El 9ENISE ejerce como escaparate global de la ciberseguridad

Con nueve ediciones a sus espaldas, el Encuentro Internacional de Seguridad de la Información (ENISE), organizado por Incibe, se ha consolidado como punto de encuentro de los profesionales a nivel global, como lo demuestra que en 2015 haya contado con representantes de Europol, Interpol, FBI o la Organización de Estados Americanos. La asistencia de este año alcanzó la cifra récord de 1.100 personas.

Tx: Bernardo Valadés/David Marchal
Ft: Red Seguridad

Miguel Rego, director general de Incibe, y Fernando Sánchez, director del CNPIC, durante la inauguración del 9ENISE.

LOS PASADOS 20 Y 21 DE OCTUBRE, el Parador de San Marcos de León acogió la novena edición del Encuentro Internacional de Seguridad de la Información (9ENISE), que, organizado por el Instituto Nacional de Ciberseguridad (Incibe), congregó a cerca de medio centenar de ponentes y 1.100 asistentes (el aforo más amplio de todas las ediciones del evento) con el objetivo de analizar los avances más significativos del sector.

Bajo el lema "Ciberseguridad: motor para el desarrollo de la economía y la sociedad digital", las jornadas fueron inauguradas por Miguel Rego, director general de Incibe, y Fernando Sánchez, director del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). El primero destacó que las ciberamenazas, orientadas tanto a contextos privados como corporativos, son cada vez más peligrosas y sofisticadas, por lo que urge "agilizar su detección y luchar contra ellas más eficazmente en un entorno sin fronteras físicas como el cibernético". Además, Rego ensalzó el desarrollo económico del sector de la ciberseguridad, que en España crece anualmente al 12 por ciento y emplea a cerca de 43.000 personas.

Continuando con las ciberamenazas, preocupan, de manera especial, las que puedan afectar a las infraestructuras críticas, encargadas de prestar servicios esenciales a la ciudadanía. Al respecto, Fernando Sánchez reveló que, entre enero y septiembre, en nuestro país se gestionaron cerca de 70 ciberincidentes contra ese tipo de servicios, cifra similar a la registrada durante todo 2014. Por sectores, los más apetecibles para los cibercriminales son los de la energía, el transporte, el agua y el financiero.

En cuanto a los ciberincidentes tratados a nivel nacional desde el CERT de Seguridad e Industria de Incibe, en el periodo reseñado se contabilizaron 39.000, el doble que el año pasado.

Seguridad Nacional

A continuación, Miguel Rego dio paso a Joaquín Castellón, director operativo del Departamento de Seguridad Nacional (DSN), a quien agradeció el trabajo que desde el órgano dependiente de Presidencia del Gobierno se ha realizado en materia de ciberseguridad. Castellón inició su ponencia hablando de la Ley de Seguridad Nacional que vio la luz el pasado mes de septiembre. "La norma que, probablemente, más apoyo ha tenido por parte de las formaciones políticas. Está pensada para afrontar los nuevos retos y la ciberseguridad encaja en ella como un guante", valoró. A esta última la consideró uno de los grandes desafíos junto al terrorismo internacional, precisamente, minutos después de que la Guardia Civil detuviese a una ciudadana española cuando se disponía a viajar a Turquía ante las sospechas de su posible integración en el Daesh.

Y si interesante resultó el desarrollo de la ponencia de Joaquín Castellón, no lo fue menos su recta final, en la que sorprendió a los asistentes al anunciar que "desde el DSN apostamos por la creación de un Centro Nacional de Ciberseguridad que colabore con el sector privado y facilite una mayor conexión con los organismos oficiales, al tiempo que coordine el CNPIC, el Incibe, etc. Podría presidirlo un secretario de Estado, pero esto es una opinión personal", concluyó.

Una revolución sin precedentes

Seguidamente, tomando como base ese escenario futuro en el que pudiese crearse un Centro Nacional de Ciberseguridad, Orlando Ayala, vicepresidente senior del Grupo de Desarrollo de Mercados Emergentes de Microsoft, dibujó un marco global propiciado, entre otros factores, por los hábitos de los nativos digitales conocidos como *millenials*.

Según el directivo de la compañía norteamericana, "nos encontramos en el amanecer de una revolución que no tiene precedentes". Y mostró su preocupación al revelar que "en EEUU apenas se llega al 50 por ciento en materia de ciberseguridad empresarial". Por ello, no consideró descabellado que, a corto y medio plazo, dicha actividad, en clara expansión, pueda llegar a dar empleo a seis millones de personas en el planeta. Un mundo, subrayó el colombiano, "en el que España debe ejercer un papel de liderazgo".

Contexto regulatorio

Ciertamente, va camino de ser así a tenor de los avances legislativos que se han producido en los últimos años, protagonistas de la mesa redonda "El nuevo contexto regulatorio", que moderó Francisco Pérez Bes, secretario general de Incibe. En ella, la magistrada Alejandra Frías López, vocal del Consejo Nacional de Ciberseguridad, hizo hincapié en que "España es el único país del mundo que, a través del Informe Anual de Seguridad Nacional, define los peligros que pueden acechar a la nación. Y con las reformas que hemos hecho durante la última legislatura, somos uno de los países más avanzados en lo que a regulación se refiere". Por su parte, Elvira Tejada de la Fuente, fiscal jefe de Criminalidad Informática, consideró que es importante legislar al tiempo que se respetan los derechos de los ciudadanos. Y para lograrlo, explicó que la Fiscalía General del Estado ha apostado por la especialización. "Estamos haciendo de punta de lanza del Ministerio de Justicia en esta materia", avanzó.

La edición de este año congregó a cerca de medio centenar de ponentes de instituciones, empresas y otras organizaciones.

Pablo García Mexía, profesor de Derecho de Internet de la universidad William & Mary, creyó necesario promover convenios internacionales en materia de regulación, mientras que Carlos Alberto Saiz, director del Data Privacy Institute de ISMS Forum Spain, abogó por un papel más activo del sector privado tanto en legislación como en gobernanza.

España como ejemplo

La agenda matinal finalizó con las intervenciones de Raúl Antonio Villegas, director de Ciberseguridad del Gobierno de México, y Pedro Janices, director de la Oficina Nacional de Tecnologías de Información (ONTI) de Argentina. En el caso del primero, anunció que, siguiendo el modelo español, en su país se contempla la creación de un CNPIC, mientras que el segundo alabó la labor realizada durante estos años por el Incibe, "toda una referencia para nosotros", enfatizó.

Ya en horario vespertino, Robert Hayes, director de Ciberseguridad y Protección de Datos de Microsoft, propuso una serie de recursos para prevenir los ciberataques en el seno empresarial y acusó a las compañías de recurrir a soluciones básicas. "Si los consejeros delegados tuviesen un perfil tecnológico, serían más beneficiosos para las organizaciones", resumió.

La primera jornada finalizó con la entrega de trofeos de los ejercicios internacionales CyberEx, que recayeron en el CERT de la Universidad de la Plata (Argentina), el equipo de Colombia y Renfe.

Castilla y León y Microsoft impulsan el "Silicon Valley" de la ciberseguridad

Un día antes de la inauguración del 9ENISE, Microsoft, una de las firmas participantes en el encuentro, y la Junta de Castilla y León anunciaron la ampliación del acuerdo que ambas entidades mantienen con el objetivo de impulsar y desarrollar la creación de empresas innovadoras de base tecnológica en la región. Dicha iniciativa contempla la participación de Microsoft en la lanzadera que el Gobierno autonómico, a través de la Agencia de Innovación, Financiación e Internacionalización Empresarial, ha creado en el Parque Tecnológico de León con el fin de promover la creación de empresas especializadas en ciberseguridad. En concreto, la compañía estadounidense colaborará como socio estratégico e impulsará el desarrollo y crecimiento de las nuevas empresas, proporcionando hasta 120.000 dólares en productos y servicios tecnológicos a cada una de ellas, además de formación, consultoría y asesoramiento especializado. En la actualidad, la ciberseguridad es una de las áreas que presenta mayores oportunidades para los emprendedores. Según la consultora Gartner, el sector alcanzará un volumen global de 76.900 millones de dólares en 2015, cifra que supone un crecimiento del 8 por ciento respecto al año pasado. Por lo que respecta a España, el mercado de la ciberseguridad superó los 150 millones de euros en 2014.

Emprendimiento

La segunda jornada se inició con una mesa redonda sobre el emprendimiento en el ámbito de la ciberseguridad. Para Daniel Solís, fundador de Blueliv, "poner en marcha un negocio supone una cura de realidad importante". De hecho, según el directivo, no todo el mundo está preparado para emprender. Algo en lo que coincidió Antonio Ramos, socio fundador de Leet Security: "lo primero que hay que tener claro es cuál es el modelo de negocio que se quiere llevar a cabo, y después rodearte de profesionales mejores que tú", reveló. Simón Roses, por su parte, puso el acento en la vocación internacional que ha de tener cualquier negocio a la hora de ponerlo en marcha. "Hay que tener una visión global desde el principio", afirmó. Finalmente, el moderador, Bruno Fernández, consejero delegado de ENISA, se encargó de recordar a los asistentes los programas de financiación que esta entidad tiene para que los emprendedores puedan poner en marcha su idea de negocio.

Internet de las Cosas

En la siguiente mesa redonda se analizó cómo la ciberseguridad se está adaptando a las nuevas necesidades que trae consigo el Internet de las Cosas (IoT). Para ello contó con la presencia de Masaya Norifusa, responsable de Ciberseguridad de Nec, quien explicó las diferencias entre seguridad tradicional y ciberseguridad y puso el ejemplo de Japón, donde recientemente se ha creado el Centro de Control de Ciberdelito. "Con este organismo esperamos llegar a frenar los ciberataques", afirmó; aunque reconoció que resulta complicado, habida cuenta de la proliferación de los dispositivos IoT en el mercado.

Para Jon Pérez, coordinador de la línea de investigación en sistemas embebidos de Ikerlan, "existe una necesidad de mercado de dotar a los sistemas de mayor inteligencia y mantenimiento más eficiente, con más servicios de valor añadido. La industria debe dar respuesta a esto a través de tecnología IoT y M2M". A continuación, Pérez puso un par de ejemplos de su aplicación: los ascensores y la señalización ferroviaria.

Finalmente, Ramón Sáez, representante del Centro Criptológico Nacional (CCN), hizo un breve recorrido por la historia reciente de la tecnología para exponer cómo se ha llegado al Internet de las Cosas, una tendencia que va a crecer de manera exponencial en los próximos años. No en vano, abogó por "incluir la seguridad en el ciclo de vida de los productos IoT, habilitarla por defecto, realizar revisiones periódicas de los dispositivos e implementar estándares de seguridad".

Gestión del talento

La mesa redonda que siguió se centró en analizar las claves para la atracción y retención del talento de los profesionales de la ciberseguridad desde la óptica de varios ejecutivos. Por ejemplo, Telefónica ha iniciado un proceso de transformación para ser empresa de gestión de datos, dejando a un lado la voz. Esto, en palabras de Eva Atienza, su directora de Recursos Humanos, está conduciendo la gestión del talento hacia ese objetivo. "Nuestro reto es que nuestros profesionales realicen este tipo de programas más especializados y robustos", confirmó.

Por su parte, José Ignacio del Barrio, socio de Ackermann Beaumont, puso sobre la mesa "el papel crítico" que desempeña el área de Recursos Humanos a la hora de "seleccionar profesionales y desarrollarlos en el mundo de la ciberseguridad". El problema para el directivo es que hay "una brecha entre la formación base y las necesidades que después demanda la empresa", afirmó.

En el caso de PwC tienen esto muy claro y cuenta con "un modelo de carrera profesional en el que cada candidato pueda comprobar el camino que debe seguir", en palabras de Elena Maestre, socia responsable de los servicios de Riesgos Tecnológicos de la consultora. En contrapartida, le ofrecen apoyo en el proceso y recompensas no sólo económicas.

Y desde el punto de vista de las administraciones públicas, también es importante el impulso del talento. Por ejemplo, Javier Requeijo, jefe del Área de Salidas Profesionales de la subdirección General de Reclutamiento y Orientación Laboral del Ministerio de Defensa, explicó en qué consiste el programa SAPROMIL, puesto en marcha por esta división, que se encarga de recoger las solicitudes de quienes se quieren desvincular de este organismo, y a través del cual formar a técnicos en ciberseguridad para ponerlos a disposición de las empresas. "El personal de las Fuerzas Armadas es perfectamente válido para después trabajar en cualquier empresa privada en este ámbito", señaló.

Cooperación internacional

El siguiente aspecto que se abordó fue la cooperación internacional

La novena edición del ENISE batió el récord de asistencia de este evento anual con 1.100 personas.

a partir, en primer lugar, de la experiencia de Belisario Contreras, gerente del Programa de Seguridad Cibernética de la Organización de Estados Americanos (OEA). Para este directivo, es crucial promover "un cambio de mentalidad, puesto que ya hay que considerar el mundo físico y el virtual uno solo"; así como potenciar tanto la cooperación como la confianza internacional. Para ello abogó por la creación de redes internacionales de cooperación. Precisamente sobre esto habló también Silvino Schlinkmann, asistente del director de Investigación e Innovación de la Interpol. En su intervención destacó los acuerdos que tienen distintos países en vías de desarrollo, a los que ofrecen "el conocimiento y las herramientas que tienen los países desarrollados".

Para finalizar, José Durán, representante de España en el J-CAT Europol, habló sobre las áreas de cooperación que en este sentido tienen Europa y Estados Unidos; mientras que Beatriz Ramos, jefa del grupo de investigación de delitos tecnológicos en la Policía Nacional, se centró en explicar las tres áreas en las que más hincapié está haciendo la Policía: "explotación sexual infantil, fraude por medios de pago y ciberataques".

'Hacktivismo' y cibercrimen

El siguiente panel intentó dar forma a una tendencia cada vez más extendida de protestar ante lo que se consideran injusticias: el *hacktivismo*, un movimiento que, según David Barroso, representante de Lost in Security, "se ha profesionalizado. Ahora se ha visto que es peligroso y no gracioso", opinó. Incluso, los gobiernos optan por esta forma de extorsionar, según apuntó Román Ramírez, de RootedCON: "El cibercrimen también lo comenten los gobiernos y las agencias, por lo que deberían ser castigados igualmente", aseguró. Y este fenómeno no ha hecho más que simplificarse, como comentó José Selvi, de SANS Expert. "Con las nuevas tecnologías, es más fácil extorsionar. Por ejemplo, cualquiera puede contratar a un experto para tumbar una empresa entera", señaló.

Nuevas tendencias

Aleccionadora también fue la ponencia de Alberto Hernández, director de Operaciones del Incibe, pues mostró a los asistentes la realidad de los ciberataques. "En lo que llevamos de año se han producido más de 39.000 incidentes de seguridad, más del doble que en todo 2014, de los cuales 70 corresponden a infraestructuras críticas", desveló. El crecimiento de estas amenazas, por tanto, está siendo de más de 3.000 al mes. Ante esto, Incibe está generando una media de 3.000 notificaciones mensuales a empresas y ciudadanos para alertarles de sus vulnerabilidades, y está poniendo en marcha "una decidida política de colaboración con distintos CERT nacionales", puntualizó.

Economía digital

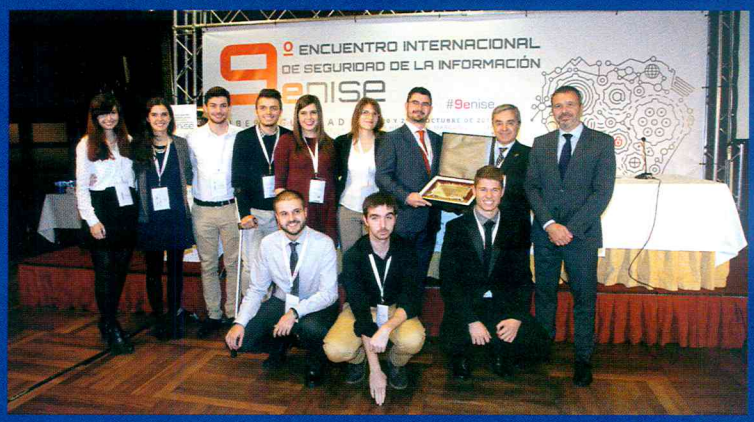
La jornada concluyó con un panel dedicado a la economía digital, en la que intervinieron Santiago Niño, economista y catedrático de la Universitat Ramón Llul; y Carlos Rodríguez, economista y catedrático de la Universidad Complutense de Madrid.

El primero se mostró convencido de que el sector de la ciberseguridad crecerá "más del 8 por ciento en todo el mundo" de aquí a 2020. Según el economista: "se va a disparar la necesidad de seguridad, porque somos conscientes de que existen problemas que no se resuelven por los caminos normales como la escasez de recursos, el excedente del factor trabajo o el exceso de capacidad productiva".

Por su parte, Rodríguez defendió el sentimiento de miedo, porque es "un movimiento del ánimo que nos hace apartarnos del mal que existe o puede existir. Por tanto, preocuparnos por nuestra seguridad es racional e imprescindible", manifestó. Y para vencer ese miedo se encuentra la tecnología, la cual también ayuda a incrementar la productividad y hace que la economía pueda mejorar.

Finalmente, la clausura corrió a cargo de Miguel Rego, director de Incibe, quien abogó por impulsar la cooperación entre todos los actores del sector de la ciberseguridad, tanto en el ámbito nacional como en el internacional. ■

El premio 9ENISE, para un grupo de estudiantes de la Universidad Carlos III



Antes de la clausura del congreso, Incibe entregó el premio 9ENISE al mejor vídeo de concienciación en ciberseguridad a un equipo de la Universidad Carlos III de Madrid, liderado por dos profesores del Computer Security Lab del Departamento de Informática de la entidad académica: José María de Fuentes y Lorena González. El equipo se complementó con ocho antiguos alumnos de la asignatura Criptografía y Seguridad de la Información de la universidad madrileña que están cursando el grado de Ingeniería en Informática.

El jurado estuvo compuesto por representantes de varios medios de comunicación, incluyendo a Borrmart (editora de *Red Seguridad*), además de ISMS Fórum, Incibe y profesionales del ámbito de la ciberseguridad en general.

El Reglamento de Protección de Datos europeo verá la luz en la primavera de 2016

El Reglamento General de Protección de Datos comunitario ha recibido el visto bueno de la Comisión de Libertades Civiles del Parlamento Europeo. La publicación de su versión definitiva verá la luz durante la primavera de 2016.

Tx: Bernardo Valadés

La Comisión de Libertades Civiles del Parlamento Europeo ha respaldado el acuerdo sobre protección de datos, alcanzado en la UE, que establece una normativa para regular la privacidad en la era digital, modernizando así un marco legal que se remonta a la década de los años noventa. De esta forma, tras un complejo proceso de negociación entre la Eurocámara, la Comisión Europea y el Consejo Europeo, se ha dado luz verde al nuevo Reglamento General de Protección de Datos comunitario, cuya versión definitiva se publicará en la primavera de 2016.

Según Udo Helmbrecht, director ejecutivo de la Agencia de Seguridad de las Redes y de la Información de la UE (ENISA), "el nuevo reglamento concede una mayor participación y poderes de ejecución a las autoridades nacionales competentes. Un elemento importante de este acuerdo, a menudo subestimado, es su potencial para proporcionar una ventaja competitiva a la industria europea mediante la adopción de la privacidad y la protección de datos como valor central".

Mejoras significativas

En el caso de nuestro país, la Agencia Española de Protección de Datos (AEPD) destaca las "mejoras significativas" que supone el reglamento europeo. "Por ejemplo", señala, "produce un máximo efecto armonizador que permitirá reducir las divergencias actuales en nivel y mecanismos de protección. Y también es importante mencionar que será de aplicación a toda empresa que trate de forma sistemática datos de ciudadanos europeos, esté o no establecida en la UE".

Además, añade, "el reglamento mejora los instrumentos de control por parte del ciudadano de sus datos personales, fundamentalmente con una mejor definición del consentimiento. Pero también con la introducción de nuevos derechos como el de la portabilidad, específicamente vinculado al entorno digital y con el que las personas ven mejorada su capacidad de decisión".

Finalmente, la agencia valora que el nuevo texto defina "un modelo de responsabilidad proactiva por parte de quienes tratan los datos de los europeos y, al mismo tiempo, amplíe y flexibilice los mecanismos que regulan sus transferencias internacionales con el objetivo de que en todo momento reciban un nivel de protección equiparable al que se les otorga en la UE".

Ámbito empresarial

Por su parte, Carlos Alberto Saiz, director del Data Privacy Institute de ISMS Forum, ha declarado a *Red Seguridad* que "el reglamento va a ser bienvenido, especialmente, por los grandes grupos de empresas, que tendrán más claras unas reglas del juego sobre tratamiento de datos únicas en el entorno europeo, y también por los proveedores tecnológicos y de soluciones de *cloud computing*. Es fundamental que las organizaciones, públicas y privadas, hagan un buen trabajo de adecuación a estos nuevos requisitos normativos en los próximos dos años para instaurar un sistema completo de gestión de los aspectos de la privacidad, que ganan relevancia en la operativa empresarial y donde primarán conceptos como *privacy impact assesment, privacy by design, accountability y data protection officer*".

Entre las novedades del reglamento se encuentra la obligatoriedad de contratar un Delegado de Protección de Datos (DPO, por sus siglas en inglés) en todas las organizaciones públicas (a excepción de los tribunales en ejercicio de la potestad jurisdiccional) y en determinadas organizaciones privadas, en general en aquellas que desarrollen *profiling* o traten datos de categorías especiales.

Al respecto, Ricard Martínez, presidente de la Asociación Profesional Española de Privacidad (APEP), comenta que "el DPO deberá posibilitar que el funcionamiento de la organización y la consecución de los objetivos lícitos y legítimos del negocio sean compatibles con la garantía del derecho fundamental a la protección de datos y la seguridad de la información. Igualmente, será el interlocutor con el regulador y la AEPD, así como el colaborador que, sin duda, necesitará cualquier institución". ■