El CCN celebró sus X Jornadas STIC-CCN CERT con récord de asistentes y manifestando la necesidad de aunar esfuerzos en ciberseguridad tanto a nivel nacional como internacional

Con más de 1.800 peticiones de inscripción y un aforo completo ocupado por 1.400 asistentes expertos en seguridad, el **Centro Criptológico Nacional (CCN)** celebró los pasados 13 y 14 de diciembre, en Madrid, sus X Jornadas STIC CCN-CERT. En esta ocasión, el evento fue abanderado por el lema "Diez años fortaleciendo la seguridad cibernética", con motivo del aniversario de la creación de este ya consolidado encuentro que tuvo su primera edición el 14 de noviembre de 2007.

Diez años en los que "ha sido preciso renovarse todos los días" y en los que "el CCN ha gestionado más de 66.000 ciberincidentes en Administraciones Públicas y empresas de interés estratégico; se han elaborado más de 80.000 reglas de detección de intrusiones; y se han creado 17 herramientas de detección análisis e intercambio de información propias, además de realizar 135 auditorías de seguridad y páginas web". Así lo destacaba **Javier Candau**, Jefe de Ciberseguridad del CCN, durante la jornada de inauguración realizada junto con **Félix Roldán**, Secretario de Estado y Director del **Centro Nacional de Inteligencia (CNI),** quien no dudó en felicitar al CCN por el éxito de convocatoria y, sobre todo, por el "camino inimaginable" recorrido en este tiempo por su Equipo de Respuesta a Incidentes.

De cara al futuro, Roldán aseguró, "seguir trabajando intensamente en tres grandes líneas: detección de intrusiones, creación de tecnologías y formación de personas". Y es que, se evidenciaron cifras muy ilustrativas:el CCN recibe diariamente 2,5 millones de eventos de seguridad y registra 1,5 incidentes al día de carácter muy grave o crítico, provocados principalmente por APTs con exfiltración de información, DoS distribuidos, ataques dirigidos y código dañino específico.

Análisis de la actualidad

Tras la inauguración, el evento continuó con un plantel de ponentes procedentes tanto de organizaciones públicas como de parte de las 32 entidades privadas. Durante dos jornadas, los expertos analizaron la situación de la ciberseguridad en España, y se adentraron en temáticas tan candentes como el ciberespionaje, la evolución de las APTs, el Esquema Nacional de Seguridad (ENS) y los actuales modelos para el intercambio de Información, entre otras materias. Asimismo, jalonando las jornadas también tuvieron lugar sesiones más técnicas que cubrieron temas específicos como las intrusiones a través de nuevas formas de software malicioso, la *shell* en la web, el *crypto-malware*, o los usos y abusos de las *blockchains* a través de ponencias tan llamativas como "Votando entre tiburones" o "Malware Kung Fu++", entre otras.

Colaboración internacional

Tras dos días intensos, **Luis Jiménez**, Subdirector Adjunto del CCN, y **Ricardo Mor**, Embajador en Misión Especial para la Ciberseguridad del **Ministerio de Asuntos Exteriores y de Cooperación**, se encargaron de clausular el evento reflexionando sobre el aumento de las capacidades de los expertos en ciberseguridad, así como de los organismos especializados de nuestro país. Y es que, según Mor, "España cuenta con recursos tecnológicos y experiencia formidables en el ámbito de la ciberseguridad, y con un marco legal y normativo muy avanzado en comparación incluso con los países punteros de Europa, alcanzando, incluso, una dimensión internacional en la materia". En este sentido, el Embajador destacó la participación de España en acciones conjuntas con la UE, la OTAN, Naciones Unidas, la OSCE y la Organización de Estados Americanos. "Este es el camino; es necesario reforzar la ciberseguridad a través de la colaboración internacional entre aliados, socios y amigos", además de "fomentar aún más una cultura de la ciberseguridad, entre los usuarios y responsables de los sistemas de información, tanto del sector privado como del sector público", concluía Mor.

MESA REDONDA

La armonización de los sistemas de notificación de ciberincidentes: 'ventanilla única'

En el transcurso de las jornadas, se dio paso a una de las dos mesas redondas organizadas. En ella, **José de la Peña** (Revista SIC) fue el encargado de moderar un debate con **Gema Mª Campillos** (MINETADSESIAD), **Andrés Calvo Medina** (AEPD), **Daniel Acuña** (ISDEFE), **Fernando Sánchez** (CNPIC) y **Luis Jiménez** (CCN) los cuales, fueron los ponentes que, subidos en la palestra, reflexionaron sobre la idoneidad de contar con una ventanilla única dada la futura transposición de la Directiva NIS, la cual, insta a disponer de un sistema adecuado y eficiente para la notificación de ciberincidentes.

En este sentido, todos ellos aludieron a la importancia de contar con dicho sistema tanto para la notificación de ciberincidentes, como para la mejora de la gestión y supervisión de la ciberseguridad de cara al futuro. Aunque, dada la diversidad de autoridades competentes existentes, se planteó la duda acerca de a cuántas autoridades habrá que notificar un mismo incidente, en qué formatos y con qué herramientas. Por este motivo, se declaró de vital importancia la armonización y la creación de un modelo de notificaciones automática y ágil, especialmente, en cuanto al destinatario, el remitente y los campos a cumplimentar, así como la necesidad de reflexionar sobre la definición de "ciberincidente" con la necesidad de crear una taxonomía lo más horizontal posible de forma que, cuando se transponga la Directiva NIS, se integre y adecue lo mejor posible, no solo para las administraciones públicas sino, también, para la empresa privada.

MESA REDONDA

¿Son las Administraciones Públicas un cliente de peso en el mercado español de la ciberseguridad?

Con **Luis Fernández** (Revista SIC) como moderador, las jornadas dieron paso a otra mesa redonda que contó con ponentes de la talla de **Félix Muñoz** (InnoTec), **Héctor Sánchez** (Microsoft), **José Miguel Rosell** (S2 Grupo), **Xavier González** (Opennac), **Xavier Homs** (Palo Alto) y **Rosa Díaz** (Panda), para debatir sobre el actual papel que juega el sector público y su peso en el mercado de la ciberseguridad nacional.

Para medir el pulso a la Administración Pública, en primer lugar se les pidió a los ponentes revelar cuál es el porcentaje que ésta representa en su facturación global. Para la gran mayoría, supone entre un 20 y un 35% de su volumen de negocio, denotando aún el notable peso del gasto privado. Ante estas cifras, Candau (CCN), único representante del sector público en el estrado, afirmó que existe bastante presupuesto, pero que éste está fragmentado. "Por ejemplo, en el CCN el 60-70% del presupuesto se dedica a la compra de tecnología, y entiendo que hay que invertir también en servicios especialmente de ciberinteligencia", puntualizaba. A ello las empresas añadían la necesidad de que las AAPP aumenten la presencia de la ciberseguridad en sus agendas de la mano del sector privado. Para Candau, en este punto es importante que las empresas demuestren sus capacidades, como por ejemplo, su adecuación al ENS y, especialmente, ofrecer a la Administración Pública confianza y sencillez en las tecnologías y los servicios ofrecidos.