CRÓNICA

XXII Jornada Internacional de Seguridad de la Información

La Estrategia Digital a debate: "Cuando nos atacan no podemos emplear nuestro tiempo en discutir si pagamos o no pagamos el rescate"

3 de diciembre de 2020. ISMS Forum celebró su **XXII Jornada Internacional de Seguridad de la Información** el pasado 26 de noviembre en modalidad online. Este año, el congreso privado nacional de referencia para los sectores de la ciberseguridad y la protección de datos, adoptó el título ***Shaping a sustainable & disruptive Digital Risk Strategy***, haciendo referencia a la necesidad de crear una verdadera estrategia digital que permita generar la estabilidad que el negocio necesita.

Fueron más de **800 profesionales** los que se reunieron en torno a cuatro Tracks con más de **30 ponencias**, y con la presencia de más de **70 ponentes** de primer nivel que compartieron las claves para afrontar los nuevos escenarios que se presentan desde el punto de vista de la *Cybersecurity Strategy* en el Track 1, liderado por **Daniel Largacha**, Director del Cyber Security Centre (CSC) de ISMS Forum; *Data Protection* en el Track 2, con **Carlos A. Saiz**, Vicepresidente de ISMS Forum y Director del Data Privacy Institute, como moderador; y el Track 3, *Cybersecurity Trends*, de la mano de **Gianluca D'Antonio**, presidente de ISMS Forum.

La Jornada contó con la presencia de representantes de instituciones internacionales de la talla del World Economic Forum, el Cambridge Cybercrime Centre, la Comisión Europea, la European Data Protection Board, la European Defence Agency, y el European Data Protection Supervisor.

La Sostenibilidad como eje central de la ciberseguridad

La primera ponencia que dio cuerda a este encuentro fue la de **Troels Oerting**, Chairman of the Advisory Board, Centre for Cybersecurity, World Economic Forum, que abordó la importancia del concepto de Sostenibilidad en el ámbito de la Ciberseguridad como piedra angular de la Estrategia Digital.

"Los ciberdelincuentes observan tres parámetros cuando deciden si quieren cometer un delito, cuál es la inversión, cuál es el riesgo y cuál es el beneficio, y en el ciberdelito tienes una inversión relativamente baja, un beneficio enorme y casi no tienes riesgo, así que, ¿por qué no continuar realizando ciberdelitos?", comentó el experto al inicio de su ponencia.

"He visto muchas pequeñas brechas que se han convertido en una gran crisis para una empresa porque se trataron mal desde el punto de vista comunicacional. Es necesario pensar en la resistencia antes, durante y después, se trata de predecir lo que va a pasar para poder prevenir y proteger nuestro estado. Por ello, es importante contar con un plan que nos guíe cuando sucede un incidente de seguridad. La clave es saber cuándo sucede, cómo lo detectas y cómo reaccionas, para poder aplicar el plan. Cuando nos atacan no emplear nuestro tiempo en discutir si pagamos o no pagamos el rescate, tenemos que contar con una política empresarial, tanto si lo hacemos como si no, y saber de qué depende. Asimismo, debemos tener muy claro quiénes son los que formarán parte de nuestro equipo de gestión de crisis, quién se comunicará con la

prensa, los accionistas o los clientes, para asegurarnos de que podemos centrarnos en el problema principal sin tener que estar pendientes de otros problemas añadidos. Por eso debemos tener un plan de resiliencia para el antes, durante y después", declaró Troels sobre cuáles son los puntos a tener en cuenta a la hora de elaborar una Estrategia Digital.

El ponente concluyó su charla haciendo referencia a los nuevos ataques a los que nos enfrentaremos tras el paso de la COVID-19, "la pandemia también ha tomado a los cibercriminales por sorpresa, ahora se están preparando para la nueva normalidad y aún no hemos visto el resultado de eso. En el futuro podremos ver nuevos tipos de cibercrimen que aprovecharán la superficie de ataque que hemos creado después de la COVID-19 y tendremos que lidiar con eso, aunque también estoy seguro de que estamos mejorando y la ciberseguridad está pasando a ser una parte muy importante dentro de cada empresa".

Troels Oerting (World Economic Forum)

En línea con el concepto de Sostenibilidad en el ámbito de la Ciberseguridad que desarrolló Troels Oerting, la **Dr. Maria Bada**, Senior Research Associate at Cambridge Cybercrime Centre, dedicó su intervención a hablar sobre el nivel de madurez en ciberseguridad como la clave para la sostenibilidad de la empresa.

La ponente se centró en el valor de los Key Performance Indicator (KPIs) para la mejora de la eficacia y productividad de las acciones que se lleven a cabo en un negocio con el fin de poder tomar decisiones y determinar aquellas que han sido más efectivas a la hora de cumplir con los objetivos marcados en un proceso o proyecto concreto.

"Los indicadores clave de negocio nos ayudan a controlar o mitigar el impacto utilizando un enfoque de gestión de riesgos centrado en priorizar las situaciones con esta métrica de riesgo e indicar las medidas que deben adoptarse y, a continuación, sobre la base de los riesgos identificados, medir la eficacia de estos controles. Los KPIs muestran la historia de éxito o fracaso de la organización a la hora de tomar decisiones eficaces. El reto es saber identificar los criterios que son más aplicables a nuestra organización, ya sea una gran corporación o una pyme".

Asimismo, la experta recalcó la importancia de la formación y concienciación en la empresa, "los CEOs y directores deben tener una formación básica en seguridad y capacidad de resiliencia de la empresa, ya que tienen que ser capaces de comprender las amenazas que les acechan. Una forma de implicar al personal de la empresa en seguridad es a través de campañas de sensibilización que les permitan ver cuáles son los riesgos a los que están expuestos y sus limitaciones".

Perspectiva europea: el tratamiento de los datos y las transferencias internacionales de datos

En clave de privacidad, una de nuestras ponentes destacadas fue **Karolina Mojzesowicz**, Deputy Head of the Data Protection Unit, Directorate General for Justice and Consumers, European Commission, que habló sobre la transformación digital y la estrategia de datos europea.

"La comisión está trabajando muy intensamente en diferentes medios para abordar el programa y las herramientas necesarias que faciliten el intercambio de datos a través de la Unión Europea y entre diferentes sectores con el fin de crear riqueza y aumentar el control y la confianza tanto de los ciudadanos como de las empresas cuando compartan sus datos, así como para ofrecer nuestro modelo europeo a las prácticas de manejo de datos de las principales plataformas. Así pues, ¿qué aborda esta gobernanza de los datos? El reglamento se refiere a un conjunto de reglas y medios para utilizar los datos, por ejemplo, a través de mecanismos de intercambio, acuerdos y normas técnicas, cada uno de los cuales implica estructuras y procesos para compartir los datos de manera segura, incluso a través de terceros", explicó Karolina.

El objetivo del Reglamento es crear las condiciones adecuadas para que las personas y las empresas confíen en que sus datos serán manejados por organizaciones de confianza basadas en los valores y principios por los que apuesta la Comisión Europea, "la Comisión tiene previsto invertir 2.000 millones de dólares en el desarrollo de la arquitectura de los instrumentos, de las infraestructuras de procesamiento de datos y el mecanismo de intercambio de datos a través de los espacios de datos seguros", comentó la experta.

Por su parte, **Ventsislav Karadjov**, Deputy Chair, European Data Protection Board, expuso el punto de vista europeo de la privacidad desde el diseño y por defecto. "La European Data Protection Board elaboró en 2019 unas directrices que proporcionan orientación sobre la obligación establecida en el artículo 25 del Reglamento General de Protección de Datos. Estas directrices se han ultimado recientemente tras una consulta pública con las partes interesadas con el objetivo de desarrollar los conceptos de la privacidad desde el diseño y por defecto y marcar una orientación muy práctica para que el responsable del tratamiento pueda comprometerse a respetar la privacidad. Esto no solo ayuda a todos los responsables del tratamiento, sino que también sirve de guía para que las pequeñas y medianas empresas apliquen los requisitos en la práctica", declaró el experto.

Según Karadjov, "el Reglamento General de Protección de Datos es tecnológicamente neutro y no especifica ninguna medida para cumplir los requisitos de protección de datos desde el diseño y por defecto, por lo tanto, el controlador puede elegir las medidas más adecuadas según las circunstancias. Debe analizar, tomar medidas y rendir cuentas de esas medidas, por lo tanto ¿deberíamos conseguir que los fabricantes y los proveedores de software considerasen la

protección de datos y la seguridad en la fase de diseño?, y ¿cómo sería esto posible? (…) la protección de datos debe considerarse en una fase temprana y no puede ser solo una comprobación formal de última hora antes de iniciar el proceso de incorporación, por el contrario, tiene que ser parte integrante de todos los debates al desarrollar cualquier nuevo producto o servicio en todas las etapas del diseño, de las actividades de procesamiento, incluidas las licitaciones de adquisición, la contratación externa, el apoyo al desarrollo, el mantenimiento, las pruebas de almacenamiento, etc.".

El ponente dedicó la última parte de su intervención a hablar sobre los procesos de certificación, "es importante saber que la certificación es alentada por el RGPD, no es obligatoria, pero proporciona y agrega un valor añadido a un controlador en el momento de elegir entre diferentes bienes y servicios, ya que le sirve para demostrar que la protección de datos está incorporada en el ciclo de vida de su solución de procesamiento".

Ventsislav Karadjov (European Data Protection Board)

En esta dinámica, **Leonardo Cervera**, Director del European Data Protection Supervisor, abordó cómo el Reglamento General de Protección de Datos contempla las transferencias internacionales de datos. Para ello, puso de ejemplo la reciente sentencia Schrems II, por la que se invalida el Escudo de Privacidad, dejando de ser un mecanismo aplicable de manera inmediata desde la publicación de la sentencia, para ofrecer garantías adecuadas en el caso de transferencias internacionales a empresas estadounidenses adheridas a este.

"El Escudo de Privacidad no garantiza un nivel de protección equivalente" declaró el experto, "debemos atender a un principio de responsabilidad proactiva, basado en catalogar las transferencias, revisar las herramientas, analizar el país tercero, identificar las salvaguardias adicionales y proceder a la suspensión de las transferencias si lo vemos conveniente" añadió.

Según Leonardo, "hay un antes y un después de la sentencia Schrems II, el problema sigue estando fuera de la Unión Europea y hay que tratar de relanzar la relación transatlántica, pero

teniendo en cuenta que la responsabilidad es compartida, de los responsables de tratamiento y autoridades de control".

ISMS Forum lanza la Guía práctica para la gestión de riesgos de terceros en privacidad

La XXII Jornada Internacional de Seguridad de la Información sirvió como marco de referencia para el lanzamiento de uno de los últimos proyectos llevados a cabo por la Asociación, la **Guía práctica para la Gestión de Riesgos de Terceros en Privacidad**. **Alfonso J. Menchén**, Delegado de Protección de Datos en Iberdrola España, fue el encargado de presentar la Guía y los motivos por los cuáles se decidió desarrollar el proyecto.

El objeto de la Guía es establecer unas pautas generales, recomendaciones o buenas prácticas que permitan a las empresas concretar e implementar el principio general de la diligencia debida, especialmente a la hora de elegir a sus proveedores. Tras definir las obligaciones legales existentes, el documento aborda cuáles son las buenas prácticas según la fase en la que vaya teniendo intervención el proveedor: fase precontractual, fase contractual y fase de terminación de la relación contractual.

Otra de las ponentes destacadas de este encuentro fue **Maite Boyero**, miembro del Centro de desarrollo tecnológico industrial (CDTI) y principal enlace para el programa de Sociedades Seguras, integrado en el Programa Marco de la Unión Europea – Horizonte 2020, como representante de los intereses de España en dicho Comité, que participó con una ponencia bajo el título "La innovación y la ciberseguridad como capacidades de una Europa Digital".

"La Comisión está empezando a poner en marcha el desarrollo de la investigación y la innovación para el período 2021-2027, será el próximo Programa Marco Horizonte Europa, el 9º Programa Marco para la investigación y la innovación en la Unión Europea cuyo objetivo es fortalecer el uso de la base científica y tecnológica en el área de investigación europea para impulsar la capacidad de innovación de Europa, la competitividad y el empleo, así como cumplir con las

prioridades de los ciudadanos y mantener nuestros modelos y valores económicos y sociales", expuso la experta.

"Nuestros principales desafíos y aspectos clave se centran en mejorar la ciberseguridad en la transformación digital asegurando la autonomía estratégica en las herramientas tecnológicas de la ciberseguridad, así como las innovaciones en el desarrollo e implementación de hardware y software seguro, pruebas y certificación, prestando atención a la privacidad y seguridad desde el diseño en las tecnologías digitales y sus aplicaciones (5G, industria 4.0, IO, Blockchain, tecnologías cuánticas, dispositivos móviles y connectec movilidad y energía cooperativa y autónoma)", comentó Maite en relación a los objetivos perseguidos por el próximo Programa Marco de la Unión Europea.

"La pandemia de COVID-19 ha puesto de relieve la necesidad de soluciones fiables y escalables"

Esta Jornada contó por primera vez con la presencia de **Mario Beccia**, Cyber Defence Officer, European Defence Agency (EDA), que abordó la temática de Ciberseguridad Transnacional. "El programa de defensa cibernética de la EDA incluye proyectos para hacer frente a desafíos como la conciencia de la situación cibernética, la protección avanzada contra amenazas persistentes, la ingeniería de sistemas para la defensa cibernética, la conciencia de la seguridad cibernética, el diseño de cursos de capacitación en defensa cibernética y muchos otros. La pandemia de COVID-19 ha puesto de relieve la necesidad de soluciones fiables y escalables que proporcionen comunicaciones fiables, ubicuas y seguras", declaró Beccia.

Asimismo, presentó el proyecto PESCO para la ciberdefensa, cuyo objetivo es desarrollar, establecer y poner en funcionamiento el Cyber and Information Domain (CID) Coordination Center (CIDCC) como elemento militar multinacional permanente, en el que -de conformidad con la resolución europea de 13 de junio de 2018 sobre la ciberdefensa- los Estados miembros participantes colaboren continuamente con personal nacional pero decidan soberanamente, caso por caso, para qué amenaza, incidente y operación contribuyen con medios o información.

Mario Beccia (European Defence Agency)

CRÓNICA

Sin duda, la **XXII Jornada Internacional de Seguridad de la Información** fue la cita ineludible de profesionales, expertos, compañías e instituciones públicas para debatir sobre el presente y el futuro que supone la Transformación Digital, la mejora constante de una Estrategia Digital que permita enfrentar los riesgos eficazmente y el tratamiento de los datos a nivel nacional e internacional, entre otros temas desarrollados.

Este encuentro no hubiese sido posible sin el apoyo de nuestros Platinum Sponsors Akamai Technologies, Huawei, IBM, OneTrust, Proofpoint, Recorded Future, RiskRecon, Sophos, VMware, Zscaler, y nuestros Gold Sponsors Aiuken Cybersecurity, BeyondTrust, BitSight, Cipher, Cloudflare, CrowdStrike, Darktrace, Deloitte, Fortinet, Forcepoint, Forescout, ForgeRock, S21sec, Aruba, Netskope, NextVision, Okta, Palo Alto Networks, Cytomic, Qualys, Radware, Retarus, HelpSystems, Thycotic y Trend Micro, ya que ha sido fundamental para que esta XXII Jornada Internacional de Seguridad de la Información pueda celebrarse.

Sobre ISMS Forum

ISMS Forum -International Information Security Community- es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. ISMS Forum cuenta con más de 250 empresas asociadas y más de 1.250 profesionales asociados. La Asociación es ya, por tanto, la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.

Contacto

Raquel García – Responsable de Comunicación Externa y Relaciones Públicas

rgarcia@ismsforum.es

Twitter: @ISMSForum

LinkedIn: ISMS Forum

Teléfono: +34 600 87 19 69