistemas de la organización y a su información más sensible.Esta última es el principal objetivo. Pero las amenazas dirigidas a empresas e instituciones públicas también repercuten en altos directivos, personajes notorios o responsables políticos. Se observa, además, una tendencia a atacar a los elementos más débiles de la cadena de intercambio de datos, como podrían ser los proveedores o contratistas. Por este motivo, las organizaciones públicas y privadas que manejan información con alto valor estratégico, económico o político deben incrementar sus medidas de seguridad.Desde el CCN-CERT se ha detectado un aumento de los ciberataques contra sectores estratégicos como el de defensa, el energético, el aeroespacial, el farmacéutico o el químico, sin olvidar a la propia Administración.

No obstante, deseo hacer una precisión en relación al empleo de los términos estratégico y crítico. Para el CNI, estos conceptos están definidos como “aquellos cuya pérdida de control, deterioro o interrupción de funcionamiento pueda suponer una amenaza para la seguridad nacional, una merma de la soberanía nacional o un daño grave para la economía española”, algo ligeramente diferente a la aproximación que se hace desde el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC). Los esfuerzos de este organismo están dirigidos a evitar las caídas de servicio y los nuestros, principalmente, la sustracción del patrimonio tecnológico.

¿Qué grado de cooperación existe entre el CCN y el CNPIC?

El CCN cree firmemente en la necesidad de cooperar y de coordinar las actividades de todos los agentes involucrados en la ciberseguridad: gobiernos, empresas y ciudadanos. En este sentido, la Estrategia de Ciberseguridad Nacional, en su Línea de Acción 1, fijaba la cooperación de los organismos con responsabilidades en

ciberseguridad, en especial entre el CCN-CERT, el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas y el CERT de Seguridad e Industria, en el que está integrado el CNPIC. Mantenemos una estrecha relación con todos los organismos citados y participamos en numerosos grupos de trabajo con los ministerios de Defensa, del Interior, de Industria, Turismo y Comercio y, por supuesto, con el de la Presidencia, del que dependemos.

¿Qué papel juegan herramientas como CARMEN 3.0, desarrollada por S2 Grupo en colaboración con el CCN, para reforzar la ciberseguridad de nuestro país? Y, ¿qué importancia le concede el CCN a la colaboración con el ámbito privado?

La cooperación entre el ámbito privado y el público es fundamental. Creo que esta colaboración siempre es mejorable y se puede decir que en el sector público existe de una forma bastante acertada. Por el contrario, es en el privado donde debería mejorarse e incrementar el intercambio de información.En cuanto a CARMEN, y otras muchas herramientas con las que cuenta el CCN-CERT, su desarrollo ha partido del propio CERT gubernamental que, en ocasiones, se apoya en distintos proveedores para reforzar su trabajo. Siempre hemos apostado por el apoyo y la promoción de iniciativas que aporten valor añadido a la ciberseguridad nacional.

Desde la puesta en marcha del Esquema Nacional de Seguridad, ¿se han ido logrando los objetivos marcados?

No del todo. Precisamente, y con el fin de elaborar el perfil general del estado de la seguridad de las administraciones públicas, tal y como recoge el artículo 35 del Real Decreto del Esquema de Seguridad Nacional, pusimos en marcha un proyecto que permitiese a los distintos organismos conocer de un modo rápido e intuitivo el estado de la seguridad de sus sistemas y, por lo tanto, adecuarse al Esquema. Se trata de la plataforma INES, que viene a complementar a la Guía CCN-STIC 824 Informe del Estado de Seguridad.

Está disponible en el portal del CCN-CERT desde septiembre de 2014 y, hasta la fecha, 145 organismos han notificado sus datos, tanto de la Administración General del Estado como de comunidades autónomas, ayuntamientos y universidades. No obstante, INES todavía es una herramienta para autoevaluación de los organismos y se tiene que ir migrando a una plataforma de recogida de datos de auditoría que nos indique el estado real de seguridad de los mismos.

En nuestro anterior número entrevistamos a Joaquín Castellón, director operativo del Departamento de Seguridad Nacional. ¿Coincide con él en que las ciberamenazas representan uno de los grandes desafíos para nuestra seguridad?

Sí. Las ciberamenazas son uno de los principales retos a los que se tienen que enfrentar los gobiernos de todo el mundo, incluido el nuestro, y así se nos marca en las prioridades establecidas en el CNI. Para asegurar el mantenimiento de nuestro desarrollo económico y social, precisamos disponer de un ciberespacio seguro, capaz de conducir nuestra actividad diaria de manera eficaz y a salvo de ataques o incidentes. A esta ingente tarea, que precisa de la implicación de todos (administraciones públicas, empresas y ciudadanos), el CNI seguirá orientando sus esfuerzos, energías y recursos.

Palabras clave:

Javier Candau, **CCN-CERT**, **información**, **ciberespionaje**, **amenazas**