CONCLUSIONES DE LA XI JORNADA INTERNACIONAL DE ISMS FORUM

LOS RIESGOS TECNOLÓGICOS A LA CABEZA DE LAS PREOCUPACIONES MUNDIALES

La XI Jornada Internacional de ISMS Forum analizó cómo los Estados y empresas afrontan las nuevas amenazas surgidas en un mundo cada vez más dependiente de las TIC. Con la participaron del World Economic Forum, la Comisión Europea, el Supervisor Europeo de Protección de Datos, el Centro para la Protección de Infraestructuras de Holanda, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, la Cloud Security Alliance, RAND Europa, y empresas como La Caixa, Check Point, Corporate Executive Board, Deloitte, Ferrovial, HP, IBM, ICB, Kaspersky, KPMG, McAfee, Prosegur, Symantec, Repsol YPF, Telefónica y Trend Micro.

Más de 300 asistentes se dieron cita en la XI Jornada Internacional de Seguridad de la Información de ISMS Forum Spain, que se celebró el pasado 6 de junio con el título *Riesgos tecnológicos, regulación y responsabilidad en un mundo globalizado e hiperconectado*. El evento congregó en Madrid a destacadas personalidades procedentes del World Economic Forum, instituciones de la Unión Europea, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, la iniciativa Cloud Security Alliance, junto a proveedores y fabricantes claves de la industria y compañías españolas multinacionales.

Como argumenta el World Economic Forum, en los últimos años han aparecido nuevas vulnerabilidades derivadas de la dependencia cada vez mayor que tienen las empresas y los Estados de los sistemas interconectados. Por ello, su último informe sobre riesgos globales, *Global Risks 2012,* subraya los riesgos tecnológicos como una de las mayores preocupaciones mundiales para los próximos 10 años.

La conferencia del **Director Gerente y máximo responsable del Centre for Global Events and Risk Response Network del World Economic Forum, W. Lee Howell**, fue una de las participaciones más esperadas y aplaudidas. Ofreció las claves de este exhaustivo informe, que señala que existe un "lado oscuro de la conectividad". "Nuestra vida diaria es casi enteramente dependiente de los sistemas interconectados, lo que nos hace vulnerables ante individuos, instituciones y naciones maliciosas, quienes han incrementado su capacidad para desatar devastadores ciberataques de forma remota y anónima", comentó Howell.

Dentro de la categoría de riesgos tecnológicos, el estudio refleja que **los ciberataques son los riesgos más probables**, y tienen un alto impacto. Por su parte, el fallo de sistemas críticos representa el riesgo con mayor impacto, pero con una probabilidad más baja. Lee Howell comentó que los principales objetivos de los ciberataques son tres: sabotaje, espionaje y subversión; y alertó que cada uno de los dispositivos o sistemas que están conectados de una forma u otra a una red puede ser comprometido por grupos externos. "Muchos de esos

compromisos todavía no han sido detectados", aseveró. De este modo, solicitó poner en marcha mecanismos que detecten las vulnerabilidades y garanticen un espacio digital seguro. Por último, puso sobre la mesa algunas recomendaciones para la "ciberresiliencia", dirigidas tanto al sector público como el privado, ya que cualquier solución debe partir de la idea del "**reconocimiento de interdependencia**" entre todos los actores implicados.

Ciberseguridad en un mundo globalizado e hiperconectado

La XI Jornada abordó las políticas y las estrategias que los organismos públicos y privados llevan a cabo con el objeto de afrontar este nuevo panorama de riesgos tecnológicos. Para su análisis se contó con la colaboración especial de dos de los **mayores expertos europeos en ciberseguridad, Andrea Servida (Comisión Europea) y Anne Marie Zielstra (CPNI.NL);** y, en materia de privacidad, el Supervisor Europeo de Protección de Datos, Peter Hustinx. También estuvieron presentes la iniciativa Cloud Security Alliance, RAND Europa, y representantes de empresas de primer nivel como La Caixa, Check Point, Corporate Executive Board, Deloitte, Ferrovial, HP, IBM, ICB, Kaspersky, KPMG, McAfee, Prosegur, Symantec, Repsol YPF, Telefónica y Trend Micro.

La sesión comenzó con una palabras del presidente de ISMS Forum Spain, Gianluca D'Antonio, quien recordaba la inminente presentación de una estrategia española para la ciberseguridad; y adelantó que la Asociación presentará una propuesta al Gobierno que "pretende ser un libro blanco" que aporte el conocimiento y la experiencia de un foro abierto y plural de profesionales y empresas con 5 años de historia como es ISMS Forum. El **Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, Víctor Calvo Sotelo,** destacó que "el Gobierno se preocupa por la Seguridad de la Información y la Protección de Datos Personales, ya que definirán la posición competitiva y de calidad de servicio que los ciudadanos disfrutarán en un futuro muy próximo". Por ello, informó que se incluirán estos temas un apartado muy destacado en la "agenda digital renovada para España".

La conferencia inaugural corrió a cargo del Jefe de Unidad Adjunto de la Dirección General de Sociedad de la Información y Medios de Comunicación (Comisión Europea), Andrea Servida. De título *Configuración de la estrategia de Seguridad para un Futuro Digital,* desgranó los principales ingredientes de las iniciativas llevadas a cabo por la UE en los últimos años, como la regulación europea sobre identificación electrónica y transacciones electrónicas desarrollada para favorecer la confianza en el entorno online y fortalecer un mercado digital seguro, y la **Estrategia Europea para la Ciberseguridad** cuya presentación, anunció, está prevista para finales de año.

Según informó Servida, su objetivo es asegurar la seguridad y "resiliencia" en el entorno digital para todos los ciudadanos de la UE, empresas y administraciones públicas, "prevenir con eficacia el cibercrimen; en el respeto a los derechos fundamentales y los valores europeos". Para ello, incidió en que desde las instituciones comunitarias se ha buscado estimular al máximo la colaboración público-privada "para aprovechar el *Know-How* y capacidad del sector privado", además de la cooperación internacional. Para Servida, en

materia de ciberseguridad hace falta un compromiso político mayor y hay que implicar a todos los actores para hacer un “frente común”.

Uno de los riesgos de mayor impacto es el que afecta a **las infraestructuras críticas**. Sobre su protección en el entorno comunitario se abordó en una mesa redonda moderada por Alfonso Mur, Head & Partner ERS de Deloitte. Neil Robinson, Research Leader de Rand Europa, con sede en Bruselas, ofreció algunas conclusiones del estudio que su organización ha desarrollado en el ámbito europeo, encargado por ENISA, haciendo hincapié en la necesidad de eliminar barreras e incertidumbres para un intercambio de información “de calidad”; lo que, además, ayuda a las organizaciones a “reducir el coste” de sus programas de protección de infraestructuras críticas. En este sentido, Anne Marie Zielstra, directora del Centre for Protection of the National Infrastructure (CPNI.NL) de Holanda, expuso el caso de su país y nombró los distintos organismos internacionales donde participa para promover el intercambio de información. La protección de las infraestructuras críticas “es una responsabilidad compartida” tanto entre el sector público y el privado, como a nivel nacional e internacional. Según Zielstra estas iniciativas funcionan si se comparte información en un entorno de confianza, y estos modelos se pueden y se deben promover.

Enmanuel Roeseler, Security Director de IBM, aportó la visión del fabricante, apostando por una “inteligencia de la seguridad” que permita ver todas las dimensiones de seguridad a la vez: datos, aplicaciones, personas e infraestructuras. Por su parte, Stephan Gerhager, Management Board and Head os Informationsecurity & Riskmanagement División de ICB, explicó gráficamente cómo se atacan las redes de distribución de energía eléctrica inteligente, las *smart grids* y propuso medidas para su protección. Para combatirlos lo importante, comentó, no es centrarse en aspectos exclusivamente tecnológicos, que son relativamente fáciles de violar, si no que hay que “fijarse en todo el modelo”, cuáles son los procesos, quién es responsable de qué en una *smart grid*, etc; y utilizar todo ese conocimiento para construir modelos que puedan modular los riesgos.

El nuevo panorama de riesgos tecnológicos

Fabricantes y clientes, representados por destacados profesionales españoles, debatieron sobre el nuevo panorama de **ciberamenazas**. Moderó Marcos Gómez Hidalgo, miembro de la Junta Directiva de ISMS Forum Spain y Subdirector de Programas en INTECO, quien introdujo el tema aludiendo a la recurrencia mediática actual de casos relacionados con la ciberseguridad y la privacidad.

Alejandro Villar, Chief Information Security Officer de Repsol, encuentra que “estamos viviendo un cambio de época”, “no sé si nuestra sociedad está preparada para ello”, aseguró. Así destacó que existe una gran “ignorancia” entre ciudadanos, empresas y gobiernos sobre temas de ciberseguridad. Todos coincidieron en que se hace imprescindible la concienciación sobre un uso seguro de la tecnología. Como destacó Joaquín Reixa, Director General para el sur de Europa de Check Point: “el mayor riesgo que existe es la persona”. En ocasiones “las empresas no saben dónde están sus datos”, exclamaba Vicente Díaz, Senior Malware Analyst, GREAT Team, Iberia, de Kaspersky.

David Barroso, Responsable de Inteligencia en Seguridad de Telefónica Digital, destacó "el derrumbe de los pilares de seguridad que tenemos hoy día", haciendo referencia a la violación de certificados SSL, entre otros problemas, y la entrada de nuevos jugadores, como los ciberactivistas y las naciones. Reixa incidió en esta idea de **ciberguerra**: "Si EEUU e Israel lo están haciendo, abren la puerta para hacer ataques cibernéticos".

Reforma de la normativa de privacidad en la UE

Dentro del marco general de riesgos tecnológicos, *leit motiv* de la XI Jornada, se analizó específicamente la reforma integral de la normativa de privacidad presentada recientemente por la Comisión Europea, que, previsiblemente, entrará en vigor en 2014. Para ello, se contó con la valiosa aportación del **Supervisor Europeo de Protección de Datos, Peter Hustinx**, quien quiso dejar claro desde el principio que el reglamento refuerza los derechos de los individuos, pero no se amplían. "No se trata de reinventar la protección de datos". El énfasis más importante, según Hustinx, está en la implantación y aplicación en la práctica. Se ha querido **dotar de mayor "efectividad" y "consistencia" a la norma**, además de procurar su armonización para todos los estados de la UE y su actualización al nuevo panorama tecnológico, marcado por un desarrollo exponencial de Internet.

Hustinx dio especial relevancia a la regulación del denominado "**derecho al olvido**", que tiene como objetivo que en la práctica "los individuos tengan derecho a la supresión de los datos en Internet" y a la portabilidad de los datos. Además se refirió al Principio de Responsabilidad de los agentes que gestionan datos personales, que ahora "comienza desde el principio", no cuando ocurre un problema. Por consiguiente, ganan en importancia las medidas, entre otras, que ponen en marcha las organizaciones para asegurar el cumplimiento normativo.

En cuanto a la aplicación del nuevo marco legal, Hustinx aseveró que el ámbito del derecho del UE ha sido redefinido. Ahora la ley básica va a ser igual en todos los Estados miembros, e incluso en terceros países, ya que las empresas que den servicio dentro de la UE deberán respetar la normativa europea, "incluso en el ámbito de Internet", comentó.

Por otro lado, explicó que "la cooperación está creciendo más allá de la UE" y que esta reforma es parte de una "**convergencia creciente en todo el mundo**". "Me atrevo a decir que el 80% está bajo consensos", concluyó. George Thompson, Information Security Director de KMPG, que acompañó a Hustinx en la mesa, aplaudió, en general, las propuestas, y comentó que cree que "debemos de ir mucho más lejos en cuanto a la armonización en todo el mundo" teniendo en cuenta, además, que hay países europeos que en este momento están basando sus economías en buena parte con las exportaciones y negocios con países de fuera de la UE. Y también para poder mejorar la competitividad de las empresas europeas con respecto a otros países con un marco normativo "más suave". Refiriéndose a la relación concreta entre UE y EEUU, Hustinx opinó que "estamos haciendo progresos lentamente", y comentó que Obama ya ha puesto sobre la mesa algunos aspectos que permitirían una mayor "aproximación" de ambas legislaciones; algo que se podría materializar en el caso de que fuera reelegido como presidente.

Protección de datos en el Cloud

Para abordar la protección de datos en la Nube, se organizó una mesa redonda específica con la participación de expertos en seguridad en Cloud Computing, procedentes de actores de referencia en la industria como HP, McAfee, Symantec y Trend Micro. Estuvo presidida por el Director Ejecutivo de la iniciativa Cloud Security Alliance (CSA), Jim Reavis.

Reavis presentó una encuesta realizada desde CSA que analiza las prácticas de seguridad en la Nube. Entre otras conclusiones, se informó que el 82% de los proveedores permitían algún tipo de especificación de una ubicación física de los datos, y se destacó que es una preocupación para CSA que sólo el 33% de estos cuenten con algún tipo de garantía sobre la supresión de datos, incluso cuando finaliza la relación con el cliente. Otro de los hallazgos del informe es que los proveedores están comenzando a incluir el servicio de encriptación de datos. En este sentido, Andy Dancer, Chief Information Officer EMEA de Trend Micro, comentó que parece pertinente para garantizar la seguridad que haya "una separación de obligaciones", entre el que realiza la encriptación, el proveedor de Cloud, y quien gestiona las claves, otro proveedor o el propietario de los datos.

Simon Hunt, VP, Chief Technology Officer, Endpoint Security de McAfee puso sobre la mesa que existen amenazas específicas para las infraestructuras físicas. "¿Si no podemos confiar en el hardware en el que funciona la Nube, como podemos confiar en alguna aplicación?", comentó. Por su parte, Enrique Matorras, Iberia Cloud Lead & Iberia Account Chief Technologist de HP destacó que "ir a la nube requiere desde el principio considerar la seguridad, y en todos los procesos", desde la fase de planificación hasta la post implantación. Todos los ponentes coincidieron en considerar que **la seguridad es uno de los servicios que aporta mayor valor en Cloud Computing**. Laurent Heslault, Chief Security Strategist EMEA Southern de Symantec declaró que además "El Cloud puede ser usado y será usado como herramienta de seguridad".

El papel del empleado en la seguridad de las organizaciones

Por otro lado, el programa de la XI Jornada de Seguridad de la Información también incluyó una conferencia de Jeremy Bergsman, Miembro de Information Risk Executive Council, Corporate Executive Board, quien presentó un estudio realizado por el Information Risk Executive Council (IREC), que analiza las **actitudes de los empleados hacia la seguridad**. Bergsman hizo hincapié en las potencialidades que tienen el estudio y el análisis de la psicología del usuario, muy útiles para elaborar modelos de sensibilización eficaces destinados a "cambiar el comportamiento" de riesgo de los empleados, evitando así errores que pueden afectar a la seguridad de la empresa y a su reputación. "Estamos convencidos de que la sensibilización de los empleados es un componente crítico del éxito", comentó.

Cómo abordar la seguridad en un entorno globalizado

La última sesión de la Jornada planteó la *Convergencia entre Seguridad Física y Lógica en un entorno globalizado*. Para ello, se organizó un debate que abordaba la coordinación entre profesionales, con el objeto de aunar los esfuerzos de seguridad y gestionar el riesgo de forma eficiente. Como destacó su moderador, Enrique Polanco, Miembro del Consejo Asesor de ISMS Forum Spain, no cabe duda que es necesario "**un frente global a una amenaza global**".

Carles Solé, Chief Information Security Officer de La Caixa, aseguró que "la convergencia no es una necesidad, es una realidad", pues "hay un objetivo común, por tanto hay un trabajo común". Juan Gross Aymerich, Corporative Security Manager de Ferrovial destacó que ya "se ha puesto al mismo nivel la seguridad física y la seguridad lógica" y que, a su juicio, el frente principal para los profesionales de la seguridad es conseguir que desde la alta dirección y el "negocio" se tengan en cuenta los requerimientos de seguridad en todo momento, asumiendo que suelen afectar a los tiempos de ejecución y al plan de negocio de la compañía. Por su parte, Antonio de Cárcer, Corporate Director of Security Consultancy and Sectorial Solutions de Prosegur, terminó su participación con una idea: "tenemos que conseguir ser un integrador global de soluciones para la gestión de riesgos".

Sobre las Jornadas Internacionales de ISMS Forum

Las Jornadas Internacionales de Seguridad de Información de ISMS Forum Spain son un foro de discusión y debate abierto que cuenta con la participación de representantes de **todos los actores implicados en el sector**: expertos, profesionales, instituciones y empresas de primer nivel. Todo ello, en un contexto que facilita el aprendizaje y el intercambio de experiencias entre los asistentes. En sus 11 ediciones han participado ya más de 200 ponentes y casi 3.000 asistentes. La próxima Jornada será en Barcelona en noviembre de 2012.