Así se vivió la XX INTERNATIONAL INFORMATION SECURITY CONFERENCE

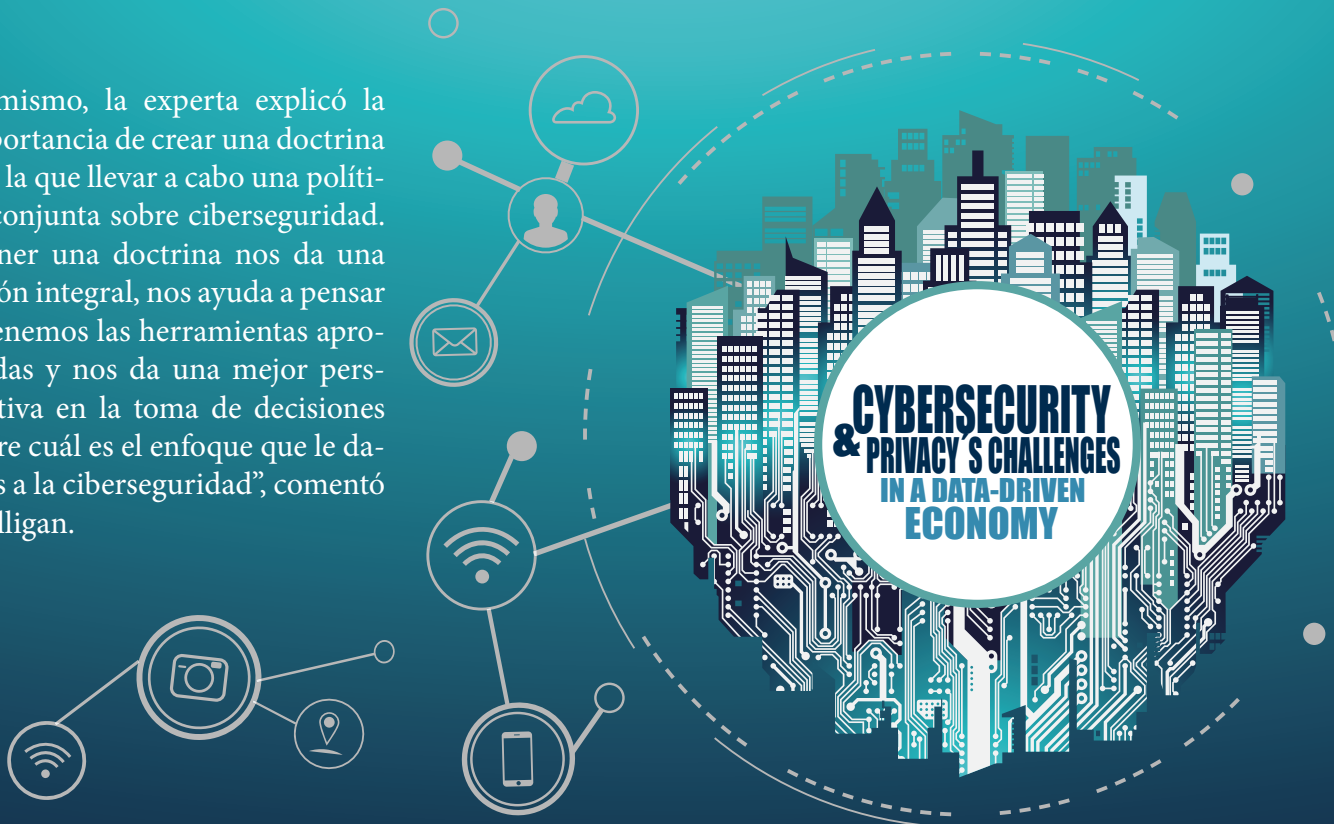
- Más de 500 profesionales de la ciberseguridad y la protección de datos se dieron cita en el mayor congreso privado nacional para profesionales del Sector, en el que participaron más de 50 ponentes de primer nivel.

- El evento contó con la presencia de expertos y representantes de empresas e instituciones internacionales de la talla del Centro Nacional de Ciberseguridad de Reino Unido (NCSC) y Comisión Europea (CE), mientras que en el plano nacional formaron parte el Instituto Nacional de Ciberseguridad (INCIBE), el Departamento de Seguridad Nacional (DSN) y el Centro Nacional para la Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC).

El pasado jueves 10 de mayo de 2018 tuvo lugar la vigésima edición de la Jornada Internacional de Seguridad de la Información de ISMS Forum Spain en el Círculo de Bellas Artes de Madrid, bajo el título "*Cybersecurity and Privacy's challenges in a data-driven economy*". "Ciberseguridad y economía, protección de datos y sociedad. Porque cada vez más experimentamos como la seguridad y la privacidad se constituyen como ejes fundamentales a todos los niveles y en todas las esferas, también en el desarrollo económico", explicaba Gianluca D'Antonio, presidente de ISMS Forum Spain, en la apertura de la jornada.

La primera ponencia que dio cuerda a este encuentro fue la de Deirdre K. Mulligan, directora del Centro de Derecho y Tecnología de la Escuela de información de la Universidad de California en Berkeley, presentando la primera Doctrina de Ciberseguridad como Bien Público. Para la investigadora, entender la ciberseguridad como un bien público significa llegar a la conclusión de que todos podemos disfrutar de ella, es decir, no es exclusiva y, además, cuando se producen avances tecnológicos en esta materia, todos podemos beneficiarnos.

Asimismo, la experta explicó la importancia de crear una doctrina con la que llevar a cabo una política conjunta sobre ciberseguridad. "Tener una doctrina nos da una visión integral, nos ayuda a pensar si tenemos las herramientas apropiadas y nos da una mejor perspectiva en la toma de decisiones sobre cuál es el enfoque que le damos a la ciberseguridad", comentó Mulligan.



Además, la directora ha querido destacar que, ante la escasa fiabilidad de los sistemas que con tanto esfuerzo intentamos sostener y el elevado coste que supone desarrollar ciberseguridad, es necesario "sacar adelante políticas que recojan los derechos individuales y llegar a acuerdos que persigan una visión común que incluya el desarrollo de estrategias de mitigación, lo que significa pensar en producir sistemas más seguros e invertir en formación y educación".

Deirdre K. Mulligan, en la XX Jornada Internacional de ISMS Forum.

Concienciar para crear una cultura de ciberseguridad

De formación y educación habló precisamente Paula Walsh, jefa del Departamento de políticas de ciberseguridad del Ministerio de Asuntos Exteriores del Gobierno de Reino Unido, mientras explicaba la perspectiva actual del gobierno británico en materia de ciberseguridad. Desde Reino Unido, han desarrollado su tercera estrategia en ciberseguridad con una inversión de 1.9 miles de millones de libras, casi el doble de lo invertido en los últimos cinco años. "Hemos constatado que cambiar la cultura en general es muy complicado, por eso hemos querido que esta nueva estrategia sea más intervencionista", aclaró Walsh.

Pero la cuestión es, ¿qué políticas se deben adoptar para mejorar esta cultura? El 24% de los negocios británicos han sufrido una o más brechas de seguridad en los últimos 12 meses y el 80% de los crímenes cometidos en Reino Unido tienen una dimensión de ciberdelitos. Eso sí, la experta asegura que la totalidad de estos ataques se podrían prevenir simplemente con implementar las mejores prácticas.

Paula Walsh, en la XX Jornada Internacional de ISMS Forum.

Una de las innovaciones más importantes que ha llevado a cabo el gobierno británico es la creación del Centro de Ciberseguridad Nacional, que ya cuenta con un año de recorrido. "No podemos impedir todos los ataques. En este sentido, tenemos que construir políticas, prácticas y tecnología para gestionar mejor los riesgos a los que nos enfrentamos. Nuestra misión es ser prósperos y tener confianza en el mundo digital".

Walsh también hizo un llamamiento a la concienciación, la educación y la responsabilidad por parte de todos, porque para tener "un ciberespacio libre, abierto, pacífico y seguro", es necesario que "todos los estados asuman su parte de culpa en ciertos ataques. Hay que hacer públicos a los culpables y hablar de ello para que no haya impunidad. Para nuestro gobierno, esto es una decisión política".

¿Demasiada autenticación?

Una ponencia que destacó especialmente fue la de Michael Kaiser, director ejecutivo de la US National Cyber Security Alliance (NCSA), bajo el título "Securing breakthrough technologies". El experto se centró en explicar en qué estamos fallando cuando hablamos de control de accesos y de la autenticación. En los últimos cinco años, ha sido uno de los pasos más importantes en la ciberseguridad y su implantación ha crecido muchísimo debido a la tecnología disponible. "Ha habido avances tecnológicos, como la biométrica, que lo hace todo mucho más sencillo. Ahora tenemos un ordenador que escanea nuestra cara y decide si podemos acceder o no a un sitio", comentó.

Michael Kaiser, en la XX Jornada Internacional de ISMS Forum.

Según el punto de vista del director, a pesar de haber avanzado mucho en este terreno, también se han cometido muchos errores. Uno de ellos es la facilidad de uso, es decir, se están utilizando autenticaciones más fuertes que a los usuarios normales les cuesta manejar. "Mismamente yo he intentado entrar en Skype para hacer una conferencia y, como hacía tiempo que no entraba, me pedía una autenticación de dos factores y he tardado 20 minutos en entrar a mi cuenta".

Esta facilidad de uso no casa con el deseo de que las personas utilicen la autenticación multifactorial cada vez más. "Si tardo 20 minutos en entrar, la próxima vez no lo voy a hacer. La gente no entiende el beneficio de la seguridad hasta el punto de decir que no le importa dedicar ese tiempo para volver a entrar a su cuenta".

El ponente también ha resaltado la importancia de crear una cultura de ciberseguridad mejorando el mensaje que se transmite a la sociedad. "La gente recibe consejo de todos lados sobre qué es lo que tiene que hacer para estar seguros y muchos de estos consejos no son buenos. La gente de seguridad es muy buena diciéndole a otros lo que tienen que hacer online pero, y no quiero ofender a nadie, no son muy buenos en la comunicación de ese mensaje".

La Ley Orgánica de Protección de Datos podría estar lista para antes de fin de año

Con el contador a cero, continúa el debate de las instituciones públicas y las entidades privadas sobre el presente y futuro de España en materia de ciberseguridad y protección de datos, ante la aplicación directa del Reglamento Europeo de Protección de Datos (GDPR, sus siglas en inglés) y una nueva Ley Orgánica de Protección de Datos (LOPD) que todavía no ve la luz.

La aplicación del Reglamento en cada Estado miembro de la Unión Europea requiere de un desarrollo normativo interno que, en el caso de España, está generando un intenso debate. "Si todo va bien, la Ley Orgánica de Protección de Datos podría estar lista para antes de fin de año. Pero hay que tener en cuenta que se trata de una ley orgánica y, por tanto, requiere de mayoría absoluta en el Congreso sobre el texto íntegro del proyecto", explicaba José Luis Piñar, exdirector de la Agencia Española de Protección de Datos. Además, añade: "Si no hay ley orgánica, tendremos en cualquier caso que aplicar el reglamento, que ya es mucho".

Habrá que esperar a su aprobación durante el segundo semestre del año o finales del mismo. Pero, mientras tanto, preocupa el impacto del GDPR y cómo afectará al sector empresarial.

En busca del talento

Alex Weishaupt, destacado investigador de tecnologías avanzadas en ciberseguridad de Korn Ferry, puso en valor la necesidad de encontrar profesionales de alto nivel en el sector que ocupen los numerosos puestos de trabajo que se están demandando hoy en día, ante el significativo aumento de las brechas de seguridad en las compañías. "Sé que muchos se preguntan por qué deberían, como empresa, invertir en una persona que forme parte de su equipo para que después se marche para trabajar con la competencia. Pero es que esto tiene que ver con crear una comunidad de ciberseguridad fuerte en la que todos nos beneficiaremos", explicó el experto.

José Luis Piñar, en la XX Jornada Internacional de ISMS Forum.

Alex Weishaupt, en la XX Jornada Internacional de ISMS Forum.

Según apuntó Weishaupt, la tasa de desempleo en este sector es del 0% y no se espera que este dato cambie durante los próximos 15 años. Además, los puestos de trabajo para los que resulta más arduo conseguir candidatos se enmarcan en áreas de ciberseguridad como la abogacía, las aseguradoras, el I+D, los proveedores, etc. Por otro lado, comenta que "el límite salarial en ciberseguridad es el cielo" porque la demanda es muy alta y "el sufrimiento de las empresas es tal que para satisfacer sus necesidades pagan lo que haya que pagar por una persona que reúna estas características".

Pero, ¿cómo capturar el talento? Para el investigador es crucial dejar de desarrollar procesos de contratación tediosos y largos porque "no funciona tener a un candidato con tres ofertas en la mesa y que tenga que pasar un proceso de selección de 17 pasos o esperar cuatro semanas a recibir una respuesta". También aconseja precaución a la hora de definir el perfil del trabajador que buscan, porque el candidato diez no existe y, una vez elegida la persona que ocupará el puesto, hay que esforzarse por crear un clima de confianza en el que se sienta importante.

Una jornada repleta de contenidos: seguridad y privacidad van de la mano

Durante esta vigésima edición, se desarrollaron dos interesantes mesas redondas en las que la línea de debate principal fue el nivel actual de resiliencia de las empresas. En la primera de ellas, 'Cybersecurity's role in the upcoming GDPR', Miguel Ángel Martos (Symantec), Jesús Vega (Imperva), Ricardo Mate (Sophos), Mario García (Checkpoint), Tony Hadzima (Palo Alto Networks), Fabiano Finamore (Forcepoint) y Rubén Frieiro (Deloitte) conversaron sobre la figura del Data Protection Officer (DPO) y qué debería tener éste en cuenta a la hora de llevar a cabo sus funciones.

Primera mesa redonda, 'Cybersecurity's role in the upcoming GDPR'.

En la segunda mesa redonda, 'Shaping the journey to the land of resilience', participaron Steve Mulhearn (Fortinet), Udo Schneider (Trend Micro), Adenike Cosgrove (Proofpoint), Josu Franco (Panda Security), Erno Doorenspleet (IBM Security), Javier J. Corrales (Prosegur Ciberseguridad) y Víctor M. Hernández (Accenture), compartiendo consejos para que las empresas aumenten su porcentaje de resiliencia a través de la elaboración de un perfil de riesgo y de informes que recojan todos los detalles posibles para tener mayores posibilidades de impedir ataques cibernéticos.

Además, se desarrollaron interesantes workshops en los que se compartieron múltiples estrategias en materia de ciberseguridad y protección de datos. Dani Creus, Analista de Malware, Global Research & Analyst Team, (GREAT) en Kaspersky Lab, se encargó de exponer los casos recientes de amenazas digitales avanzadas y su impacto en las doctrinas actuales; Federico Dios, Principal Solutions Engineer en Akamai, explicó la implicación de Akamai con los DevOps; Raúl Benito, Territory Account Manager Spain & Portugal de Qualys, centró su ponencia en la transformación digital y la forma de controlar los principales activos en la empresa; Eduard Seseras, Experto en Automatización, Seguridad y Monitorización en HelpSystems, participó comentando las principales estrategias para compartir información de forma segura para cumplir con el GDPR; y Adolfo Hernández, miembro fundador de THIBER, basó su conferencia en el cibercrimen como negocio.

También se presentaron iniciativas de valor como la Segunda Edición del Proyecto de Gestión de Ciber-Crisis, desarrollado en colaboración con el Departamento de Seguridad Nacional, el Instituto Nacional de Ciberseguridad y el Centro Nacional para la Protección de Infraestructuras Criticas y Ciberseguridad; la Cuarta Edición de la Guía de Seguridad de Áreas Críticas en Cloud Computing en colaboración con Cloud Security Alliance; la Guía Top 10 Cyber Risks, editada junto a la Asociación Española de Gerencia de Riesgos y Seguros (AGERS); y mostramos una demo de hacking asociada al laboratorio de análisis de vulnerabilidades que mantiene el Centro de Estudios en Movilidad e IoT de ISMS Forum en colaboración con la Organización de Consumidores y Usuarios (OCU), por parte de David Barroso, Miembro de la Junta Directiva de ISMS Forum y Pedro Cabrera, Miembro del equipo de Amenazas y Sensibilización del Centro de Estudios en Movilidad e Internet de las Cosas de ISMS Forum.

La XX Jornada Internacional de Seguridad de la Información ha sido posible gracias al apoyo de los siguientes patrocinadores.

PARTNERS

Platinum Sponsors

Akamai · Check Point · HUAWEI · McAfee · panda · Symantec.

Gold Sponsors

accenture · Aiuken Cybersecurity · ca technologies · Deloitte. · FORCEPOINT · FORTINET · helpsystems · IBM · IMPERVA · Infoblox · KASPERSKY · lidera · OneTrust · orange · paloalto · proofpoint · PROSEGUR · Qualys. · S21sec · SailPoint · SAMSUNG · SOPHOS · TREND MICRO