José M. Vera, 20 octubre 2017, http://www.onemagazine.es/analisis-internet-de-las-cosas-alberto-hernandez-isms-forum-spain

Qué está pasando con el 'maldito' Internet de las Cosas

No hay quien lo pare. Quizá no lo percibas, pero las máquinas y los sensores ya están colonizando el mundo. En menos de cinco años tendrás luces, neveras, termostatos y coches inteligentes. Pero…. Los expertos alertan de que nada está haciendose seguro. El ISMS Forum Spain, la principal asociación de ejecutivos de ciberseguridad, ha dedicado una jornada para analizar cómo hacerlo de forma segura.

No hay quien lo pare. Quizá no lo percibas pero las máquinas y los sensores ya están colonizando el mundo. En menos de cinco años tendrás luces, neveras, termostatos y coches inteligentes. Pero…. Los expertos alertan de que nada está haciendose seguro. El ISMS Forum Spain, la principal asociación de ejecutivos de ciberseguridad, ha dedicado una jornada para analizar cómo hacerlo de forma segura.

Alberto Hernández, director general del Incibe: "El Internet de las Cosas es un problema hasta para los juguetes de los niños"

"Se está produciendo innovación tecnológica pero se está pasando directamente a su comercialización rápida. Ese factor de acelerar el modelo evolutivo la seguridad no esté presente con los graves problemas que presenta. Y a ello se suma que el ciudadano cobra un papel fundamental porque el usuario de estos dispositivos, que consumirá de forma masiva, va a ser de nuevo el eslabón más débil", ha explicado el director general de Incibe, Alberto Hernández, durante la inauguración de

la jornada que ha presentado Francisco Lázaro responsable de temas de movilidad en el ISMS Forum Spain.

Hernández ha explicado que en su visita en el centro de innovación de Sansumg en Seul pudo ver la primera nevera inteligente. Y preguntaron si el ciudadano pagará más por tenerla conectada a Internet. Y la respuesta era muy fácil: sabiendo el inventario de la nevera no hará falta hacer la compra o permitirá conocer si tenemos los ingredientes necesarios para lo que queremos comer.

“Para hacer un mundo conectado seguro hay que pasar por tres fases. La primera es tener conciencia de que hay riesgos y amenazas. Mucha gente es consciente de ello desde WannaCry. La segunda es que el ciudadano lo entienda. Y estamos en ello. Los ciudadanos saben que hay ciberataques y tienen que protegerse. Y el tercer paso tiene que ver con automatizar esto. Y no es sencillo. Poca gente tiene un antivirus en el móvil… ni los expertos en ciberseguridad.

Desde Incibe recuerda que en septiembre de 2017 ya se han pasado las amenazas detectadas en 2016. “Y con el Internet de las Cosas esas amenazas van a ir a más y los ciudadanos van a formar parte de ellas bien como víctimas o como cómplices”.

El problema que plantea un mundo conectado es que muchísimos dispositivos no tienen ningún tipo de autenticación. En segundo lugar que, además, usan contraseñas por defecto o débiles. Los routers ya han conseguido superar esta fase pero muchísimos dispositivos aún no lo han hecho. Por ejemplo, algunas empresas se han visto afectadas por un ransomware porque un cibercriminal ha entrado en la red por una contraseña insegura. Por último el gran problema es que muchos servicios innecesarios se quedan en el olvido de una empresa…. Siendo una nueva forma de entrar en la empresa, ya que carece de la seguridad adecuada.

En cuanto a las comunicaciones y datos los problemas son un cirado débil o inexsistente, un problema de privacidad de datos y por último que se puede acceder físicamente a ellos para romper su seguridad. Igual pasa con el software y el firmware de los dispositivos conectados. En unos

casos, son tan baratos, que se han vendido sin una auditoría de seguridad. En otros no tienen actualizaciones, tampoco un soporte para solucionar problemas y, por último, algunos, incluso, tienen puertas traseras que permiten el acceso a ellos y su toma de control.

Alberto Hernández también ha recordado el papel de los ciudadanos para que exijan que un producto cumpla con características de ciberseguridad, además de la labor que debe hacer la administración para regular la seguridad de los productos conectados.

Entre los casos más populares de productos conectados con fallos de seguridad están desde la Hello Barbie que tenía una brecha de seguridad y que permitía que un criminal pudiera acceder al juguete. También han surgido problemas con televisiones inteligentes, por ejemplo de Samsung, que estaban en modo de escucha pasiva o de los routers que han vuelto a ser considerados vulnerables esta semana con el agujero de seguridad descubierto en el protocolo WPA2. “Un fallo que puede minimizarse con las actualizaciones de seguridad de los fabricantes, usando https que cifra las comunicaciones o a traves de sistemas VPN”, ha explicado Hernández.

También está el caso de los coches conectados con casos de fallos de ciberseguridad como el que se dio a conocer en 2015 en un Jeep Cherokke. También un hacker español ha demostrado este año cómo puede acceder al sistema de control 3G de camiones de carga…

Y el problema también afecta a nuestra salud. Recientemente un investigador ha evidenciado que medio millón de marcapasos podían ser hackeados y, en el peor de los casos, dañar gravemente a su usuario por lo que las personas que los tenían tuvieron que pasar por los hospitales para actualizarlos.

Por último los dispositivos conectados de forma no segura tienen el problema de que pueden ser controlados para ataques de redes zombies -botnet- como ocurrió con la Bornet Mirai. Cientos de miles de cámaras y sistemas de grabación, también de España, permitieron hacer un ataque en EE.UU. Que dejó sin Internet a 1.000 millones de personas durante una tarde, sobre todo en EE.UU.

¿Tiene solución la falta de seguridad en el Internet de las Cosas?

En primer lugar hay que trabajar en el diseño seguro, en los dispositivos, hay que hacer mejor configuración, realizar auditorías de seguridad, actualizaciones y en la red implementar la red y ella autenticación. En aplicaciones y servicios es importante poner en marcha la confidencialidad y privacidad y la seguridad de los datos. La seguridad del Internet de las Cosas es un problema de todos, de los usuarios y de las empresas. Todos en los próximos años debemos estar concienciado y, como hoy te pones el cinturón de seguridad, tendrás que tomar medidas para manejar de forma segura millones de dispositivos", ha destacado Hernández.

Cinco claves para hacer un mundo conectado seguro

"Los retos de la seguridad del Internet de las Cosas es que habrá una superficie de ataque mucho mayor, mayor cantida de amenazas, mayor diversidad de riesgos, con entornos físicos no controlados, y difíciles de aislar, incluso, con el problema de reiniciar procesos que pueden suponer interrumpir un servicio. Hay una necesidad de actualizaciones y mantenimiento y crear una normativa y regulación necesaria para que todo sea lo más seguro posible.", ha pedido Hernández en el Caixa Forum donde se ha celebrado el II Foro de Movilidad e IoT del ISMS Forum Spain.

¿A quién impacta el riesgo de un mundo conectado sin seguridad? Pues seguramente a los ciudadanos, a las empresas… Habrá que crear una cultura para que el ciudadano exija seguridad. La seguridad no es un coste sino una inversión y una ventaja. Es importante que la seguridad comience en el diseño y se mantenga en el tiempo, que sea aplicada en toda la arquitectura y ser gestionada en todas las organizaciones implicadas", ha terminado.

¿Rama de olivo o palo, qué hace falta para regular de forma segura los dispositivos conectados?

Durante la mesa redonda dedicada a normativa se ha hablado que actualmente casi no hay normativas que obliguen a las marcas de dispositivos conectados a cumplir normas de seguridad. Ese ha sido el

punto de la mesa redonda que ha celebrado el ISMS Forum y que ha tenido cuatro peticiones muy claras a los fabricantes…

En la mesa redonda de seguridad en los dispositivos IoT y la parte de cómo se usan los dispositivos han internvenido expertos como Dani Creus, de Kaspersky, Jorge Laredo. De HPE, Fernando Romero de Prosegur y José María Cayuela de Akamai que ha explicado nuevas iniciativas para identiicar para dispositivo cuando se conecta a la nube.

“En el IoT es que hay que facilitar las cosas al usuario. El usuario no siempre tiene la culpa”, dije entre sonrisas Romero de Prosegur. “Seguramente los gobiernos y los responsables de la normativa tienen mucho que ver con la poca seguridad de muchos dispositivos”, ha destacado el moderador de la mesa Jorge Hurtado de Cap Gemini.

“El problema es que mucha gente se dedica a escanear con malware dispositivos y cuando encuentra aparatos vulnerables los deja inutilizados”, ha alertado Creus.

En la mesa también se ha expuesto que ya hay cosas que atacan cosas, cosas que roban la identidad de más cosas… Ya hay ‘fabricantes’ de malware para dispositivos conectados. “Hay que ver que los criminales ven en esto un negocio. Hay software malicioso detectado desde 2008 y actualmente se están viendo muchos ataques”, destacó Creus.

En cuanto a la labor de los gobiernos para crear un marco regulatorio que haga de las cosas seguras se ha analizado la iniciativa, por ejemplo, de ISMS con un sello de ciberseguridad, y de cómo el gobierno debería acometer iniciativas similares. “Creo que es importante que se pongan en marcha normativas de ciberseguridad que hagan las cosas seguras de forma obligatoria. Así que más que por rama de olivo apuesto por ‘el palo’ para el que no cumpla los estándares mínimos de ciberseguridad”, ha comentado Cayuela de Akamai.

“Creo que la normativa es una palanca más que ayuda a mejorar la ciberseguridad. El usuario quiere usar cosas sin causar problemas así que hay que darle herramientas para ello”, ha dicho Romero. “Regulación va haber. Es evidente y si no hay seguridad habrá sentencias judiciales. El

problema es que de momento la seguridad es un tema que va paso lento hasta que ocurra algo. Tras el 11S EE.UU. Dedicó mucho personal y medios a regular la seguridad en el aire. Algo parecido, desgraciadamente, puede pasar en la ciberseguridad", ha dicho Laredo. "Igual que hay un sello de seguridad en temas de juguetes también tienen que tenerla los dispositivos conectados como un termostato", ha añadido. "Lo importante es que no pensemos que por tener una regulación el sector se puede "dormir en los laureles" ha terminado destacando Dani Creus, de Kaspersky.

En este sentido se han pedido que todas las comunicaciones en Iot estén cifradas, se dedique más inversión a concienciación, a dar a conocer las amenazas y que los fabricantes de dispositvos dejen de poner contraseñas por defecto o incorporar servicios que se dejan abiertos y que realmente no sirven para el uso del dispositivo.