MÁS DE 300 PROFESIONALES DE LA SEGURIDAD Y LA PROTECCIÓN DE DATOS ACUDIERON A LA JORNADA

VI Foro de Ciberseguridad: éxito de asistencia y ponentes

Más de 300 profesionales de la seguridad y la protección de datos se dieron cita el pasado 27 de septiembre en Madrid en la sexta edición del foro de la Ciberseguridad organizada por el Cyber Security Center de la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum. Una jornada cuyo hilo conductor fue la aplicación de la inteligencia artificial en las soluciones emergentes de ciberseguridad como forma de afrontar los nuevos riesgos que se presentan en una sociedad hiperconectada para el desarrollo de la economía digital.

EL acto estuvo presidido por el director del Cyber Security Centre, Daniel Largacha, acompañado del presidente de ISMS Forum Spain, Gianluca D'Antonio, y con la inauguración especial de José María Lassalle, Secretario de Estado para la Sociedad de la Información y Agenda Digital. Durante su discurso, Lassalle hizo hincapié en que «la ciberseguridad debe formar parte de las infraestructuras tecnológicas porque tan importante es el despliegue de canales por donde circula comunicación como su adecuada protección».

Tras la bienvenida, se prestó especial interés al área de la Inteligencia Artificial de la mano de Anthony Bucci. En su ponencia titulada «Coevolution and cyber exploitation», explicó las claves de la computación evolucionaria y la Inteligencia Artificial, así como la manera en que se puede aplicar a la ciberseguridad a través de la información obtenida a partir de algoritmos.

De izquierda a derecha: Gianluca D'Antonio, José María Lassalle y Daniel Largacha.

En palabras de Anthony, «lo preocupante es que el 75% de los ataques no son detectados a tiempo, el 72% de las empresas, la mayoría PYMEs, son atacadas de forma constante y no salen en el telediario a pesar de las pérdidas que le supone». «En 2017 nos enfrentamos a 400 nuevas amenazas por minuto.» La respuesta de las empresas siguen siendo reactivas y se ponen soluciones una vez ha ocurrido el ciberataque. «Se diseña un antivirus... tras detectar el virus».

Casos de éxito

Los casos de éxito y war stories en la lucha contra las ciberamenazas vinieron por parte de Álvaro Cordero, Security Operations Center Manager en Akamai, y Drew Schuil (Imperva), que aportaron los puntos clave para afrontar los nuevos desafíos. Cordero, en su intervención, explicó cómo desde Akamai, fueron capaces de detectar varios ciberataques gracias al análisis de evidencias previas.

Marcaron como puntos críticos, la capacidad y Centro de Data Center, las herramientas de la propia empresa y, por último, pero no menos importante, el soporte continuo de la empresa. Cordero sentenció que «el problema para anular este tipo de ataques es que están muy distribuidos, con más de 200.000 servidores».

Por otra parte, Drew Schuil, habló acerca de los desafíos cotidianos al te-

ner que detectar amenazas desde dentro de la compañía. Habló de las aplicaciones de seguridad que tiene a su alcance y de las herramientas que le facilitan el trabajo en su día a día.

A lo largo de la mañana se produjeron varios debates y ponencias sobre los nuevos vectores de ataque y la aplicación de medidas basadas en inteligencia artificial para su detección y mitigación fuera del radar de la seguridad.

En una primera mesa redonda se contó con las aportaciones de los principales proveedores de seguridad. Estuvo compuesta por Raúl Pérez, Global Security Solutions en Panda Security, quien remarcó que cada vez que llega un ataque es muy probable que sea nuevo, por lo que han optado por trabajar con el goodware y así hacerle frente.

Alberto Ruiz, Presales Engineer en España y Portugal de Sophos, «el deep learning es un paso más sobre el machine learning. Este depende del ser humano, ya que somos nosotros los que establecemos los patrones de trabajo». Alberto Cita, SE Manager Iberia en Symantec, apostó también por el Deep Learning ya que empresas tan innovadoras como Facebook, Google o Amazon lo han implantado en sus estrategias.

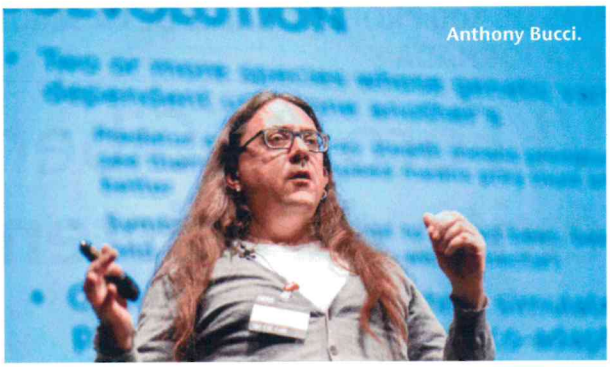
Estrategias de ciberseguridad

Alfonso Martínez, Consulting Sales Engineer EMEA Forcepoint, declaró que hay que ser consciente y establecer una gran base en la capa del machine learning pero hay que protegerse para evitar ciberataques.

José de la Cruz, director técnico en Trend Micro, expuso que una compañía para establecer una estrategia de ciberseguridad tiene que tener en cuenta cuáles son los riesgos y amenazas de la misma.

Samuel Bonete, Regional Sales Manager en Fortinet, apuntó que el 70% del malware nuevo está entrando por el correo electrónico, ends points conectados en sitios que no deberían estar conectados, redes Wireless.

Rogier Holla, Deputy Head CERT EU, centró su participación en contar los esfuerzos que se hacen desde CERT – EU en materia de ciberseguridad y protección de datos.


Anthony Bucci.

La gestión del riesgo de terceros, tanto de las necesidades de seguridad y cumplimiento en la gestión con terceros (proveedores, partners, etc.) como en las medidas de seguridad preventivas y la gestión de identidades, fue el hilo conductor de esta mesa redonda por parte de las compañías Micro Focus, Prosegur, Huawei o Level 3 Communication.

Jesús Prieto, responsable de productos de seguridad de Microfocus planteó dónde están los límites de lo que se quiere compartir y lo que la ley obliga. Allan Guillén, Cybersecurity DDos Specialist en Level 3 Communications, sentenció que hay que saber qué tipo de información queremos compartir, por qué canal lo queremos difundir y con quién queremos compartirlo.

Incidentes de seguridad y protección de datos

Manuel Díaz, DPO Huawei, manifestó que la cultura instaurada en España no es propensa a compartir con terceros los incidentes de seguridad causados, pero con la nueva RGPD que entrará en vigor el próximo mes de mayo irá cambiando esta tendencia. Mientras, Jordi Martínez, director de Comunicación y Relaciones Institucionales del Instituto Cerdá, explicó a lo largo de su ponencia la importancia de una buena comunicación durante la gestión de un incidente de seguridad.

Peter Maier – Borst, Managing Director de Virtual Forge, explicó cuál es la mejor forma de hacer un perfecto pen-testing en sistema SAP y cuáles son los temas que hay que desarrollar, tales como, reparación, hallazgo de vulnerabilidades, así como concienciación a todos los niveles. Roi Fortes, responsable de Servicios de Seguridad en Inprosec, explicó a su vez las bondades del whitetesting, así como las medidas que llevar a cabo para evitar el robo de datos en sistema SAP por parte de usuarios malintencionados.

La sesión vespertina puso el foco de atención en las nuevas consideraciones incluidas en el nuevo Reglamento Europeo de Protección de Datos sobre responsabilidad proactiva y resiliencia, con las experiencias prácticas de Gas Natural Fenosa, Abanca y Abertis Autopistas.

Esta mesa redonda, moderada por Carlos Alberto Sáiz, vicepresidente de ISMS Forum, e integrada por Roberto Baratta, Global Executive VP Abanca; Andreu Bravo, CISO de Gas Natural y Ángel Pérez, Responsable de Organización y Ciberseguridad de Autopistas, concluyeron que hasta la entrada en vigor del nuevo Reglamento Europeo de Protección de Datos se va a ir produciendo poco a poco un cambio cultural para cubrir todas las áreas de ciberseguridad, tecnología e incluso marketing.

Por último y como broche de oro para cerrar la jornada, Manuel González, analista de ciberseguridad de THIBER dio una ponencia sobre tactical response, en la que aportó las claves para «compartir la información de cada uno de los incidentes que vamos analizando y van saliendo de manera confiable como los indicadores de compromiso». ●

Texto y Fotos: ISMS Forum