

La seguridad IoT es un problema de todos

23 OCT 2017 <http://www.itdigitalsecurity.es/reportajes/2017/10/la-seguridad-iot-es-un-problema-de-todos>



Durante el II Foro de la Movilidad e Internet de las Cosas organizado por ISMS Forum, se ha analizado el estado de la seguridad en IoT y la forma de generar concienciación y sensibilización sobre los riesgos y amenazas en un mundo cada vez más interconectado.

Cuatro son los pilares en los que se basa la seguridad del Internet de las Cosas, según Francisco Lázaro, director del **II Foro de la Movilidad e Internet de las Cosas** celebrado el pasado 18 de octubre en Madrid: regulación, normativa y leyes; concienciación y sensibilización; buenas prácticas; y, por último, la construcción y mantenimiento correcto de los dispositivos conectados.

La ponencia inaugural del foro estuvo a cargo del director general del Instituto Nacional de Ciberseguridad (INCIBE), Alberto Hernández, en la que aportó la visión de INCIBE sobre el estado actual y las políticas públicas en el ámbito del IoT. Habló de las tendencias tecnológicas, subrayó que las Smart Cities serán el futuro y aseguró que “el nuevo ámbito tecnológico de la ciberseguridad presenta una gran **oportunidad para las PyMES** para desarrollar productos y

servicios". Además, señaló que, en la actualidad, hay una falta de talento en ciberseguridad y esto va a condicionar también a la hora de poder dar soluciones a problemas de ciberseguridad. "El fabricante será el responsable para establecer mecanismos de seguridad por lo que el ciudadano ha de estar concienciado con las buenas prácticas de seguridad" dijo Hernández.

El director general de INCIBE explicó los **tres puntos importantes en materia de ciberseguridad** en IoT donde habrá que trabajar tanto empresas del sector público, así como del sector privado. El primer punto que destacó es la realidad de las ciberamenazas. Como segundo punto explicó la importancia de la concienciación ciudadana, el tercer paso tiene que ver con la automatización e interiorización de los dos pasos anteriormente descritos. "Interiorizar las reglas de ciberseguridad será un apartado en lo que tenemos que trabajar intensamente". Hernández concluyó manifestando "la seguridad IoT es un problema de todos: empresas, fabricantes y usuarios."

Desde Comisión Europea, se revisaron los retos que presentan las tecnologías emergentes en materia de ciberseguridad y protección de datos con la participación especial de Jakub Boratynski, jefe de la Unidad "Confianza y Seguridad" responsable de ciberseguridad y asuntos de privacidad digital de **Comisión Europea** (Dirección General de Redes de Comunicación, contenido y tecnología). Boratynski comenzó su discurso diciendo que "la digitalización de nuestra sociedad, en general, necesita una mayor ciberseguridad en todos los aspectos" y recalzó que, ENISA, en colaboración con Comisión Europea hace frente a los nuevos retos de ciberseguridad a través del desarrollo, implementación y revisión de las políticas y leyes que se están llevando a cabo para establecer una normativa rigurosa. Para concluir, animó a todos a "construir una ciberseguridad más robusta para toda la Unión Europea."

Desde el Centro de Estudios en Movilidad e Internet de las Cosas (CEM IoT), se presentó el estudio que aborda el estado y nivel de adopción de tecnologías IoT, el análisis de los vectores de ataque en dispositivos IoT, o el impacto de las tecnologías IoT en la privacidad de las personas.

Paloma Llana, Líder del área Legal del Centro de Estudios en Movilidad e IoT señaló que "ha llegado el tiempo de la responsabilidad, el tiempo del accountability". Asimismo, se preguntó cuánto tendrá que ser de inteligente un dispositivo conectado, por ejemplo, un vehículo para conducirse solo. "**¿Quién es el responsable de garantizar la seguridad del producto?** ¿Quién será el responsable de garantizar la seguridad en el tiempo?", se preguntó la directiva. Ya no solo se trata de fabricarlo de una manera segura sino de mantenerlo actualizado y ser capaz de mantener la seguridad del software en el momento que haya una actualización. "¿Cuáles serán las consecuencias de no hacerlo? Y sobre todo saber, ¿Quién va a ser responsable y de qué?" Por último, manifestó que "IoT es un concepto evolutivo".

Jorge Hurtado, Líder del área de Certificación y buenas prácticas del Centro de Estudios en Movilidad e IoT, explicó el objetivo principal de este estudio fue la definición de cuáles son las mejores prácticas orientadas hacia productos orientados al consumidor final. así como proporcionar un mecanismo de confianza que avale el seguimiento de las mismas. También explicó cuáles son los dominios más relevantes presentes en el estudio: Ciberseguridad por diseño y defecto, seguridad en sistemas, protección tanto en el hardware como en el firmware, seguridad en comunicaciones, así como seguridad en el ciclo de vida comercial, en el que se debe habilitar algún canal para poder comunicarse con

el fabricante en caso de duda por parte del usuario o consumidor y, por último y no menos importante, la seguridad jurídica.

El II Foro de la Movilidad e IoT fue el escenario de presentación de la **Marca de Garantía en Ciberseguridad IoT**, desarrollada por el CEM IoT de ISMS Forum y que se presentará en los próximos meses. “Esta marca de garantía será útil tanto para el usuario o consumidor y el fabricante”, subrayó Jorge Hurtado.

A continuación, tuvo lugar una mesa redonda en torno a la necesidad de implementar la ciberseguridad en los entornos conectados como forma de afrontar la “jungla digital” en la que premia el Time to Market. Esta mesa estuvo compuesta por Dani Creus, Kaspersky; “el parcheado agresivo deja inutilizable cualquier dispositivo conectado” Jorge Laredo, Hewlett Packard Enterprise; “la regulación en dispositivos IoT va a haber, la duda es cómo y cuándo la van a implementar.” Fernando Romero, Prosegur ha apuntado “ahora todo está conectado, estamos empezando a utilizar un mayor número de dispositivos IoT.” José María Cayuela de Akamai, “**las comunicaciones IoT deben estar cifradas** y hasta que no lo estén debemos estar preparados para adaptarnos a las diferentes medidas de ciberseguridad necesarias.”

David Gascon, co-fundador y Chief Technology Officer en Libelium, dio a conocer la implementación de seguridad desde el diseño de fabricación de sensores de Libelium, mientras que José Ramón Monleón, CISO Orange, se centró en el compromiso que tiene Orange con la aplicación de la seguridad en las nuevas tecnologías. Este compromiso ha aglutinado las diversas etapas en las que se mejora la protección de los clientes, fomenta la seguridad e incluso se anticipan a posibles ataques cibernéticos. También como punto importante ha destacado la importancia de la innovación tecnológica. En palabras de Monleón, “el futuro viene por la movilidad e IoT, vamos a tener millones de IoT conectados y es conveniente que colaboremos entre todos los actores”.

Máximos expertos de la tecnología y del hacking como son Raúl Siles, Pedro Cabrera y Raúl García, realizaron una **demostración de hacking en directo** y pusieron de manifiesto las vulnerabilidades que los dispositivos hiperconectados tienen y cómo han pasado a formar parte de nuestra vida con los riesgos que ello conlleva

Por su parte, Hugo Teso habló en su ponencia acerca de los retos y la aproximación de la ciberseguridad para entornos críticos como la aviación o la automoción.