

JORNADA SEGURIDAD TELCO 2018 ORGANIZADA POR ALAI SECURE

# Seguridad en las comunicaciones: tendencias, oportunidades, riesgos

## Instaladores y CRAs descubren los nuevos servicios de Alai aplicados a seguridad

La tercera edición de las Jornadas de Seguridad Telco, organizada por Alai Secure en el hotel Pullman de Madrid, volvió a despertar el interés de destacados integrantes del sector de la Seguridad Privada. Profesionales de Centrales Receptoras de Alarmas e instaladores se dieron cita en esta jornada bajo el epígrafe "La Seguridad en las comunicaciones". Durante el evento, ponentes de primer nivel desgranaron casos de éxito, últimas tendencias y nuevas prestaciones en seguridad: Innovación, tecnología, comunicaciones y servicios pensados por y para la seguridad.

**E**l encargado de dar la bienvenida al cerca de medio centenar de asistentes fue el director comercial de Alai Secure, Javier Anaya, quien hizo una semblanza del impacto de las comunicaciones, marcadas por la hiper-

conectividad de los dispositivos que utilizamos, en el ámbito de la seguridad. En su charla 'El futuro de las comunicaciones en seguridad: oportunidades y amenazas', Anaya recordó que "todo el mundo quiere tener sus cosas conecta-

das", en referencia al Internet of Things (IoT), lo que puede constituir una brecha en términos de seguridad. En este sentido, Anaya resaltó que "la banda libre ya no se puede securizar como otros sistemas". En concreto, se refirió a lo que denominó "la madre de todos los IoT: abrir la puerta de casa sin utilizar una llave física".

El director comercial de Alai también puso otro ejemplo de la transformación que supondrá la evolución de los sistemas de comunicaciones, al señalar que Dinamarca dejará de tener dinero en efectivo en 2030, "lo que cambiará el sector bancario y el transporte de fondos". 'La ciberseguridad en un mundo conectado' fue el tema sobre el que giró la primera de las ponencias del programa, a cargo de Elena García Díez, responsable de Servicios de Ciberseguridad para Empresas y Profesionales del INCIBE. García Díez comenzó con un dato revelador: en 2020 habrá 20.800 millones de dispositivos conectados, lo que da una idea de la trascendencia que cobra el Internet of Things en nuestras vidas.

Esta realidad hace que la ciberseguridad "esté presente por todas partes" para hacer frente a las amenazas que presenta esta proliferación de dispositivos vinculados. La representante del INCIBE las clasificó entre las que se originan por una configuración inadecuada, por comunicaciones y datos o bien por un software/firmware vulnerable. El reto de la hiperconectividad su-



pone el riesgo de que nuestro dispositivo pase a ser parte de un botnet IoT, que, a diferencia de los botnets tradicionales, se caracteriza por su facilidad de creación y expansión, su bajo coste y su alta disponibilidad. En este contexto, García Díez hizo balance de la labor que desarrolla el INCIBE y que en el último año se tradujo en 123.064 ciberincidentes gestionados, de los que 116.642 fueron sufridos por ciudadanos y empresas.

Asimismo, desgranó las distintas herramientas de ciberseguridad que el organismo público pone al servicio de profesionales (a través del CERTSI) y de empresas, proporcionando a las compañías de menor carácter técnico un kit de concienciación para protegerse de las ciberamenazas. “La ciberseguridad no es una opción”, concluyó la representante de INCIBE.

La tercera ponencia de la jornada fue ofrecida por José Montori, CEO de Bold Technologies, quien explicó las funcionalidades de su solución Manitou Cloud Services, un software que facilita a los clientes la infraestructura necesaria para operar su centro de alarma, ya sea en parte o en su totalidad, a través de una interfaz en línea segura.

A continuación fue el turno de Eduardo Mohedano, Infraestructure



Architect del Grupo Ingenium, cuya intervención llevó por título ‘Desmontando el mito de las APNs privadas. ¿Son realmente seguras como pensamos?’. Tras hacer un repaso de la evolución de la seguridad basada en GPRS, Mohedano expuso los nuevos riesgos que suponen el IoT y el M2M (Machine to Machine). En este punto se refirió al ataque MIRAI, que el 21 de octubre de 2016 afectó a millones de usuarios en EEUU y Europa y que tumbó a servicios de internet como Twitter, Amazon o PayPal. El responsable de este “Pearl Harbour 2016”,

como lo calificó Mohedano, fueron cien mil dispositivos IoT.

Por su parte, Francisco Valencia, director general de Secure&IT, disertó sobre las ‘Medidas organizativas y técnicas de adecuación al GDPR’, que cambiará el paradigma de la gestión de datos personales a partir que sea obligado cumplimiento desde el próximo 25 de mayo. La única mesa redonda de la jornada giró en torno a la ‘Problemática de la gestión de llaves y las nuevas soluciones en validación y apertura remota’, donde intervinieron Florencio Martín, director general de Atenzia; Roberto Vilela, director de Servicios y Soluciones de Techco Security, y Adriano Marqués de Magallanes, CEO de Imagina Ingenio.

El colofón a la jornada lo puso Sergio Cano, CEO de Alai Secure, con la ponencia ‘Nuevas propuestas de Seguridad Telco para sistemas de autenticación y apertura remota’. Se trata de un sistema de apertura remota, denominado M-Key Secure, basado en Seguridad Telco y que está llamado a sustituir a las llaves físicas. ●



TEXTO Y FOTOS: EMILIO S. CÓFRECES