V Foro de la Ciberseguridad:

Security Intelligence, clave para la Transformación Digital

El pasado 28 de septiembre, el **Centro de Estudios en Ciberseguridad** de **ISMS Forum** celebró la quinta edición del **Foro de la Ciberseguridad**, presentado y dirigido por Daniel Largacha como director de la iniciativa y Global Control Center Assitant Director de Mapfre.

El Foro **congregó a más de 250 profesionales de la seguridad y la protección de datos** con el objetivo de examinar la evolución de los sistemas tradicionales de seguridad de la información hacia nuevos entornos basados en el análisis y la compartición de información, para mejorar la resiliencia empresarial ante un panorama de ciberamenazas cada vez más sofisticado, unido a la transformación digital que experimenta la Industria.

En las palabras de bienvenida, **César Arranz**, presidente de la Asociación Española de Ejecutivos y Financieros (AEEF), **destacó la creciente preocupación que la ciberseguridad supone para ejecutivos y financieros**, debido al impacto que tienen las ciberamenazas en los activos de la empresa. Además, nuevos fenómenos como el Cloud o el Big Data, hacen ver que el uso masivo de la tecnología supone una mayor exposición a los riesgos asociados. "*Hay una preocupación creciente*" por este nuevo negocio, explicaba Arranz, exponiendo los recientes casos de Yahoo, MySpace, LinkedIn, Adobe, Dropbox, entre otros.

La ponencia inaugural corrió de la mano de **Paul Cornish**, Director del Centro Global de Ciberseguridad de Oxford University y Director del área de Estudios de Rand Europe. Durante su discurso trató de responder a una cuestión clave: cómo la ciberseguridad se convierte en un importante catalizador para la Transformación Digital. Y una de las claves que apuntó Cornish es la resiliencia como elemento principal para afrontar los nuevos retos tecnológicos. **Empresas de todo el mundo acumulan pérdidas anuales por valor de quinientos mil millones de dólares debido a ciber-incidentes**, lo que hace cobrar máxima importancia a las herramientas para hacer frente a las ciberamenazas. Mientras las nuevas tecnologías facilitan el desarrollo económico y social de los Estados, es importante que todos los actores colaboren para minimizar los riesgos asociados al cambio.

A continuación, tenía lugar una interesante mesa redonda para abordar la protección de la información que se encuentra fuera de las empresas. Un nuevo escenario que afecta a la seguridad de la información y, por tanto, es imprescindible examinar las herramientas que

necesitamos para hacer frente a las ciberamenazas. La mesa redonda fue moderada por **Eduvigis Ortiz**, Global Alliances & Innovation Director Cybersecurity de Prosegur, y formada por **Javier Santiago**, Responsable de Ciberseguridad y Networked Defense de Trend Micro; **Alberto Cita**, SE Manager, Southern Europe de Blue Coat (Symantec); **Félix Martín**, EMEA Security Consulting Lead de HPE; y **Manuel Díaz**, Chief Information Security Officer de Huawei España. Fabricantes y proveedores de seguridad coincidieron en que **la creciente demanda de seguridad en entornos Cloud hace necesario un reenfoque de la seguridad hacia soluciones basadas en el dato**. Arquitecturas que puedan seguir a los servidores, visibilizar y controlar el uso y la compartición de los datos corporativos, y que permitan la gestión de identidades de las aplicaciones. "Herramientas que se integran en la Nube y están dirigidas a proteger la Nube", apuntaban los miembros de la mesa. Además, es necesario tener en cuenta los aspectos regulatorios, como el nuevo Reglamento Europeo de Protección de Datos, que introduce la extraterritorialidad, un principio que supone que los datos deben estar protegidos allá donde estén.

Un caso práctico sobre un gran ataque de denegación de servicio, presentado por **Marco Pacchiardo** de Akamai, ponía de manifiesto los posibles efectos devastadores para la actividad las empresas, medidos en tiempo de inactividad e inoperatividad. El ataque presentado por Pacchiardo, el ataque DDoS más grande rastreado por Akamai, resultó ser una amenaza de 363Gbps. Un tipo de ataque que se ha incrementado en un 126% en el último año y que cada vez se realiza con mayor dureza.

Continuaba una de las sesiones más esperadas, protagonizada por **Troels Oerting**, Chief Information Security Officer de Barclays para Europa, para hablarnos acerca del **nuevo Centro de Operaciones de Ciberseguridad de próxima generación de Barclays**. Una inversión en capacidades de inteligencia, señalaba Oerting, que permitirá utilizar grandes volúmenes de datos para mejorar la estrategia defensiva de la compañía y adaptarse a un futuro hiperconectado.

Para abordar el futuro del antimalware, se organizó una mesa con los principales fabricantes. Formaban la mesa redonda, **Rosa Díaz**, Directora General para España de Panda Security; **Mario García**, Country Manager Iberia de Check Point; **Carlos Muñoz**, Iberia Presales Manager de Intel Security; y **Luis Miguel Garrido**, Sales Manager de Fortinet. Como principales conclusiones, los nuevos entornos de IoT y movilidad fueron el punto de atención. **Los nuevos escenarios no estarán limitados a una serie de dispositivos, por lo que será necesario implementar soluciones analíticas que nos lleven de una seguridad preventiva a una seguridad que implemente elementos correctivos con una arquitectura integrada y escalable adaptada al nuevo panorama**. El objetivo es que las soluciones de seguridad estén integradas en el diseño de los nuevos dispositivos, pero también será necesario tomar medidas conjuntas para poder hacer un verdadero frente a las ciberamenazas con la compartición de Indicadores de Compromiso en tiempo real.

En la seguridad corporativa, por el contrario, encontramos carencias todavía muy importantes. **Xavier González**, co-fundador y CTO de OpenCloud Factory, presentó la solución Opennnac, una herramienta para el control y la monitorización de las redes y los dispositivos corporativos, que garantiza la seguridad y el cumplimiento normativo. Una herramienta para mejorar la

securización de una red corporativa identificando usuarios, dispositivos, casos de uso y comprobando el comportamiento basándonos en la política de seguridad aplicada e independientemente de la tecnología utilizada.

Y no menos importante es la seguridad de los sistemas SAP. **Peter Maier-Borst**, director ejecutivo de Virtual Forge Iberia, analizó las principales características de SAP concluyendo que **existen particularidades que no pueden ser cubiertas por las normas generales de seguridad TI**. Estas particularidades hacen que sean frecuentes algunas vulnerabilidades que permiten acceder a los datos, provocar tiempos de inactividad o tomar el control del sistema.

En la sesión vespertina, **Bryn Norton**, Director - Solutions Architecture EMEA de Level 3 Communications, abordó la necesaria adaptación de los sistemas de Inteligencia ante amenazas para mejorar la respuesta ante posibles incidentes. Mientras el número de dispositivos conectados aumenta rápidamente, también lo hace el número de vulnerabilidades. Norton analizó cómo **las empresas pueden hacer uso de las capacidades de Inteligencia para entender mejor las amenazas de su organización y responder de manera eficaz** a dichas amenazas.

Continuando con las amenazas en entornos IoT (Internet de las Cosas), **Stephan Gerhager**, Chief Information Security Officer de Allianz Deutschland AG e investigador en el área de movilidad e Internet de las Cosas, ofreció una magnífica visión de **los vectores de ataque que utilizan los ciberdelincuentes en el sector de la automoción y las posibles consecuencias de la digitalización** de un sector altamente sensible.

El foro llegó a su fin con la intervención de **THIBER, The Cybersecurity Think Tank**, con una demostración del proceso de perfilado de usuarios a través de la información que voluntaria o involuntariamente asociamos en las distintas plataformas y, por ende, la realización de ejercicios de atribución.

Sobre el Centro de Estudios en Ciberseguridad:

El **Centro de Estudios en Ciberseguridad** (CSC en sus siglas en inglés) es una iniciativa de ISMS Forum, creada con el objetivo de ser un punto de encuentro, debate e intercambio de conocimiento, así como para fomentar la colaboración público-privada en materia de Ciberseguridad en España.

El CSC quiere crear un estado de conciencia para controlar y gestionar los riesgos derivados de la dependencia actual de la sociedad respecto a las Tecnologías de la Información y la Comunicación (TIC), siendo un aspecto clave para asegurar el desarrollo socio-económico del país.

Para alcanzar la misión anteriormente descrita, el CSC lleva a cabo una importante labor de análisis (estudios), concienciación (eventos) y formación, entre otras actividades relacionadas con la ciberconcienciación.

Sobre ISMS Forum:

La Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, 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. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad.

ISMS Forum Spain tiene ya a más de 120 empresas asociadas y más de 800 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.

La Asociación organiza su actividad a través de distintas iniciativas, que abordan desde una perspectiva global o especializada la Seguridad de la Información: Jornadas Internacionales, Data Privacy Institute, Cloud Security Alliance, Cyber Security Center, el Centro de Estudios en Movilidad e IoT, el portal Protegetuinformacion.com, workshops sobre materias concretas y formación. Además gestiona las certificaciones Certified Data Privacy Professional (CDPP) y Certificate Of Cloud Security Knowledge (CCSK) en castellano para España y Latinoamérica.

Platinum Sponsors:

Gold Sponsors: