El Gobierno creará en 2018 un SOC para la Administración del Estado

El Gobierno creará en 2018 un centro de operaciones de seguridad destinado a mejorar las capacidades de vigilancia y protección de la Administración General del Estado. La vicepresidenta del Gobierno lo anunció en las Jornadas STIC CCN-CERT, que congregaron a más de 1.700 profesionales de la seguridad TIC. Las revistas RED SEGURIDAD y SEGURITECNIA participaron en el evento como medios colaboradores.

Tx: E. González y D. Marchal
Ft: Redacción

ESPAÑA CONTARÁ A PARTIR DE 2018 con el Centro de Operaciones de Seguridad de la Administración General del Estado, cuyo objetivo será "reforzar las capacidades de vigilancia" y "proporcionar una respuesta aún más eficaz ante las ciberamenazas". La vicepresidenta del Gobierno, Soraya Sáenz de Santamaría, anunció la creación de este órgano durante la inauguración de las Jornadas STIC CCN-CERT, donde también avanzó –ya en declaraciones posteriores a la prensa– que tendrá un coste inicial de 16 millones de euros.

El organismo, que dependerá del Ministerio de Hacienda a través de la Secretaría General de Administración Digital (SGAD), entrará previsiblemente en funcionamiento a partir del próximo junio. El subdirector general del Centro Criptológico Nacional (CCN), Luis Jiménez, aseguró por su parte que el nuevo centro servirá para facilitar una "respuesta rápida y centralizada" frente a los ataques que se produzcan sobre las tecnologías de la información y las comunicaciones de la Administración del Estado.

La vicepresidenta del Gobierno daba la noticia en unas jornadas donde se concentraron, los días 13 y 14 de diciembre, en Madrid, más de 1.700 profesionales de la seguridad TIC. Durante su intervención, también apuntó algunos de los principales retos tecnológicos a los que se enfrenta España, como son el Big Data, el Internet de las Cosas, la protección de los menores en la Red, la seguridad de los datos o garantizar derechos de los ciudadanos como la intimidad, el honor o la privacidad,

Soraya Sáenz de Santamaría en la inauguración./ Foto: CCN-CERT.

haciéndolos compatibles con la libertad de expresión.

También se refirió al desafío que representa la desinformación en Internet al afirmar: "La tecnología ha modificado profundamente el acceso a la información y quién la produce. Internet es el mayor medio de comunicación actual y las noticias falsas pueden poner en jaque la estabilidad de los gobiernos y de la economía de los países". Para hacer frente a esta problemática, añadió, es necesaria "la actuación y el compromiso firme" de los medios de comunicación y las grandes compañías mundiales.

Durante su discurso, la vicepresidenta sostuvo además que "los riesgos y amenazas del ciberespacio son globales y solo pueden defenderse con una respuesta conjunta y coordinada". No en vano, mencionó que en los últimos años se ha producido un incremento de los ataques procedentes desde el exterior contra intereses nacionales, ante lo que "es necesaria la mejora de capacidades de inteligencia y comunicación para garantizar una respuesta más eficaz".

El nuevo SOC

Las Jornadas STIC CCN-CERT, organizadas por el CCN –organismo adscrito del Centro Nacional de Inteligencia–, contaron durante los dos días de duración con la intervención de cerca de 60 especialistas en diversos temas, cuyas ponencias se dividieron en sesiones plenarias y paralelas. Miguel Ángel Amutio, subdirector adjunto de la Subdirección General de Coordinación de Unidades TIC de la SGAD, y Pablo López, segundo jefe del Departamento de Ciberseguridad del CCN, ampliaron en una de ellas información sobre el nuevo centro de control de seguridad (SOC, por sus siglas en inglés). "El centro permitirá la protección de perímetro de seguridad de la Administración central y de sus organismos frente a amenazas externas y perseguirá una mayor capacidad de vigilancia y respuesta ante incidentes; todo ello con una visión de economía de escala, capacidad técnica y reducción de costes", expuso López.

Según explicó a continuación Amutio, la SGAD será responsable de coordinar la respuesta a las ciberamenazas y a los diferentes actores que intervengan en ella, así como del seguimiento del servicio. Por su parte, el CCN-CERT se hará cargo de la implantación de las infraestructuras, procedimientos, inteligencia, investigación de amenazas y análisis de vulnerabilidades, entre otras funciones. Es decir, este último prestará el servicio bajo la supervisión de la SGAD.

De este modo, el centro ofrecerá servicios "de alerta temprana, detección, respuesta coordinada, soporte

Más de 1.700 profesionales asistieron a las jornadas organizadas por el CCN-CERT, un 21% más que en la edición anterior.

a la investigación, análisis de vulnerabilidades, etc.", enumeró Amutio. Asimismo, el SOC dispondrá de tres niveles –operación, vigilancia e inteligencia– y ejercerá de "nexo de unión" entre el CERT competente y el organismo que esté afectado. Para ello incorporará en un plazo de tres años a entre 50 y 60 profesionales.

Aunque comenzará a operar este año, el desarrollo completo del proyecto irá más allá. A lo largo de 2018 se procederá a la instalación y el equipamiento del SOC, mientras que en 2019 se extenderá el servicio a todos los organismos de la Administración Central.

Actividad del CCN-CERT

La operación del SOC de la Administración se sumará por tanto a los servicios del CNN-CERT, cuya actividad en 2017 resultó intensa. Como explicó en sesión plenaria Javier Candau, jefe del Departamento de Ciberseguridad del CCN, el organismo dependiente del Centro Nacional de Inteligencia publicó una veintena de guías –entre las que destacó la 652: *Seguridad en cortafuegos Palo Alto*–, lanzó nuevas herramientas –como Gloria, para el análisis de amenazas, y Atenea, una aplicación de retos para encontrar talento– y aumentó "notablemente" el número de auditorías a empresas.

La alerta temprana y recepción de incidencias es otro de los apartados en los que se detuvo Candau. Sobre la notificación de incidentes, el responsable del CCN sostuvo que es necesario "eliminar burocracia y reportar solo por una vía", para lo que el centro se apoyará en la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas), desarrollada por el propio CCN-CERT para la gestión de ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad.

El jefe del Departamento de Ciberseguridad del CCN defendió además la necesidad aumentar la inversión para el refuerzo de la vigilancia y la respuesta a las ciberamenazas, así como fomentar la formación y el intercambio de información.

Cerca de 26.500 ataques

De lo contrario el futuro se presenta complicado porque la cantidad de ataques contra la Administración y las empresas estratégicas no para de aumentar. El CCN-CERT ha registrado este año cerca de 26.500 incidentes sobre dichos objetivos; es decir, un 26,5 por ciento más en comparación con 2016. De todos ellos, 1.126 fueron catalogados como muy peligrosos y 65 como críticos.

Los datos los ofrecieron dos miembros del equipo de Gestión de Incidentes del CCN, quienes también realizaron un recorrido por los principales ciberataques que se han producido en los últimos 12 meses. Entre ellos, los más conocidos fueron los *ransomware* WannaCry o NonPetya, pero también se produjeron intentos de injerencia política a través de diferentes técnicas (como las acciones maliciosas dirigidas a manipular las elecciones autonómicas de octubre en Cataluña) o las amenazas persistentes avanzadas contra diferentes empresas o la Administración (como el caso de Emissary Panda, cuyo objetivo fue robar información y conseguir credenciales de acceso de varias compañías americanas).

Uno de los aspectos característicos de algunos de estos ataques es el desconocimiento real de su autoría. De hecho, suenan con frecuencia las operaciones llamadas 'de falsa bandera', definidas por David Barroso, CEO de CounterCraft, como: "operaciones encubiertas de gobiernos, corporaciones y otras organizaciones, diseñadas para que parezca que fueron llevadas a cabo por otras personas".

Las pautas de observación de los analistas para evitar este engaño deben centrarse –aclaró Barroso– en la infraestructura (dominios, correos, IP, binarios, etc.), así como en aspectos geopolíticos, operacionales (hora del ataque, por ejemplo) o en la reutilización de código de ataques anteriores.

Uno de los mayores exponentes de ataque de falsa bandera fue el que sufrió hace dos años la cadena de televisión francesa TV5 Monde, que

aparentemente procedía del grupo terroristas *Daesh* aunque quien estaba detrás realmente era el grupo APT28, ligado a Rusia.

En todo caso, la identificación de los culpables que hay detrás de un ataque también presenta lo que el profesor de Ciencias Políticas de la Universidad Pablo de Olavide de Sevilla Manuel Torres llamó el 'dilema de la interpretación'. El experto se refería con ello a las dificultades que se presentan a la hora de conocer cómo se comportan los enemigos en la red. La visión segmentada de la realidad, dar por válidos ciertos axiomas que no están demostrados o los límites de la medición son algunos de los obstáculos que se encuentra el analista en Internet.

Para atenuar esa incertidumbre, Torres ofreció lo que desde su punto de vista es la mejor opción: la inteligencia. "El análisis técnico no nos dice, por ejemplo, si un ataque es un acto de represalia o si tiene una inspiración política. Por ello, hace falta incorporar otros elementos que tienen que ver con la ciencia política, el conocimiento experto, etc.", sostuvo.

Vulnerabilidades

Ya en el segundo día del evento, Raúl Siles, fundador y analista de seguridad de Dinosec, desgranó algunas vulnerabilidades y explicó cómo los atacantes se aprovechan de ellas para adentrarse en los sistemas tecnológicos de las organizaciones. Para concienciar a los presentes, este profesional se refirió a BlueBorne, una vulnerabilidad del Bluetooth que puede afectar a 5.000 millones de dispositivos, pues simplemente con que se tenga activada esta conectividad inalámbrica un atacante puede enlazar con el dispositivo e infectarlo con *malware*. Por eso, recomendó para 2018 "inventariar todas las tecnologías de la empresa y actualizarlas a las últimas versiones disponibles".

El sector público volvió a ser el protagonista en una mesa redonda donde participaron directivos de ocho empresas de seguridad TIC. Todos ellos se refirieron a la necesidad de mejorar las medidas de seguridad en las distintas administraciones públicas fomentando la colaboración público-privada y mejorando la concienciación entre todos los usuarios.

Para concluir dicho encuentro, intervino Javier Candau, quien puso sobre la mesa los problemas que tienen las administraciones públicas a la hora de contratar tecnología de seguridad. "En España, en los procesos de contratación se prima mucho la libre competencia y el precio, y a veces se dejan a un lado las certificaciones o la calidad de las personas que dan el servicio", afirmó el jefe del Departamento de Ciberseguridad del CCN. Algo, continuó, sobre lo que se debe trabajar.

Javier Candau, jefe del Departamento de Ciberseguridad del CCN.

Para terminar su intervención, Candau enumeró los objetivos del sector público para ser más seguro: "Tenemos que auditar y controlar la calidad del sistema; también hay que parchear; así como vigilar seleccionando la mejor tecnología; y por último, compartir las amenazas para que el resto se beneficie de ello".

A partir de aquí, las sesiones se dividieron en varias salas. En una de ellas, Ramsés Gallego, experto de Symantec, abordó el tema de la inteligencia artificial y el *machine learning,* y cómo estas tecnologías pueden ayudar al sector de la ciberseguridad. "Con el *machine learning* pretendemos entrenar a las máquinas para predecir patrones. Para ello, es necesario tener datos, muchos datos y plantear una hipótesis que será cierta o no, según la calidad de esos datos".

El experto confirmó que el *machine learning* se divide en cuatro pilares fundamentales: el supervisado, en el que la presencia humana es fundamental para sacar conclusiones; el no supervisado, en el que no se necesita tanta intervención; el *reinforcement learning*, en el que la máquina aprende de sí misma; y el *deep learning*, "basado en capas de redes neuronales que permite a la máquina aprender qué variables de datos son importantes para la pregunta que se le ha hecho".

A las capacidades relacionadas con la inteligencia artificial se suman otras que ya son una incipiente realidad, como el Internet de las Cosas. La seguridad es ya un reto cuando todos los dispositivos que se fabrican cuentan con algún modo de conexión a Internet; por ello, como alertó Juan Garrido, investigador en ciberseguridad, es necesario apostar por la seguridad desde el diseño de los aparatos o aplicaciones. "Tenemos muchos dispositivos y todos ellos nacen con la idea de poder conectarse a Internet. Ahora bien, en ese proceso hay que tener en cuenta un aspecto importante como es el de la seguridad", advirtió.

Otros muchos profesionales completaron con sus intervenciones unas jornadas que crecen en interés cada año, como muestras sus cifras de asistencia. No en vano, la asistencia aumentó en esta edición de las Jornadas STIC un 21 por ciento respecto a la de 2016.

Premios CCN-CERT

El CCN entregó durante las Jornadas STIC sus primeros premios a la trayectoria profesional en favor de la ciberseguridad. La vicepresidenta del Gobierno fue la encargada de entregarles el galardón a los dos premiados de este año: José Antonio Mañas, catedrático de la Universidad Politécnica de Madrid y desarrollador de la herramienta PILAR de análisis de riesgos, y José Antonio Mirá, asesor del CCN. ■