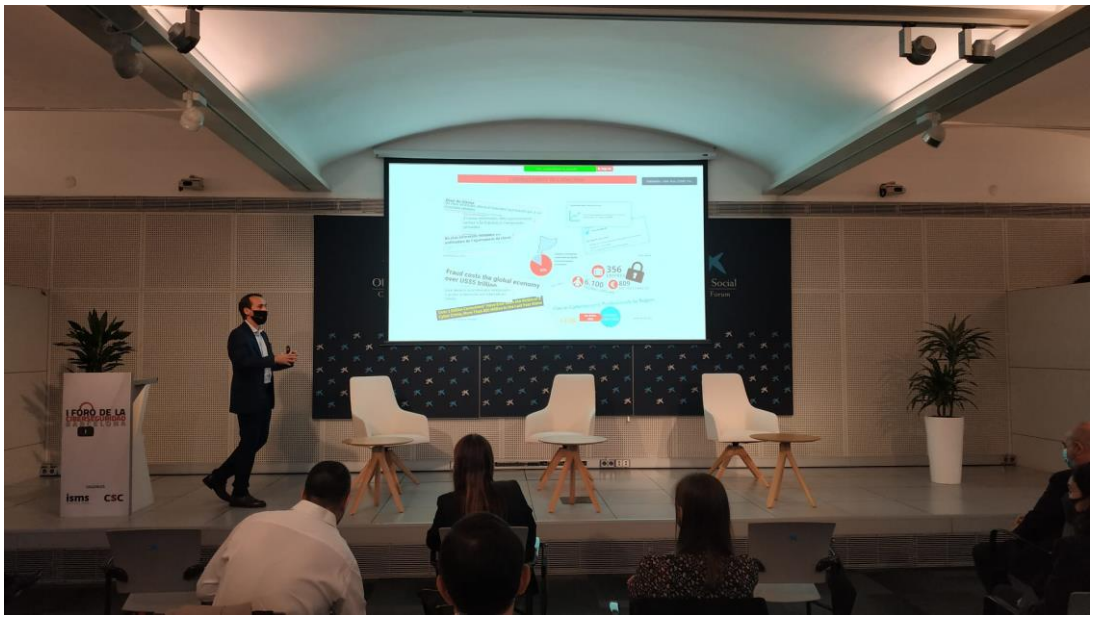
I Foro de la Ciberseguridad de Barcelona

“Nuestro objetivo es que los ciudadanos, las empresas y las instituciones de Cataluña tengan un servicio público de ciberseguridad”

ISMS Forum, junto con el Capítulo de ISMS Forum Barcelona, celebró el I Foro de la Ciberseguridad de Barcelona el pasado miércoles 7 de octubre de 2020, donde se reunieron de forma online más de 150 profesionales del sector.

Toni García, Steering Committee and board member, ISMS Forum Cataluña Chapter, fue el encargado de inaugurar el acto y dar paso a la ponencia que inició el encuentro, impartida por **Oriol Torruella**, Director de la Agència de Ciberseguretat de Catalunya.



Oriol Torruella en el I Foro de la Ciberseguridad de Barcelona.

“Me gustaría agradecer a ISMS Forum el darnos la oportunidad de venir a explicar cuáles son las próximas líneas de acción que está desarrollando la Agència de Ciberseguretat de Catalunya, así como acompañaros en estos actos aportando y compartiendo nuestro conocimiento”, comenzó Oriol. “Hoy en día la ciberseguridad no es solo un elemento técnico o de discusión para determinados perfiles de gente que no tiene nada que ver con el negocio, la sociedad o la actividad de las empresas, sino que es un ámbito que aborda todo el espectro de nuestras vidas. Llevamos un año desarrollando nuestra estrategia de ciberseguridad, en la que pretendemos contar con un modelo de ciberseguridad para la sociedad catalana que les permita abordar todos los retos que van surgiendo en esta materia” añadió.

"Nuestro objetivo es que los ciudadanos, las empresas y las instituciones de Cataluña tengan un servicio público de ciberseguridad de calidad. La Agència de Ciberseguretat de Catalunya apuesta por una estrategia y un servicio público de ciberseguridad diseñado, dirigido y gestionado con la misión desarrollar y desplegar todos los Servicios Públicos de Ciberseguridad. De esta manera, colaboramos con el Gobierno para elaborar planes de ciberseguridad y ejecutarlos. Asimismo, es importante resaltar la gestión de las campañas de capacitación, formación y sensibilización, y promover un entorno de confianza y ciberseguridad para contribuir al desarrollo de la economía y la sociedad digital en Cataluña", comentó el experto.

La siguiente ponencia **"Data driven third-party risk management"** vino de la mano de **Vicente de la Morena**, Country Leader en RiskRecon, que presentó un estudio llevado a cabo por la compañía en el que valoraba la gestión de terceros. "Como podemos ver, en la mayoría de los casos hay solo una persona que participa en la gestión de proveedores", comentó Vicente. El estudio se basa en las respuestas de una muestra significativa de empresas en función de la relación con sus proveedores.

Por otro lado, **Richard Meeus**, Director of Security Technology and Strategy EMEA en Akamai Technologies, habló sobre los ataques DDoS, en los que un grupo de sistemas comprometidos atacan a un solo objetivo para causar una denegación de servicios a los usuarios que sí son legítimos. Según el experto, un 85% de estos ataques son premitigados, sin embargo, hay que contar con la seguridad pertinente para detectarlos.

Toni García, Grupo DAMM y Board member de ISMS Forum, **Santiago Minguito**, Board member de ISMS Forum Barcelona, y **Óscar Sánchez**, Board member de ISMS Forum Barcelona, abordaron las conclusiones sobre **el "Estudio sobre el nivel de madurez en ciberseguridad"** realizado por el Observatorio de Ciberseguridad.

De izquierda a derecha, Toni García, Santiago Minguito y Óscar Sánchez.

“El objetivo de este estudio es analizar el nivel de madurez, evolución y nuevos fenómenos en el ámbito de la seguridad de la información, así como generar indicadores nacionales sobre el estado de la ciberseguridad en empresas y entidades privadas y públicas. El “Estudio sobre el nivel de madurez en ciberseguridad” se presenta como un divulgador de conocimiento e investigación a través de la creación de métricas y referencias nacionales, y la interlocución con instituciones y reguladores”, comentó Toni García.

"Más del 60% de las empresas cuentan con una política donde se definen los roles y responsabilidades, junto con los requerimientos legales y regulatorios, dentro del marco de los procesos de gobierno y gestión del riesgo de ciberseguridad. Cerca del 50% de las empresas identifican y comunican las dependencias y los requisitos de los servicios y funciones críticas, asociadas a la misión, visión y objetivos de la organización. Sin embargo, el inventario de dispositivos, sistemas, aplicaciones y recursos de información solo es completo en un tercio de la muestra", comentó Santiago Minguito. El documento recoge que hasta un 50% de las empresas mantienen identificadas y documentadas las vulnerabilidades y amenazas de ciberseguridad, analizando el riesgo en base a la probabilidad e impacto en el negocio, pero solo el 30% de la muestra manifiesta que los procesos de gestión del riesgo, así como el nivel de tolerancia, están establecidos, acordados e informados con las partes interesadas. En relación a los procesos de gestión del riesgo de la cadena de subministro, predomina (40%) la existencia de un proceso de gestión del riesgo de terceros y el establecimiento de las medidas en los contratos, pero no se auditan.

En cuanto a la protección de los sistemas y activos de información, más del 40% de las empresas manifiesta documentar los procesos y procedimientos, y más del 50% identifican los datos, pero los protegen de manera parcial. Casi la mitad de las empresas encuestadas manifiesta la existencia de una gestión de identidades y accesos en base al principio de menor privilegio y segregación de funciones, sin embargo, en la gestión del cambio, si bien la mitad de los encuestados afirma la realización de un mantenimiento de los sistemas de información de forma controlada, los accesos no se auditan.

Por otro lado, en referencia al dominio de Respuesta, Óscar Sánchez comentó cómo “en el 50% de las entidades, los procedimientos de respuesta ante incidentes de ciberseguridad están documentados, actualizados y se prueban con carácter anual. La opción mayoritaria muestra que los principales procesos, roles e interlocutores en la comunicación de respuesta ante incidentes están identificados, y el grueso de empresas participantes investiga las alertas más relevantes generadas por los sistemas de detección de acuerdo a un proceso definido, pero sin SLAs formalizados”. En referencia a la identificación temprana de vulnerabilidades y amenazas, la mitad de la muestra la realiza mediante procesos automáticos y solo un 8% revisa los planes de respuesta ante incidentes más de una vez al año y hasta un 36% lo hace únicamente ad hoc.

La siguiente ponencia titulada **"Cyber security & privacy challenges of emerging technologies"** fue la de **Abhik Chaudhuri**, Tata Consultancy Services, en la que el experto habló sobre los nuevos retos que presenta la era de las tecnologías digitales a través de conceptos como "Trustworthiness", que consiste en la fiabilidad o grado en que el sistema funciona como se espera frente a las perturbaciones ambientales, la pérdida de calidad y precisión del funcionamiento, los errores humanos, los fallos del sistema y los ataques.

La mesa redonda **"Security challenges for the enterprise of things"** estuvo compuesta por **Iker del Fresno** Director Comercial en Aruba, **Carlos Gándara**, Senior B2B Sales Manager en Samsung, **Tristan Reed**, International Presales Coordinator en Cytomic, y como moderador **Antonio Fontiveros**, Responsable de Ciberseguridad, Autopistas, y Miembro del board de ISMS Forum Cataluña Chapter. La temática giró en torno a seguridad en un escenario de teletrabajo y los riesgos que conllevan los dispositivos personales (WiFi del hogar, ordenador familiar, teléfono particular…). Asimismo, se debatió sobre cómo afrontar los retos de seguridad en los dispositivos IoT de entornos empresariales que no cuentan con una seguridad por defecto incorporada.

De izquierda a derecha, Alberto Francoso, Carlos Gándara y Tristan Reed.

Alberto Francoso, Jefe de Análisis del Servicio de Ciberseguridad de OCC y **Alejandro Villar**, Miembro de ISMS Forum y Coordinador de la Guía para la Gestión de vulnerabilidades en entornos OT, fueron los encargados de presentar la nueva **Guía para la Gestión de vulnerabilidades en entornos OT**. Esta Guía tiene el objetivo de identificar las carencias de seguridad en los sistemas de operación en producción y la definición de las medidas compensatorias tasadas que podrían subsanar dichas carencias, ya sean de carácter técnico, organizativo o procedimental. Se trata de ayudar a los responsables de

seguridad de los sistemas a desempeñar su función con garantías, así como evitar la indefinición en los procesos de consultoría y de auditoría.

El encargado de poner el broche final al I Foro de la Ciberseguridad de Barcelona fue **Adolfo Hernández**, Co-founder member de THIBER con su ponencia **"Evolución de las amenazas en entornos industriales"**, donde expuso varios casos prácticos para ilustrar los diferentes tipos de riesgo, tales como los producidos por sistemas inseguros by-default (redes planas, autenticación débil, sin cifrado, protocolos inseguros, parcheo difícil, errores de configuración de dispositivos), vectores de amenazas activos (cibercriminales con ataques dirigidos y no dirigidos, foros donde se muestran las vulnerabilidades y comercializan CaaS dirigido a ICS…), o derivados de la hiperconectividad.

El I Foro de la Ciberseguridad de Barcelona se ha consolidado como un esencial a la hora de divulgar conocimiento en ciberseguridad a nivel regional. Fueron más de 150 asistentes de modo online los que disfrutaron de debates de alto rango en materia de Ciberseguridad.

Esta jornada ha sido posible gracias al apoyo de Akamai Technologies, Forescout Technologies, OneTrust España, RiskRecon, Aruba, Cytomic y Samsung España.

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 Spain tiene ya a más de 250 empresas asociadas y más de 1.100 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

rgarcia@ismsforum.es

Twitter: @ISMSForum

LinkedIn: ISMS Forum

Teléfono: 600 87 19 69