REPORTAJE

XVI JORNADA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN

20 de noviembre de 2014. Madrid

TOWARDS PREVENTION WITH RESILIENCE… AND BEYOND!

El auditorio de Mutua Madrileña volvió a albergar una jornada de reflexión sobre el complejo ámbito profesional de la Seguridad de la Información, sometido continuamente nuevas amenazas y ataques. En este encuentro, celebrado el pasado 20 de noviembre, la asociación ha querido poner el foco sobre la capacidad de resistir ante estos ataques y sobre la flexibilidad de las infraestructuras de TI para rehacerse tras un más que probable embate del cibercrimen organizado.

Como es habitual, esta XVI Jornada Internacional de ISMS Forum congregó a una notable representación de expertos y profesionales de la Seguridad TIC (un total de 285 asistentes acudieron a la cita) con la colaboración de los **Global Gold Sponsors** (Akamai, Blue Coat, Cisco, Deloitte, HP, Intel Security, IBM, SVT Cloud, Symantec, Telefónica y Trend Micro), **INCIBE** y **Media Partners** (Grupo Atenea, Dintel, GlobbTV y Red Seguridad).

, en busca de novedades, networking y conocimiento compartido. **Gianluca D'Antonio**, presidente de ISMS Forum Spain, fue el responsable de inaugurar este encuentro junto a **Carlos Alberto Saiz**, vicepresidente de la asociación, y la nueva directora general, **Sara Degli-Esposti**.

La ponencia inaugural de la jornada corrió a cargo del invitado estrella, **Benoit Godart**, Head del departamento EC3 Outreach de Europol, que presentó las principales conclusiones del informe Internet Organised Crime Threat Assessment (IOCTA). Este documento insta a las instituciones privadas a colaborar conjuntamente con las administraciones públicas en la lucha contra el ciberterrorismo. "La coordinación entre países europeos es importante, pero también lo es la colaboración internacional con países como Colombia, Canadá, Estados Unidos o Australia", declaró Benoit Godart. "En la actualidad, 2.800 millones de personas están conectadas a Internet, un gran logro de la tecnología y una gran oportunidad para el negocio. Esto es fantástico, pero este escenario presenta también que una situación ventajosa para los criminales contra los que estamos luchando".

El experto de Europol subrayó el aumento extraordinario de ataques personalizados, sobre todo a través de técnicas de phishing y orientadas a dispositivos móviles, según se recoge en el último informe de EC3. "El *Crime as a Service* (CaaS) es una realidad expandida en todo el planeta y supone una revolución para las investigaciones policiales, por lo que debemos facilitar el intercambio de

información a escala internacional. Muestra de ello es que Europol está impulsando la colaboración contra el fraude y otros delitos como la explotación sexual a través de Internet".

Por último, como caso real de colaboración público-privada, Benoit Godart citó el trabajo de Europol con las líneas aéreas para combatir el fraude, como la usurpación de identidad de los ciberdelincuentes para viajar gratis: "Es demasiado tarde cuando el banco se da cuenta de este engaño; todos juntos somos capaces de parar estas operaciones casi en tiempo real y 60 personas ya fueron detenidas el año pasado, con el inconveniente añadido de que ninguna de ellas estaba en nuestros registros –expuso Godart–. Debemos trabajar por la concienciación y reforzar la seguridad de Internet con alianzas globales".

A continuación, dio comienzo "*Construyendo una defensa resiliente frente a los ciberataques*", la primera mesa redonda de la jornada, moderada por Gianluca D'Antonio. El panel estuvo integrado por el propio Benoit Godart, en representación de Europol; **Michael Kaiser**, Executive Director de US National Cyber Security Alliance; **David Van Duren**, Coordinating policy advisor Cyber Security del Ministerio de Seguridad y Justicia de Países Bajos; y **Taylor Roberts**, Global Cyber Security Capacity Centre de la Universidad de Oxford.

Por su parte, David Van Duren destacó el nivel de cooperación que España ha logrado en los últimos años y destacó que la estrategia puesta en marcha hace ahora cuatro años en Países Bajos les está permitiendo conseguir una sociedad más responsable y consciente de los peligros del cibercrimen.

Michel Kaiser, en este sentido destacó que la inversión en seguridad está aumentando a todos los niveles, desde los hogares hasta los gobiernos: "Esto es bueno porque indica que aumenta la concienciación, pero no es suficiente. En Estados Unidos vemos cómo las pymes invierten en medidas de seguridad preventivas, pero no son resilientes. Esto es porque no están contemplando tecnologías que les ayuden a pensar en el futuro, a reaccionar después de un ataque".

Desde un punto de vista académico, Taylor Roberts se refirió a la ciberresiliencia como un concepto que precisa, además de las herramientas tecnológicas (encriptación, seguridad de red, etc.), de tres elementos clave y tangibles: organización, coordinación y compromiso. "Un modelo de madurez es necesario de cara al futuro para tener claras cuáles son las prioridades en cada área y contar con una evaluación continua de nuestra ciberresiliencia". La lucha contra el cibercrimen requiere una respuesta inmediata, extremadamente rápida, donde el trabajo más complejo es identificar a los atacantes, según refirió Benoit Godart: "Combatir el terrorismo en la Red y proteger a los menores, por ejemplo, son objetivos importantísimos y necesitamos la colaboración de todas las instituciones".

Tras el primer panel llegó el turno de **Miguel Rego**, director general del Instituto Nacional de Ciberseguridad (INCIBE), que focalizó su intervención en la identificación y gestión del talento en este sector, una problemática complicada en un tiempo en el que escasean profesionales formados en Seguridad de la Información. "En España existen unas 20.000 personas dedicadas a la ciberseguridad y se estima un crecimiento del 20% en la demanda, según un estudio que hemos realizado –apuntó Miguel Rego–. Desde INCIBE venimos trabajando en distintos aspectos para fomentar el desarrollo de 125 empresas dedicadas a ciberseguridad y contribuir a potenciar la demanda interna y externa de esta industria nacional".

Por otra parte, INCIBE estimula el interés de los jóvenes por la ciberseguridad con becas para prácticas en empresas y programas de formación práctica en institutos de Educación Secundaria a partir de proyectos piloto en Madrid, Castilla-León y Baleares. Además, según enunció Rego, el Instituto ha lanzado programas de formación a distancia (en modalidad MOOC) sobre diferentes facetas de ciberseguridad. En segundo término, INCIBE verá facilitada su tarea a la hora de detectar el talento entre aquellos alumnos que concluyan cada curso.

Tras la exposición del portavoz de INCIBE, dio comienzo un bloque de tres interesantes mesas redondas, nutridas por un conjunto de ponentes que estuvieron a la altura de las expectativas. La primera de ellas versó sobre "*Strategies for an effective defence against APTs*". Los contertulios que tomaron parte: **Loic Guezo**, Information Security Evangelist y Director para el Sur de Europa de Trend Micro; **Vicente Díaz**, Security Malware Analyst, de Kaspersky Lab; y **Darren Thomson**, Chief Information Security Officer de Symantec EMEA, fueron moderados por el partner de Deloitte, **Fernando Picatoste**. Todos ellos coincidieron en que la detección de amenazas persistentes avanzadas es cada vez más ardua en unas redes que cada vez son mayores y a las que acceden millones de dispositivos. Desde una perspectiva metodológica, el portavoz de Symantec hizo hincapié en la detección y respuesta como claves diferenciales: "La inteligencia y la preparación de los empleados (formación) debe ser una prioridad para desplegar una estrategia eficaz, realmente proactiva; el uso de tecnología es necesario pero de nada sirve si no permite adelantarse a las APTs".

Desde el punto de vista de Trend Micro, estas amenazas tan personalizadas están cambiando su orientación tradicional hacia las grandes organizaciones como las entidades financieras y tienden a democratizarse por medio de técnicas como el phishing. "Necesitamos construir redes de inteligencia global y Trend Micro está participando en ellas desde 2008 con el objetivo de reforzar funcionalidades como *Deep Packet Inspection* (DPI) y establecer una protección eficiente de próxima generación", espetó Guezo. Sin embargo, para Vicente Díaz, las APTs se sirven de desarrollos de software muy básicos como ataques *Zero Day* para adentrarse en la red y no considera que se estén democratizando, como señalaba Guezo. Sí coincidió con sus compañeros de mesa en la dificultad que entraña identificarlas precisamente por su persistencia: "Ésta es la palabra clave; los atacantes arremeten una y otra vez durante más de dos años hasta que logran hallar un descuido, una brecha. Para combatir las APTs , aún más importante que contar con tecnología es disponer de profesionales que la entiendan y éste es el problema real".

Después de la pausa para el café, llegó el turno para la siguiente mesa redonda de esta productiva jornada: Bajo el título "*Managing information security breaches*" se analizaron cuestiones relacionadas con la pérdida de información sensible desde diferentes perspectivas. Moderados por **Álvaro Torres**, Research & Consulting & IMP Director de IDC Research Spain; participaron los expertos **David Grout**, Director, Presales SEUR de McAfee, part of Intel Security; **Emmanuel Roeseler**, Security Systems Manager de IBM; y **Michael Hartmann**, vicepresidente de Advanced Security Solutions de Blue Coat EMEA. En primer lugar, y como acicate para el intercambio de opiniones, Álvaro Torres puso sobre la mesa tres predicciones de IDC: En 2020, el 50% de los recursos de seguridad serán y estarán en Cloud; en segundo lugar, el 20% de los recursos de seguridad se dedicará a comunicar unas cosas con otras (Internet de las Cosas); y el software de inteligencia frente a las amenazas será diez veces más eficaz que las herramientas tradicionales.

David Grout apostó por el optimismo: "Si compartimos más inteligencia va a ser más sencillo combatir las amenazas. Es el reto de la industria, que debe ayudar a las organizaciones a ser resilientes". En este sentido, Grout añadió que la orquestación durante una reacción ante un ataque es importantísima: "La estandarización es fundamental e Intel está apostando por ella, por lo que hay motivos para sentirme optimista".

Durante su intervención, Michael Hartmann puso de relieve el valor de una reacción rápida y eficaz: "Diferentes analistas hablan de semanas o incluso meses hasta que algunos ataques son detectados. La clave es reducir el tiempo de reacción si mi red ha sido comprometida y solo es posible si se cuenta con el armamento adecuado". Hartmann, ahondando en esta cuestión, recomendó reparar la vulnerabilidad antes de restaurar el sistema: "Aunque parezca obvio, no todo el mundo lo hace. Después de esto, se debe crear un plan de respuesta y monitorización".

Emmanuel Roeseler utilizó su tiempo para compartir una reflexión. El directivo de IBM entiende que la 'joya de la corona' en una empresa es la información confidencial y para protegerla todas las herramientas deben estar integradas: "Prevención, detección y respuesta deben estar constituidas como parte de un mismo equipo. Los investigadores forenses y los responsables de detección de fraude deben hablar porque defienden la misma joya". Roeseler añadió que Cloud está cambiando la seguridad y también está ayudando a responder en tiempo real antes de que se produzcan las temidas brechas.

Un año más, el Capítulo Español de Cloud Security Alliance (CSA-ES) ha presentado su estudio "*Cloud Computing Security – State of the Art analysis 2014*" con importantes novedades respecto a la primera edición. Aprovechando la celebración de esta jornada, **Mariano J. Benito,** WG Coordinator de Cloud Security Alliance Spain y CISO de GMV, anunció su disponibilidad en la web de ISMS Forum antes de dar el pistoletazo de salida al siguiente panel: "*Securing Next Generation Cloud*", compuesto por **Félix Martín**, EMEA ITI & Cloud Assurance and Security Pursuit Lead de HP; **Mark Armitage**, director de Cloud Security Products de Akamai; **Eutimio Fernández**, Security Account Manager de Cisco; y **Josep Bardallo,** Cloud & Security Business Manager de SVT Cloud.

El portavoz de Akamai, Mark Armitage, señaló que "quizá la nube es más insegura, pero el outsourcing está siendo el enfoque más extendido a la hora de afrontar una estrategia de protección ante incidentes", apostilló. Por su parte, Josep Bardallo puso el foco sobre la problemática de la seguridad en las pymes, que no disponen de un equipo de TI para combatir las amenazas: "Las pymes no están encontrando aplicaciones de seguridad en la Nube tan fácilmente como otros servicios más clásicos como el almacenamiento".

Desde el punto de vista de Cisco, Eutimio Fernández se refirió a la importancia de combatir las amenazas con una aproximación global, con una plataforma basada en nube híbrida, capaz de detectar ataques y responder con inteligencia, adelantándose a los promotores del cibercrimen. En estos casos, la información sensible permanece siempre encriptada y solamente es accesible para los usuarios autorizados. Otro gran proveedor de soluciones cloud con representación en la mesa, HP, expuso por boca de Félix Martín su parecer sobre los requisitos necesarios para securizar la Nube: "Existe una explosión de clientes y proveedores de servicios cloud, pero conviene no olvidar las preocupaciones de seguridad. En el caso de nuestros clientes se trata de conocer ofertas de IaaS

o PaaS para completar el uso de los servicios, pero también están preocupados por garantizar la seguridad de un nuevo sistema antes de que entre en fase de producción".

Después del descanso para la comida y el cultivo de las relaciones públicas, los ponentes asumieron el reto de volver a captar la atención de los asistentes, ya hasta el final de la jornada en español. Gianluca D'Antonio, presidente de ISMS Forum fue el responsable de presentar un nuevo estudio de ISMS Forum realizado en colaboración con el *think tank* Thiber: "*Incentivando la adopción de la ciberseguridad*", en el que se pone de relieve el papel de España en esta materia frente a otros países de nuestro entorno. En formato de entrevista, uno de los autores del estudio, **Manel Medina**, catedrático de la Universitat Politècnica de Catalunya y miembro del Consejo Asesor de ISMS Forum, respondió a las cuestiones planteadas por Gianluca D'Antonio.

Para el experto, los poderes públicos deben involucrarse también en la Ciberseguridad, pero impulsando un modelo de incentivos en detrimento de las tradicionales sancionas. En este texto se exponen recomendaciones para que el Estado tome nota de cómo llevarlo a cabo. En opinión de Manel Medina, la Ciberseguridad supone menos pérdidas económicas para las empresas, lo que redundaría en beneficios notables para el Estado, que –en consecuencia– podría aumentar sus ingresos vía impuestos de sociedades. Entre los incentivos más destacados, el catedrático enunció los legales/fiscales para las empresas que cumplan con los mecanismos de seguridad; el acceso a mejores condiciones de financiación; ayudas a la internacionalización, etc.

Seguidamente, llegó el tiempo para entrar de lleno en el terreno jurídico con la presentación del informe "La Responsabilidad Legal de las Empresas ante un Ciberataque", iniciativa de ISMS Forum y Enatic, que ha estado coordinado por **Carlos A. Saiz**, vicepresidente de ISMS Forum Spain y Director del Data Privacy Institute; y **Francisco Pérez Bes**, secretario general de INCIBE. Asimismo, este estudio legal ha contado con la colaboración del Consejo General de la Abogacía e INCIBE. El propio Carlos A. Saiz hizo un recorrido sobre el propósito de este trabajo, que nace con la vocación de servir de herramienta de consulta y que dará pie, sin lugar a dudas, a futuras ediciones.

Desde el punto de vista penal, Francisco Pérez Bes, reparó en la dificultad universal de adaptar los mecanismos penales a los ciberdelincuentes y destacó la necesidad de establecer una armonización jurídica internacional para una tipología de delictiva para la que no existen fronteras."Debemos ser creativos para evitar los frenos que a veces supone el sistema judicial para lograr que jueces extranjeros atiendan las peticiones de un país como España –afirmó–. Desde el punto de vista jurídico también es necesario aumentar la concienciación de la ciudadanía sobre los aspectos de seguridad".

La primera mesa redonda de la tarde giró en torno a privacidad y Big Data: "*Next Big Data- challenge to our privacy*", que estuvo moderada por el propio Carlos Alberto Sáiz. Contó con la participación de **Emilio Aced**, jefe de Área de la Agencia Española de Protección de Datos (AEPD); **Asier Crespo**, director legal para España y Portugal de Microsoft; y **Marco Bressan**, Chairman & CEO de BBVA Data & Analytcs.

El moderador trajo a colación tres titulares de noticias recientes con el objetivo de ilustrar la complejidad del desafío de la privacidad en un escenario donde se duplica el volumen de información cada año y, según los analistas, en 2020 cada uno de nosotros contará con una media

de 16 dispositivos conectados a Internet. En primer lugar, Marco Bressan vinculó el fenómeno de Big Data con la transformación digital de las empresas, que cada vez se hacen más preguntas para optimizar su negocio. El portavoz de BBVA indicó que con menos datos es posible dar respuestas al negocio y en la mayoría de las ocasiones no son precisos los datos personales para conseguirlo. "Los datos con los que tengo libertad para hacer análisis y son aquellos que no son personales", aclaró Bressan.

Cada proyecto de Big Data es diferente y Emilio Aced explicó que lo más adecuado es ir "partido a partido", pero es básico aplicar la ley si se tratan temas personales. En este sentido, el experto recomendó a las organizaciones no escabullirse, ya que no siempre tratar datos disociados (para no ser considerados como personales) indica que no haya que ceñirse a la legislación. "Las personas tienen derecho a saber qué consecuencias puede tener para ellos la utilización de sus datos en procesos de Big Data con minería de datos, ya que pueden derivar en la no concesión de un crédito o en la asignación de un perfil de cliente erróneo", argumentó Aced.

En otro orden de cosas, Asier Crespo expuso como un gran logro el reconocimiento reciente de la AEPD a los clientes de Microsoft para que puedan exportar sus tatos: "El director de la AEPD garantiza que quienes firmen un contrato con Microsoft están dotando de un nivel de seguridad adecuado los datos para su exportación", puntualizó. Para logarlo, el experto puso en valor el acercamiento previo de su compañía a la Agencia de forma proactiva.

Por otro lado, Emilio Aced anunció la disponibilidad de una nueva herramienta para realizar Evaluaciones de Impacto la Protección de Datos (EIPD). "Aunque no sea un ejercicio obligatorio, es importante como análisis de riesgos de privacidad, también para las empresas de menor tamaño", declaró Aced. Los componentes de la mesa abogaron por el derecho a la privacidad e instaron a las organizaciones a no engañarse disfrazando de datos no personales aquellos que sí lo son para su tratamiento en proyectos de Big Data.

La última mesa redonda de la jornada puso el foco en la protección de aquellas instalaciones vitales para el día a día de una sociedad. Bajo el título "*La primera línea en las Infraestructuras Críticas*", **Fernando Sánchez**, director del Centro Nacional de Protección para las Infraestructuras Críticas (CNPIC); **Joaquín Reyes**, Chief Information Officer de Cepsa; y **Eduardo Di Monte**, director de Coordinación y Continuidad de Negocio - Seguridad Corporativa en Aguas de Barcelona (Agbar), contribuyeron a una enriquecedora tertulia. **Carles Solé**, director del Spanish Cyber Security Institute (SCSI) de ISMS Forum Spain, presidió esta mesa, que se marcó el objetivo de exponer cuáles son los principales desafíos a los que se enfrentan compañías relevantes en el suministro de energía, transportes, etc. "¿Cómo están interpretando el análisis de riesgos en las Infraestructuras Críticas (IC), se aprovechan los que se tienen hechos o es necesario homogeneizarlos? ¿Se ha materializado la coordinación, va a servir de palanca la Ley de Protección de IC (LPIC)?".

A pesar de ser una de las figuras más representativas de esta disciplina en España, Fernando Sánchez declaró que a medida que se profundiza, surgen más dudas y nunca se sabe lo suficiente sobre IC. "Hay que ser prácticos para acercarse a un problema tan complejo, pero está claro que tanto las empresas como la Administración han madurado", sostuvo el directivo. Respecto a la LPIC,

Fernando Sánchez calificó que esta norma nace para marcar unas pautas y que se consideren en estos análisis de riesgos algunas cuestiones que no tenían en cuenta en sus planes tradicionales.

El portavoz de Agbar, Eduardo Di Monte, destacó que la continuidad de negocio es el hilo conductor de la normativa internacional, aunque en cada sector es diferente la adaptación que se hace de la misma. "El desafío es 'bajar' la legislación a situaciones prácticas en las plantas de agua en nuestro caso –puntualizó– para asegurar la continuidad del servicio".

El único CIO de la mesa, Joaquín Reyes, puso de manifiesto la cultura de seguridad integral como primer paso a la implementación de una estrategia de IC: "En nuestra compañía la seguridad es una prioridad; en 2003 aprobamos la norma básica de Seguridad de la Información y es el origen de la norma básica de Seguridad Integral, que engloba al resto de elementos".

Tal y como subrayó Carles Solé, un enfoque de seguridad integral supone una reorganización, que en muchas ocasiones se traduce en un comité compuesto por los directores de cada una de las áreas (Seguridad de la Información, Seguridad Física y Seguridad Industrial). Tanto en Cepsa como en Agbar se aplica este enfoque, como manifestaron sus portavoces.

Respecto a la cuestión de la coordinación entre operadores críticos y Administración, la continuidad de negocio se erige como una pieza esencial, según Fernando Sánchez, que recordó que el responsable de Seguridad y Enlace en una IC es la figura más importante. "El CERT de Seguridad Industria (CERTSI) nació precisamente para frenar incidentes en los operadores; si, además, pueden constituir un delito, entra en juego la Oficina de Coordinación Cibernética, donde se pone en contacto a los operadores críticos con las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE)", aseveró Sánchez. Ante hechos de este calibre, el director del CNPIC recordó la importancia de denunciar para que pueda arrancar la investigación pertinente.

Para concluir la jornada, la periodista Mercè Molist presentó a la audiencia "*Hackstory. La historia nunca contada del underground hacker en la Península Ibérica*", fruto de un trabajo de investigación de más de diez años que se han plasmado en un libro virtual, disponible en Hackstory.es. La autora retrata al hacker español desde sus comienzos en grupos de adolescentes que se unen con la voluntad de aprovechar sus conocimientos para compartir información. Más allá de esta visión romántica de la figura del hacker, Molist refleja la evolución y transformación de su *modus operandi* para participar en la defensa en la red de múltiples organismos nacionales e internacionales.

Patrocinadores de la Jornada

La XVI 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, Blue Coat, Cisco, Deloitte, HP, IBM, Intel Security, Symantec, SVT Cloud, Telefonica y Trend Micro.