REPORTAJE

28 de mayo de 2014. Madrid

XV JORNADA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN

LA SOCIEDAD DIGITAL ENTRE CONFIANZA Y CIBER-RIESGOS

Salón de Actos de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. C/ Capitán Haya, 41, Madrid.

LA SOCIEDAD DIGITAL ENTRE CONFIANZA Y CIBER-RIESGOS

Los retos a los que se enfrenta la sociedad digital actual pasan inevitablemente por la defensa activa de la seguridad y la privacidad de sus integrantes: ciudadanos, empresas, organizaciones y países en su conjunto. La XV Jornada Internacional de ISMS Forum Spain que tuvo lugar el pasado 28 de mayo en la Secretaría de Estado y Telecomunicaciones y para la Seguridad de la Información del Ministerio de Industria, Energía y Turismo, reunió a expertos representantes de organizaciones tanto pública como privadas de primera línea para debatir sobre el pasado, presente y futuro de la seguridad de la información en un mundo global.

El acto comenzó con la apertura de la Jornada por parte del presidente, vicepresidente y directora general de ISMS Forum Spain, Gianluca D´Antonio, Carlos A. Saiz y Ariadna Hernández respectivamente, quienes agradecieron, por adelantado, la participación de los ponentes, además de la asistencia de **más de 300 profesionales**, que llenaron por completo la sala, y la colaboración de los **Global Gold Sponsors** (Akamai, Cisco, Deloitte, HP, Intel Security, Symantec, Telefónica y Trend Micro), **Gold Sponsors** (BT, Fire Eye, Huawei, IBM, Kaspersky y Necsia), **INTECO** e **ISACA** y **Media Partners** (Grupo Atenea, Dintel, GlobbTV y Red Seguridad).

Tras la bienvenida, comenzó el discurso inaugural del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, Víctor Calvo-Sotelo, quien resaltó la revolución mundial que está suponiendo la evolución en las TICs. “Siete de cada 10 ciudadanos en nuestro país y prácticamente todas las empresas españolas desarrollan su actividad en el ciberespacio”, afirmó, al tiempo que no ha querido dejar de destacar la otra cara de la moneda que no es sino “la inminente necesidad que existe en este contexto por establecer un clima de confianza adecuado”.

“Siete de cada 10 ciudadanos en nuestro país y prácticamente todas las empresas españolas desarrollan su actividad en el ciberespacio”, Víctor Calvo-Sotelo.

Calvo-Sotelo hizo mención de las acciones que, con este objetivo fundamental, se han llevado a cabo desde el Gobierno, tales como la aprobación de la Estrategia de Ciberseguridad Nacional en diciembre del pasado año 2013, además del órgano encargado de ejecutar los planes específicos en ella definidas: el Consejo de Ciberseguridad Nacional. Dos iniciativas que cuentan con un presupuesto superior a los 59 millones de euros (desde 2013 hasta 2015), lo cual es un indicativo, en palabras del Secretario de Estado, del "grado de compromiso adquirido en materia de ciberseguridad por parte de la Administración".

Seguidamente, el auditorio contempló la ponencia de Martin Libicki, Senior Management Scientist, RAND Corporation y Visiting Proffesor, US Naval Academy, quien expuso un recorrido por los múltiples riesgos que acechan a los usuarios digitales que cada día son más numerosos en todo el mundo y crecientemente interconectados. Ya que a día de hoy, recalcó Martin, la práctica totalidad de la vida de los ciudadanos que viven en países desarrollados se articula en torno a lo que en sus inicios este experto ha denominado no era más que "un juguetito". Ordenadores que hoy por hoy se sitúan en el centro del funcionamiento social. Martin Libicki hizo asimismo especial hincapié en la imprescindible colaboración entre países sin duda cuando se produce un incidente en la seguridad de uno de ellos, pero también, puntualizó, antes de que éste se produzca. Una colaboración internacional que redunda en la seguridad nacional de cada país en concreto. Libicki también analizó las particularidades e implicaciones de la ciberguerra en comparación con las características y desarrollo de una guerra 'tradicional'.

A continuación, Dimitra Liveri, Security and Resilience of Communication Networks Office in the CIIP Unit, European Network and Information Security Agency (ENISA) explicó las funciones de este organismo europeo (que cumple este año su décimo aniversario), y que Liveri sitúa en el eje de la arquitectura de la seguridad de la Unión Europea. Recordó cómo la Estrategia de Ciberseguridad de la UE (2013) apeló a la colaboración de ENISA para el correcto cumplimiento de varias de sus estrategias principales y mencionó los ciberejercicios que ENISA ha realizado en los últimos años y en los que España ha participado activamente. Liveri apelaba también a la necesaria colaboración público-privada en ciberdefensa, un requerimiento que ha sido leit motiv de esta Jornada Internacional.

Dimitra Liveri formaría parte también de la posterior mesa redonda que, bajo el título **'Fighting emerging Cyber Treats'** y coordinada por Carles Solé, Director, Spanish Cyber Security Institute, contó con la participación de Vicente Pastor, Head, Enterprise Security Services Cell Senior Engineer, Cyber Security, NATO; Paolo Passeri, System Engineer, Lastline; Creator of the Cyber Attacks Timelines at Hackmageddon.com; Ilias Chantzos, Senior Director of Goverment Affairs EMEA, Global CIP and Privacy Advisor, Symantec. Carles Solé incidió en la proporcionalidad existente entre la interconexión digital, cada vez mayor, y la consiguiente vulnerabilidad. Una vulnerabilidad que, según Solé, "afecta no sólo a la propia evolución tecnológica sino también a la competitividad de las empresas por lo que se antoja imprescindible la creación de un entorno de confianza, logrado sin duda gracias a la cooperación imprescindible entre los distintos agentes implicados".

'Cyber Security Trends that will concern your business' fue el título escogido para la mesa redonda en la que, tras la pausa del café a media mañana, participaron Greg Day, VP & Chief Technology Officer EMEA, Fire Eye; Maurice Cashman, Director, Enterprise Architects EMEA, McAfee part of Intel Security; y Loïc Guezo, Information Security Evangelist – Director, Southern Europe, Trend Micro; bajo la moderación de Juan Miguel Velasco, Member of the Advisory Council, ISMS Forum Spain. Una mesa de diálogo que comenzó con la intervención de Greg Day, con una reflexión acerca del significado del éxito frente a las ciberamenazas. "¿Qué es realmente el éxito? ¿El volumen de ataques que impedimos que se produzcan cada día o, por el contrario, el impacto que evitamos que se produzca en las organizaciones a consecuencia de estos ataques?", planteaba el representante de Fire Eye, que sin duda se decantó por la segunda de las respuestas. "Todas las empresas tienen su razón de ser en la creación de beneficios", afirmaba, "por tanto el éxito ha de medirse por la capacidad de mitigar el impacto que pueda llegar a afectar a estos beneficios". Day abordó también la singularidad de los ciberataques y cómo en los últimos tiempos éstos se han personalizado en función de la víctima. "Tenemos que saber defendernos de las invasiones singulares y no sólo de los ataques masivos".

Por su parte, Maurice Cashman, apelando a su experiencia militar, realizó un símil con este campo al afirmar que "de igual modo que en el mundo militar lo principal es la supervivencia de los soldados, en las empresas lo fundamental es la continuidad del negocio". Y, respondiendo a la pregunta sobre el éxito formulada por su compañero de mesa, Cashman fijó en tres los parámetros para medirlo: velocidad, agilidad y colaboración. A su juicio, los dos primeros se encuentran muy lejos de ser alcanzados en materia de ciberseguridad por parte de las empresas (ya que, según estudios del Sector, las empresas tardan una media de 240 días en detectar que están siendo víctimas de un ciberataque) y el tercero tiene aún mucho recorrido a todos los niveles: tecnológico, de intercambios de información relevante, entre toda la comunidad, etc. Y es que, según Cashman, para que una nación sea resistente lo tienen que ser sus empresas y organizaciones. Y si los directivos de éstas comparten información, esto revertirá en el fortalecimiento del país en su conjunto.

"Según la última encuesta de ISACA, existen un millón de vacantes en el ámbito de la seguridad de la información". Un dato que puso encima de la mesa Loïc Guezo a fin de poner de manifiesto la falta de recursos de la que muchas empresas aún hoy siguen adoleciendo. Trend Micro, sin embargo, ha afirmado, "puede enorgullecerse de ser una compañía muy fuerte en investigación y desarrollo. De las 5.500 personas que forman el equipo humano de Trend Micro, el 25% se dedica a I+D". Guezo hizo hincapié en la creciente actividad maliciosa en aplicaciones y dispositivos móviles: "a finales del primer trimestre del presenta año hemos detectado hasta dos millones de aplicaciones maliciosas". El representante de Trend Micro también mencionaba en su intervención la relevancia de las denominadas AAP (Amenazas Avanzadas Personales), para luchar contra las cuales su empresa dispone de un equipo especializado, además de la colaboración que mantienen con organismo de seguridad como la Interpol, Europol y, en España, la Guardia Civil.

La tercera mesa redonda de la Jornada giró en torno al **'Information Security within the Internet of Things'**. En ella participaron, con la moderación de Ramsés Gallego, David Francis, UK Chief Security Officer, Huawei; Sean Newman, Security Evangelist and Field Product Manager in EMEA for Cyber security vendor, Sourcefire parto f Cisco; Martin Borrett, Director, institute for Advanced Security Europe, IBM; y José Francisco Pereiro, Head of Assure Iberia, BT. La realidad es que a día de hoy estamos cada vez más interconectados digitalmente. Una realidad que tiende a hacerse más y más compleja en este sentido. Igual de complejo que es el denominado 'Internet de las cosas' que, Martin Borret denominaba como "un sistema de sistemas para el que precisamos", reclamando "nuevos protocolos y normas y de cuya "inteligencia" vamos a poder beneficiarnos en un futuro próximo para analizar y detener actividades maliciosas".

David Francis, por su parte, destacaba el tremendo avance protagonizado por las TICs en las últimas dos décadas y que, en su opinión, ha traído simultáneamente consigo una falta de confianza por parte de los usuarios. Asimismo, planteó que la seguridad sea abordada desde el principio en todos los procesos empresariales, además de que el CEO de toda empresa se implique a este nivel igual que se implica en los demás aspectos de su negocio. "Internet de las cosas ya está aquí", afirmaba Sean Newman, quien instó a un cambio de mentalidad necesario a la hora de entender la seguridad por cuanto que "en la actualidad la mayoría de los ciberataques son dirigidos hacia un objetivo concreto y no podemos seguir utilizando métodos tradicionales para defendernos". Newman constataba también que "el perímetro de seguridad ya ha desaparecido y el reto se encuentra ahora en parar los ataques antes de que provoquen un impacto en nuestras organizaciones".

José Francisco Pereiro cifró en más de 26.000 millones los dispositivos conectados a Internet en todo el mundo, situando el comienzo de la revolución tecnológica en el Internet de la Cosas a partir del momento que nos sean personas comunicándose con la máquina sino las máquinas dialogando entre sí; y enumeraba tres puntos a tener en cuenta en esta tendencia creciente del Internet of Things. En primer lugar, las comunicaciones y su disponibilidad, ya que, "si en la actualidad estos dispositivos están conectado a Internet a través, por ejemplo, de Bluetooth, en el futuro se conectarán a través de IPs lo que va a suponer un reto tanto para los proveedores de contenidos (que habrán de ofrecer grandes ampliaciones de los anchos de banda) como para los profesionales de la seguridad. En segundo lugar, la gestión de la vulnerabilidad por cuanto que "el desarrollo seguro es una de las áreas más débiles de las empresas". Y, por último, la privacidad. "En el futuro, el espía, el atacante, no va a ser como ahora una multinacional o un país, sino que podrá ser cualquier persona".

La cuarta mesa redonda de la Jornada, **'Ciberespacio en el ámbito de la seguridad nacional'**, con la moderación de Fernando Picatoste, Partner, Deloitte; reunió por primera vez desde la aprobación de la Estrategia de Ciberseguridad Nacional a los principales representantes y articuladores en materia de ciberseguridad en España, como el General de Brigada Carlos Gómez López de Medina, Jefe del Mando Conjunto de Ciberdefensa; Miguel Rego, Director General de INTECO; Joaquín Castellón, Director Operativo del Departmento de Seguridad Nacional; Fernando Sánchez, Director del CNPIC; y Gianluca D´Antonio, en representación de ISMS Forum Spain.

GB Carlos Gómez de Medina recordó que el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) fue creado hace aproximadamente un año y medio y, en este tiempo, sus acciones se han centrado en las que son sus dos principales áreas de actividad: la defensa de sistemas de telecomunicaciones militares, además de la defensa de todos aquellos sistemas que se les asigne, siendo en cualquier caso su máxima prioridad, ha afirmado, "la mejora de la capacidad operativa y la formación del personal militar en el área de la ciberseguridad".

Joaquín Castellón, por su parte, destacó la aprobación el pasado año de la Estrategia de Ciberseguridad Nacional (donde se definen hasta 12 riesgos a combatir) y el Consejo Nacional de Ciberseguridad (órgano encargado de hacer cumplir y ejecutar los planes específicos elaborados a partir de la Estrategia). Castellón aseguraba que, a día de hoy, "la ciberseguridad es una de las prioridades en la agenda de nuestro país" y enumeró una serie de condicionantes imprescindibles en este ámbito como son un adecuado marco legal, una correcta organización, cooperación internacional, la construcción de una cultura de seguridad y la necesaria colaboración público-privada.

Desde INTECO, Miguel Rego explicó el papel del Instituto Nacional de Tecnologías de la Información (INTECO) que, para su desarrollo en el periodo que va desde 2013 hasta el próximo año 2015, cuenta con una dotación económica de 59 millones de euros lo que, en palabras de Rego, "es símbolo del compromiso de la Administración en el ámbito de la ciberseguridad". Las funciones de INTECO a día de hoy pasan por la concienciación en materia de ciberseguridad, el impulso de la industria, la mejora de capacidades del Centro de Respuesta a Incidentes de Seguridad (CERN) y la implementación de una serie de iniciativas para el desarrollo de talento de los profesionales en ciberseguridad. Todo ello, tal y como afirmó Rego, con "la aspiración de ser un organismo horizontal de los que otros agentes puedan beneficiarse".

"Los límites se van difuminando cada vez más y el panorama está cambiando a marchas forzadas", alertó Fernando Sánchez quien no olvidó recordar que el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) fue pionero en la introducción en España de conceptos como 'seguridad integral' y la colaboración público-privada en esta área. Asimismo, avanzó que, en menos de un mes, estarán listos los planes estratégicos sectoriales de la energía, nuclear y financiero en el ámbito de la protección de las infraestructuras críticas (enmarcados dentro del proceso de implantación del Sistema de Protección de Infraestructuras Críticas, en el marco de la Ley 08/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC), y su desarrollo reglamentario a través del Real Decreto 704/2011).

El coloquio finalizó con la intervención por parte de Gianluca D´Antonio quien destacó la vocación de ISMS Forum para constituirse como un aglutinador de todos los agentes que en esta mesa convergen y promotor de la colaboración público-privada, y aseguró que el camino por el que deben transitar las acciones precisas en materia de ciberseguridad en España está ya bien marcado.

Tras un receso para el almuerzo y el networking, la Jornada continuó con la primera mesa redonda de la tarde constituida a partir del tema **'Security within the Apps based on Cloud Computing'** presidida por Luis Buezo, Chairman, Cloud Security Alliance España, IT Infraestructure and Cloud Computing Director EMEA, HP; y en la que participaron expertos como Federico Dios, Security Analyst, Akamai; Jesús Millán Lobo, Head of IT Risk & Security Business services, Telefónica España; y Ángel Márquez, Partner, Necsia. Todos ellos focalizaron en tres cuestiones centrales los problemas actuales que existen en los servicios Cloud y que pasan, en primer lugar, por la inseguridad en el tratamiento de los datos que existe en los usuarios de este tipo de servicios, la necesaria homologación de certificados que vengan a asegurar esta cuestión y, por último, la dificultad que encuentran los usuarios de servicios en la Nube a la hora de migrar sus datos o interconectarlos con otras herramientas Cloud.

Además, Federico Dios cifraba en un 30% el tráfico web mundial que pasa por Akamai y, bajo su experiencia, afirmaba que en la actualidad la mayor parte de ataques a aplicaciones de sus clientes se llevan a cabo desde modelos Cloud. Jesús Millán reconocía el uso cada vez más extendido del modelo Cloud en forma ya sea de páginas web, correo electrónico, almacenamiento de datos, aplicaciones de negocio, etc. Y Ángel Márquez hizo hincapié en las prácticas que existen para securizar los datos en los dispositivos, ante la multitud de procesos por los que éstos pasan, y cada uno de los cuales entraña un riesgo.

'La privacidad como herramienta para la Confianza Digital' tenía como título la última mesa redonda moderada por Carlos A. Saiz, Vicepresidente, ISMS Forum Spain; Director, Data Privacy Institute; Attorney, Partner and Head of Governance, Risk & Compliance practice, Ecix Group y compuesta por Rafael García Gozalo, Vocal Asesor Jefe del Área Internacional, Agencia Española de Protección de Datos; Iñaki Pariente, Director, Agencia Vasca de Protección de Datos; y María Àngels Barbarà, Directora, Autoridad Catalana de Protección de Datos. Los cuatro integrantes de la mesa mostraron su preocupación por un Reglamento Europeo de Protección de Datos que se encuentra en proceso de aprobación pero que probablemente se retrase sine die a consecuencia de las recientes elecciones europeas. También coincidieron todos ellos en que la privacidad se trata de un valor añadido que las empresas de servicios han de ofrecer a sus clientes y que dicha privacidad ha de exigirse por parte de las autoridades competentes desde el diseño ya no tanto a golpe de sanción como de incentivos.

Por supuesto, la conocida como 'sentencia Google' fueron objeto de debate en esta mesa redonda donde todos sus participantes reconocieron su importancia si bien, tal y como puntualizó Rafael García Gozalo, "no se trata de una sentencia rompedora". En referencia a la polémica que esta sentencia ha causado desde distintos sectores que la critican por entrar en colisión con el derecho a la información, Maria Àngels Barbarà recordaba que no existen derechos absolutos y que esta sentencia que ratifica el derecho al olvido se circunscribe a los resultados de búsquedas y no a la anulación de la información en sí misma (lo cual habría de realizarse por otras vías en caso de que se trate de una información inexacta, no autorizada, etc.). Por su parte, Iñaki Pariente señaló que a partir de ahora se abre un periodo de incógnitas en cuanto al método por el cual buscadores como Google llevarán a cabo este tratamiento de datos y cómo velarán por el cumplimiento de este

derecho al olvido. "¿Se tratará de un proceso mecanizado que atenderá a todas las peticiones en el momento en que se formulen o, por el contrario, será un tratamiento individualizado que afronte cada petición de manera personalizada?", cuestionaba.

Por último, la Jornada culminó con la dinámica ponencia del científico, escritor y conferenciante Gonzalo Álvarez Marañón, autor del libro 'El arte de presentar' quien explicó ante una audiencia entregada los objetivos, métodos y herramientas a aplicar para llevar a cabo una presentación en público que deje huella y conecte con el público. Así, a base de ejemplos y juegos para los que el autor solicitó la participación de los presentes, Gonzalo Álvarez ha abordado los métodos existentes para lograr conectar con la audiencia en una presentación tanto a nivel intelectual, como ético y emocional, además de ofrecer una serie de consejos para captar la atención y, por último, enumeró una serie de técnicas dirigidas a fomentar la comprensión y el recuerdo de la temática expuesta.

Patrocinadores de la Jornada

La XV 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.

Akamai, BT, Cisco, Deloitte, Fire Eye, HP, Huawei, IBM, Intel Security, Kaspersky, Necsia, Symantec, Telefonica y Trend Micro.

XV JORNADA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN

LA SOCIEDAD DIGITAL ENTRE CONFIANZA Y CIBER-RIESGOS

Global Gold Sponsors

Akamai · Cisco · Deloitte · hp · intel Security · Symantec · Telefónica · TREND MICRO

Gold Sponsors

BT · FireEye · HUAWEI · IBM · KASPERSKY lab · NECSIA