

## REPORTAJE

28 de noviembre de 2013. Málaga

### **XIV JORNADA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN** **CYBER THREATS SITUATIONAL AWARENESS - THINKING FORWARD**

# CYBER THREATS SITUATIONAL AWARENESS THINKING FORWARD

> *La XIV Jornada Internacional de ISMS Forum analizó las estrategias nacionales de ciberseguridad y ciberdefensa desde las perspectivas europea y americana y examinó la competitividad de las empresas en relación al ciberespionaje gracias a la participación de organismos y empresas punteras en el sector como el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), el Centro Criptológico Nacional (CCN), Inteco, IBM, Symantec, Deloitte, Microsoft, Innoverly, Akamai, McAfee, PwC, Eleven Path, Trend Micro, Check Point y Cisco.*

Alrededor de 280 asistentes se dieron cita en la **XIV Jornada Internacional de ISMS Forum** que tuvo lugar el pasado 28 de noviembre en el Palacio de Ferias y Congresos de Málaga. Bajo el título ‘*Cyber Threats Situational Awareness - Thinking Forward*’, el evento congregó a destacados expertos del sector que, desde distintas perspectivas, analizaron tanto las estrategias nacionales de ciberdefensa como los retos de las grandes y pequeñas compañías en cuanto a la protección de la información y el ciberespionaje.

En relación al primero de estos grandes temas versó la ponencia de **Howard A. Schmidt**, ex asesor de la Casa Blanca en materia de ciberseguridad, que fue una de las más esperadas y aplaudidas de la jornada. Schmidt resaltó la increíble evolución que ha sufrido el sector de Internet en los últimos 20 años. Una progresión que incluye las dos caras de una misma moneda. De un lado, sus beneficios y su inmenso universo de posibilidades pero, del otro, también, un buen número de fraudes surgidos al calor de esta tecnología. El reto de combatir la acción delictiva en el ciberespacio ha sido el reto de la ciberseguridad que, progresivamente, ha ido aumentando sus recursos tanto tecnológicos como humanos en respuesta al **desafío que supone la puesta en riesgo de la ingente cantidad de información que reside en Internet** (y que implica a toda la sociedad en su conjunto, desde los Gobiernos hasta los ciudadanos, pasando por las empresas).

Del caso español y su Estrategia de Seguridad Nacional, con sus múltiples líneas de actuación, habló **Fernando J. Sánchez**, Director del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), quien expuso con detalle los diversos riesgos y amenazas a los que se enfrenta cada día las redes y sistemas de información de nuestro país. En su conferencia, Fernando J. Sánchez hizo especial hincapié sobre la **necesidad de “capacitación de profesionales en materia de ciberseguridad”** que velen por la defensa y protección de dichos sistemas de información en base a

una capacitación público-privada tanto en foros y eventos como en determinados ejercicios cibernéticos, publicaciones y campañas de sensibilización”. El director del CNPIC cerró su intervención con la exposición de su pleno convencimiento de que **“no se puede disociar la ciberseguridad de la seguridad física”** y realizó una llamada a la acción a este respecto por cuanto que, afirmó, **“no es momento de centrarse en quién hace qué sino en unir esfuerzos para responder a una demanda de la sociedad”**.

Y es que la realidad actual de la ciberseguridad en España es, tal y como dejó patente en su intervención **Javier Candau**, Jefe del Área de Ciberseguridad del Centro Criptológico Nacional (CCN), que España es objeto a día de hoy de multitud de ciberataques. Un hecho comprobado en el ‘Informe de amenazas 2012 y tendencias 2013’ realizado por el CCN-CERT, organismo adscrito al Centro Nacional de Inteligencia (CNI), que revela cómo **durante el pasado año 2012 los ataques recibidos se han convertido en la más significativa de las amenazas** y la protección contra ellos se ha convertido a su vez también en una de las principales preocupaciones de los responsables de seguridad de Tecnología de la Información. Así, y según este informe, las organizaciones —tanto públicas como privadas— que manejan información con alto valor estratégico, económico o político son hoy más vulnerables que nunca, por cuanto que las medidas de seguridad no terminan de estar debidamente implantadas. En este sentido, Candau cifró en “menos de un 25% la capacidad de detección de los sistemas de seguridad, lo cual significa”, concluyó, **“que apenas se detectan 1 de cada 4 ciberataques”**.

Sobre ciberdefensa y la necesaria colaboración público-privada versó la primera mesa redonda de la jornada, moderada por **Fernando Picatoste**, partner de Deloitte, y compuesta por **Nick Coleman**, Global Head Cyber Security Intelligence de IBM; Ignacio González, Deputy Director of Operations Directorate de Inteco; y Zoltan Precsenyi, Government Affairs Manager de Symantec. Coleman señaló dos retos fundamentales en materia de ciberdefensa que, a su juicio, radican en el **exacto entendimiento, por un lado, de los escenarios a defender y dónde tienen lugar estos ataques a fin de saber aplicar las óptimas medidas de seguridad** en función de las particularidades de cada circunstancia; y, por otro, en la adecuada capacidad del analista encargado de velar por dicha seguridad en cuanto a la correcta selección de los eventos clave a estudiar, las políticas de prevención, la gestión de riesgos, etc.

**Ignacio González** remarcó la tremenda importancia que, a su juicio, tiene hacer frente a las ciberamenazas de manera conjunta intercambiando información y conocimientos, al respecto de lo cual hizo mención de ENISA, la Agencia Europea de Seguridad de las Redes y la Información, y cuya misión principal no es otra que el intercambio de información, mejores prácticas y conocimientos en el campo de la Seguridad de la Información. Un ejemplo de que, apuntó, “los Gobiernos lo tienen claro: **tenemos y debemos colaborar y es imprescindible construir las infraestructuras que permitan esta colaboración”**.

Sobre este intercambio de información, **Zoltan Precsenyi** reclamó **“una legislación específica y muy precisa sobre confidencialidad de datos que la posibilite de manera segura”**. “Existe una gran cantidad de información sensible y crítica que permitiría a la comunidad mejorar sin duda su seguridad pero que”, puntualizó, “en manos erróneas podría llegar a causar un increíble daño”. Precsenyi reconoció la gran demanda por parte de las empresas españolas de compartir información pero, al mismo tiempo, también la reclamación de unas redes de confianza que posibiliten y garanticen este proceso.

Uno de los retos más importantes de las empresas es crear valor desde la privacidad y la seguridad. **Ismael Valenzuela**, Principal Architect and Foundstone EMEA de McAfee, reconoció el gran reto que ante sí afrontan las compañías en materia de seguridad, muchas de las cuales carecen de una estrategia o de herramientas para ello, y, de manera muy gráfica, afirmó que **“hay muchas empresas que se están enfrentando a una pistola con una cuchara”** en este sentido.

**Cornelia Kutterer**, Director Inst. Relations EU and Director of Regulatory Policy de Microsoft, hizo memoria de los 11 años que lleva Microsoft atendiendo a las exigencias de ciberseguridad lanzadas por sus clientes. “Ya no somos tan sólo una empresa de software”, admitió, “sino una empresa de servicios y consultoría sobre ciberseguridad y en este sentido hemos entendido que debemos ser muy transparentes en cuanto a los datos, también garantizamos la seguridad con sistemas de encriptación cada vez más sofisticados e incluso **trabajamos desde hace 11 años con el Consejo de Europa para armonizar las reglas internacionales sobre protección de datos y ciberdelitos**”. Con todo, Kutterer no dejó de apuntar los riesgos para la innovación —en cuanto a bloqueo de la misma— que puede llegar a causar un exceso de regulación.

**“La seguridad no es algo que podemos dar por sentado tanto desde el punto de vista jurídico como tecnológico”**. Con esta contundente frase comenzó su intervención **Martin McKey**, Security Advocate de Akamai, quien reconoció que en los últimos años se ha producido un daño enorme a la seguridad de la información en Internet y reclamó una puesta a punto en este ámbito progresiva por parte de unas empresas con las que, en opinión de **Gianvittorio Abate**, Chief Executive Officer de Innovery, **se antoja imprescindible realizar un intensivo trabajo de concienciación a nivel de seguridad**.

Acerca de qué está pasando en las empresas españolas en cuanto a ciber-espionaje y competitividad trató de dar respuesta la mesa redonda presidida por **Carlos A. Saiz**, Vicepresidente de ISMS Forum Spain, y conformada por expertos de primer nivel como Chema Alonso, Chief Executive Officer de Eleven Path; Javier Candau, Jefe del Área de Ciberseguridad del CCN; y David Sancho, Investigador Senior anti-malware de Trend Micro. En ella se abordó la situación en cuanto a seguridad de la información de sus sistemas por parte de las pequeñas y medianas empresas (PYMES) españolas, las cuales sufren cierto grado de indefensión (total para algunos de los componentes de la mesa) por cuanto que su capacidad y sus recursos para hacerle frente son escasos. Una vulnerabilidad que los miembros de la mesa señalaron de manera unánime habría de ser paliada con la colaboración de la Administración Pública.

**Javier Candau** focalizó en **el alto nivel de vulnerabilidad de muchas empresas** que, pesar de tener antivirus en sus puestos informáticos —“lo cual afortunadamente ya está en el ADN de mucha gente”, reconoció— siguen manteniendo un alto nivel de vulnerabilidad ante ataques informáticos. Por su parte, **Chema Alonso** focalizó en **el “ransomware” como el principal problema de seguridad en las pequeñas y medianas empresas españolas**. Mientras que **David Sancho** llamó la atención sobre multitud de ataques a Pymes que se realizan de manera continuada en el tiempo y de forma tan sigilosa que, afirmó, **“hemos tenido en Trend Micro casos de clientes que han dado la voz de alarma hasta tres años después de haber empezado a ser atacados”**.

El nivel de confianza en el Cloud Computing fue el último de los temas debatidos en esta XIV Jornada que contó con la presencia de destacados expertos en la materia como **Luis Buezo**, Presidente del Cloud Security Alliance, **Mario García**, Director General Iberia de Check Point; **Román Vargas**, Security Business Developer Manager de Cisco; y Mariano J. Benito, Coordinador del Comité Técnico Operativo del Cloud Security Alliance España.

**Mariano J. Benito** documentó la existencia de **hasta un 77% de empresas españolas que tienen toda o parte de su información subida al Cloud**, siendo el almacenamiento el servicio por excelencia para el que se emplea esta herramienta, mientras que el correo electrónico queda en una tercera posición. Unas cifras que revelan una mayoritaria adhesión de las empresas a este servicio del Cloud Computing y que, sin embargo, tal y como puso en evidencia Benito, no se corresponde para nada con el nivel de satisfacción que sobre él tienen los usuarios: quienes le ponen como nota más alta apenas un 4 sobre 10. “Parece que en España los proveedores de Cloud no están cumpliendo las expectativas de los usuarios”, sentenció Mariano J. Benito.

### Patrocinadores de la Jornada

La XIV Jornada Internacional de ISMS Forum Spain es posible gracias al respaldo de sus patrocinadores, empresas de referencia en España que muestran así su compromiso con la Seguridad de la Información. Patrocinadores Oro: **Akamai, Check Point, Cisco, Deloitte, HP, IBM, Innovery, McAfee, PwC, Symantec, Telefónica y Trend Micro.**

### Sobre ISMS Forum Spain

[La Asociación Española de la Seguridad de la Información, ISMS Forum Spain](#), es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. ISMS Forum Spain tiene ya a más de 120 empresas asociadas y más de 800 profesionales asociados. La Asociación es ya, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.