Conclusiones de la XIX Jornada Internacional de Seguridad de la Información de ISMS Forum Spain

Protecting and securing Data in the Digital Jungle

- Más de **600 profesionales** de la ciberseguridad y la protección de datos se dieron cita en el mayor congreso privado nacional para profesionales del Sector.

- Entre las instituciones presentes, la **División de Ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN)**, el **Grupo Europeo de Protección de Datos del Artículo 29**, y el **Supervisor Europeo de Protección de Datos**; mientras que en el plano nacional participaron el **Instituto Nacional de Ciberseguridad**, el **Centro Nacional para la Protección de Infraestructuras Criticas**, el **Instituto Nacional de Ciberseguridad** (INCIBE) el **Departamento de Seguridad Nacional**, el **Centro Criptológico Nacional** y la **Agencia Española de Protección de Datos**.

ISMS Forum reunió el pasado **11 de mayo** a **más de 600 profesionales** de la seguridad de la información y la protección de datos en la decimonovena edición de la **Jornada Internacional de Seguridad de la Información** celebrada en el Círculo de Bellas Artes de Madrid.

Bajo el título "***Protecting and securing the Data in the Digital Jungle***", durante toda la jornada se sucedieron hasta 60 ponencias y debates con la presencia de reconocidos expertos y autoridades, nacionales e internacionales, que nos ayudaron a entender mejor las claves para afrontar con éxito la Transformación Digital. Como principales temas, se abordaron l**os riesgos y amenazas que presenta la automatización y la digitalización de procesos** en el entorno corporativo, y el papel de **la ciberseguridad como eje fundamental y garantía de la transformación digital** en empresas y en la sociedad en general.

La bienvenida de **Enrique Sánchez De León**, director general de la Asociación para el Progreso de los Directivos, junto a **Gianluca D'Antonio**, presidente de ISMS Forum, dio el pistoletazo de salida al congreso con la representación y asistencia de un colectivo cada vez más sensibilizado con la ciberseguridad.

En la ponencia inaugural, **Bruce Schneier**, apodado **"Gurú de la Seguridad"** por *The Economist*, e internacionalmente reconocido como experto en ciberseguridad, habló del futuro "inseguro" de los dispositivos conectados (IoT). Schneier, explicó los problemas de confidencialidad derivados de los IoTs y la manera en que afecta a nuestro día a día, dejándonos vulnerables a todo tipo de ataques. Según Bruce, el problema radica en que la Industria funciona en torno a las premisas FAST (rápido), CHEAP (barato) y EASY (fácil) como forma de responder a la demanda el mercado, pero deja a un lado la seguridad desde el diseño y por defecto.

A lo largo de la mañana diferentes ponentes se dieron cita *como* **Andy Purdy**, CSO de Huawei USA. Purdy, manifestó durante su ponencia que "las amenazas existentes en el ciberespacio requieren que los líderes de la Administración y del sector privado deben tener un firme compromiso para abordar los riesgos de seguridad y privacidad cibernéticos de una manera comprensiva y confiable, para lo que deben utilizar mecanismos de gestión de riesgos y estándares internacionales y mejores prácticas. Cooperaciones concretas como la establecida en España entre Huawei e INCIBE son necesarias para impulsar la ciberseguridad.

Óscar Serrano, desde OTAN, expuso en su intervención los esfuerzos que están llevando a cabo en torno a la compartición de información e indicadores de compromiso como forma de generar alertas tempranas y, en última instancia, el refuerzo de ciber-inteligencia frente a las amenazas para que mejoren las capacidades de analizar y prevenir, identificar, localizar y atribuir ataques o amenazas.

Resultó destacable la intervención de **Isabelle Falque – Pierrotin,** presidenta del CNIL y del Artículo 29 con su ponencia *"Privacy shield & GDPR in the new international context***"**, en la que nos habló de la gran labor que hacen desde WP29 y los cambios que se avecinan en los próximos meses debido al nuevo Reglamento Europeo de Protección de Datos, afirmando que será severo y debemos estar preparados para afrontarlo.

Otra de las ponencias individuales vino de la mano de **Michael Shaulov**, CheckPoint, titulada *"The spy in your pocket*" donde nos explicó los riesgos desconocidos a los que estamos expuestos únicamente por llevar el smartphone conectado a las diferentes apps en nuestro bolsillo. "Es necesario protegerlos, tanto los de propiedad corporativa como los BYOD, con una solución integral que bloquee ataques de malware y de red, y evite la fuga de datos y el robo de credenciales. Todo esto debe hacerse sin que afecte a la experiencia del usuario." Afirma Michael Shaulov.

José Selvi, Senior Security Research at Global Research & Analysis Team de Karspersky, nos mostró la importancia de poder localizar las APTs con anterioridad al ataque para poder neutralizarlas antes de que ocasionen cualquier problema. Por parte de **Peter Maier-Borst**, CEO de Virtual Forge Iberia abordó cinco propuestas para lograr hackear SAP y por lo tanto poder entender cómo podemos evitar y atajar estos ataques.

Porteriormente, **Javier Guerra**, System Engineer de Cloudfare, y **Maurizio Monti**, Costumer and Partner Development Manager for EMEA de Cloudflare, explicaron la evolución de los ataques DDoS y las implicaciones para las empresas, advirtiendo la importancia de soluciones seguras en cloud que prevengan la sobrecarga de los servidores.
Posteriormente, la mesa redonda "*CISO´s vs. CISO´s views on cybersecurity and Data Protection*" presidida por Gianluca D´Antonio e integrada por Eduardo Di Monte, CISO de AGBAR; Francisco Lázaro, CISO de Renfe; Cristina Alvarez, CIO de Telefónica; y Paloma Peinado, CIO de AIRBUS, aportó los diferentes puntos de vista para CIOs y CISOs en ciberseguridad y protección de datos. Como conclusión, los panelistas determinaron que la clave está en que el

CIO y el CISO no tengan dependencia para agilizar todas las gestiones relacionadas con cualquier unidad de negocio.

Asimismo, se desarrollaron interesantes debates que conectaron a los primeros niveles de los principales proveedores de seguridad en torno a la manera de hacer frente a una brecha de seguridad en la nueva ERA digital, la protección del dato en la Nube y la gestión de identidades, o la generación de ciber inteligencia a partir del análisis de ciberamenazas.

También hubo espacio para los workshops y hacking, en donde el equipo de Amenazas y Sensibilización del Centro de Estudios en Movilidad e Internet de las Cosas de ISMS Forum demostró la facilidad con la que la seguridad de los dispositivos conectados como un móvil, una cámara de seguridad o una alarma del hogar, puede ser violada y caer bajo el control del hacker.

La sesión de tarde comenzó con la intervención de otro de los ponentes más destacados, **Giovanni Buttarelli**, Supervisor Europeo de Protección de Datos. En su discurso abordó los retos del nuevo marco normativo europeo para la protección de datos. Buttarelli se declaró partidario de una legislación muy restrictiva que garantice la privacidad y la protección de datos, y recomendó no esperar a que entre en vigor la nueva normativa para estar preparados.

Para terminar la jornada, hubo una mesa redonda titulada "*Data Breach Notification y su impacto en el negocio*" moderada por Carlos A Saiz e integrada por representantes de CaixaBank, la Agencia Española de Protección de Datos, y Técnicas Reunidas. En ella dieron cuenta de la necesidad de notificar una brecha de seguridad en las siguientes 72 horas de haberse puesto de manifiesto, y el tiempo medio de reacción.

Proyectos y actividades de ISMS Forum

En el marco de la Jornada, la Agencia Española de Protección de Datos junto con ISMS Forum presentaron el **Código de Buenas Prácticas en Protección de Datos para proyectos de Big Data**. Mar España, Directora de la AGPD, junto Carlos A Saiz, Vicepresidente de ISMS Forum Spain y Director del Data Privacy Institute, fueron los encargados de presentar esta guía elaborada por profesionales especialmente implicados en esta área y define los principios para que legitimen los datos en su tratamiento para Big Data.

Mar España, en su intervención, afirmó que cuando hay un mayor volumen de datos, es evidente que existe un mayor riesgo y, por tanto, un mayor esfuerzo para los responsables de la protección de datos que velan por la anonimización de los datos. Tanto el sector privado como el público deben estar preparados para la implementación de la regulación del año que viene. Es mucho mayor el daño reputacional que una brecha de seguridad puede hacer a una empresa que la multa económica que puedan tener. "

En palabras de Carlos A Saiz, utilizar grandes cantidades de información no es un problema en sí mismo, pero hay que utilizarlo de la manera correcta y aportando las garantías necesarias para una correcta protección de los datos de las personas interesadas. "Queremos que sea un punto de partida de referencia práctica para las empresas, con un primer bloque que incluye el

régimen jurídico aplicable y cuestiones clave como la definición del responsable del tratamiento de los datos y el encargado", afirmó Carlos A. Sáiz.

ISMS Forum presentó durante la jornada el proyecto de Compartición de indicadores de compromiso (IOC´s, en sus siglas en inglés) como forma de industrializar la defensa frente a ataques, de modo que, si una empresa recibe un ciberataque de cualquier índole, el resto de empresas obtendrán anónimamente esa información para protegerse y estar alerta y preparados para ello.

Asimismo, se presentó el proyecto de gestión de crisis cibernéticas, un simulacro gamificado en el que participaron multitud de empresas y cuya finalidad es generar concienciación sobre los riesgos existentes a todos los niveles, reforzar la comunicación y la coordinación (interna y externa) y, en definitiva, entrenar a las empresas en la gestión de ciber-crisis.

La XIX Jornada Internacional de Seguridad de la Información ha sido posible gracias a la colaboración institucional del Departamento de Seguridad Nacional, el Instituto Nacional de Ciberseguridad, el Centro Nacional de Protección de las Infraestructuras Críticas, el Centro Criptológico Nacional y la Embajada Británica. Gracias también al apoyo de los patrocinadores: Akamai, CA Technologies, Check Point, Cloudflare, Deloitte, Forcepoint, Fortinet, HPE, Huawei, IBM, Kaspersky, McAfee, OneTrust, Panda Security, Proofpoint, Prosegur, Sailpoint, Symantec, Trend Micro y Virtual Forge.