NOTA DE PRENSA

25 de mayo de 2021, Madrid.

"Se espera que el coste global de las brechas de datos, como los pagos por ransomware, supere los 6 billones de dólares en 2021"

ISMS Forum -International Information Security Community- y su grupo de trabajo, **Cyber Security Centre (CSC)**, celebraron la **Décima Edición del Foro de la Ciberseguridad** el pasado jueves **27 de mayo** de 2021 en formato online.

Durante la jornada, intervinieron expertos internacionales y nacionales que aportaron su visión y conocimiento sobre cómo afrontar los retos presentes y futuros para la ciberseguridad: la transformación y securización del puesto de trabajo digital, los modelos de seguridad basados en el licenciamiento, la respuesta ante incidentes la inteligencia sobre amenazas, la monitorización continua y el registro de eventos de seguridad, el factor humano, o la gestión de identidades y el control de accesos, entre otros aspectos relevantes en materia de *Compliance* de ciberseguridad y protección de datos.

Una de las ponencias más destacadas fue la de **Lisa Short**, Digital Tech Transformation Strategist Analyst Design Ecosystems; Chief Research officer, Global Foundation for Cyber Studies and Research, que centró su intervención en la confianza digital como un activo y la responsabilidad de seguir el ritmo de la tecnología emergente para gestionar el riesgo y la oportunidad de la seguridad digital.

"Se espera que el coste global de las brechas de datos, como los pagos por ransomware, supere los 6 billones de dólares en 2021 y los 10,5 billones en 2025. Se puede poner esto en perspectiva al darse cuenta de que la cantidad es mayor que el coste de todos los desastres naturales a nivel mundial en un solo año y que se considera una amenaza mayor para la humanidad que las armas nucleares de destrucción masiva", comentó la experta.

Por su parte, **Nico Fischbach**, CTO Global y Vicepresidente de Ingeniería SASE en Forcepoint, abordó los aspectos del factor humano, en el que los malos comportamientos de un personal poco concienciado pueden llevar a poner en riesgo a la compañía. "Un indicador de comportamiento es la forma en que un usuario, dispositivo o cuenta se comporta. Por sí mismos, los comportamientos no suelen ser ni buenos ni malos. El contexto en torno a los comportamientos y la combinación de múltiples comportamientos determinan lo bueno y/o lo malo, expresado como el riesgo global resultante de una entidad", explicó Nico.

El **X Foro de la Ciberseguridad** acogió la presentación de la cuarta edición del **Proyecto de Gestión de Crisis Cibernéticas**, organizado por ISMS Forum, que ha contado con la participación de 28 compañías españolas, y con el apoyo por parte del sector público del Departamento de Seguridad Nacional, INCIBE y el CNPIC, y privado, a través del Business Continuity Institute (BCI), ECIX Group, F24, Nextvision, Mapfre y OYLO Trust Engineering.

"Continuamos mejorando la madurez de las compañías y el nivel de documentación de procesos, e incluso se han creado planes específicos para gestionar el ransomware. En cualquier caso, sigue predominando el conocimiento tecnológico sobre otras áreas, si bien todavía hay dificultades para involucrar o tratar incidentes con una visión más transversal e integral, permitiendo un análisis sobre la casuística y no uno centrado en la metodología. Por otro lado, se van dando unas respuestas cada vez más regladas sobre cómo categorizar y evaluar el impacto de los incidentes y se va extendiendo el servicio SOC, con el que cuentan cada vez más compañías", comentó **Carlos González**, Director de Resiliencia de Oylo, a modo de conclusión.

Christopher Painter, President, The Global Forum of Cyber Expertise Foundation; Commissioner, Global Commission on the Stability of Cyberspace; Former top, US Cyber Diplomat, un líder mundialmente reconocido en ciberpolítica, ciberdiplomacia, ciberseguridad y lucha contra la ciberdelincuencia, focalizó su intervención en los grupos de trabajo sobre el ransomware, "una amenaza que ha crecido exponencialmente desde 2018 y cuyos principales objetivos son hospitales, colegios, gobiernos, grandes y pequeñas corporaciones", afirmó el ponente.

"Los gobiernos deberían establecer fondos de ciberrespuesta y recuperación para apoyar la respuesta al ransomware y otras actividades de ciberseguridad; obligar a las organizaciones a informar sobre el pago de rescates; y exigir a las organizaciones que consideren alternativas antes de realizar los pagos", añadió Painter.

Uno de los ponentes estrella del **X Foro de la Ciberseguridad** fue **John McCumber**, Former Co-chair, National Institute of Standards and Technology (NIST), que explicó la necesidad de contar

con un marco de trabajo común que permita establecer procesos regulares -desde la contratación hasta la formación y la evaluación- para múltiples funciones en una organización.

“Este sistema debe compartir información clara sobre el trabajo de ciberseguridad para ayudar a los estudiantes interesados en este campo profesional, a las personas que buscan un nuevo empleo o cambiar de función, y a los trabajadores que buscan demostrar o aumentar sus competencias, así como proporcionar información directa sobre lo que una fuerza de trabajo necesita saber, ayudando en el desarrollo de certificados, insignias y otras técnicas de verificación para describir de forma coherente las capacidades del alumno”.

Esta **Décima Edición del Foro de la Ciberseguridad** de ISMS Forum finalizó con una pequeña reflexión sobre la necesidad de concienciación, formación y buenas prácticas en el sector de la ciberseguridad. Un año más, este encuentro, que ya cuenta con más de 600 asistentes cada año, contó con el apoyo de nuestros Platinum y Gold Sponsors: Darktrace, Forcepoint, Netskope, Pcysys, Recorded Future, Thycotic, Zscaler, Akamai Technologies, Aruba, BeyondTrust, CrowdStrike, Cytomic, Devo, Fastly, FireEye, Fortinet, HelpSystems, Huawei, NextVision, Palo Alto Networks, RiskRecon, S21sec, Splunk y Trend Micro.

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

rgarcia@ismsforum.es

Twitter: @ISMSForum

LinkedIn: ISMS Forum

Teléfono: +34 600 87 19 69