One Hacker

José M. Vera http://www.onemagazine.es/primer-sello-de-producto-ciberseguro-espana-isms-forum-para-iot-internet-de-las-cosas-88-check-list

Así es y así se ha creado el primer sello de 'Producto ciberseguro' que todas las empresas pueden tener

88 puntos. Ese es el 'examen' que deben cumplir las empresas y sus productos conectados para obtener el primer sello de España que certifique que son seguros ante ciberataques o fugas de información -aunque en este campo el 100% de seguridad no existe. Se trata de una iniciativa de la principal asociación de ciberejecutivos españoles, ISMS Forum, que

buscar evitar el caos que ya está viviéndose con millones de dispositivos conectados sin control alguno.

El ISMS Forum Spain, la principal asociación de ciberseguridad, ha dedicado una mesa redonda sobre quién tiene que trabajar más para hacer un mundo conectado seguro. Han intervenido en ella grandes expertos como **Rasul Siles,** de Dinosec, **Paloma Llaneza**, del **Centro de Estudios de Movilidad** e IoT del ISMS Forum, y **Jorge Hurtado, de Capgemini**, en un mesa presentada por Francisco Lázaro, de ISMS Forum.

“Aún hay esperanza”, ha explicado el responsable del equipo de Movilidad e IoT del ISMS Forum, Raul Siles, CTO de la empresa Dinosec. “Es importante analizar los vecotes de ataque de IoT. Es importante definir que el IoT es “cualquier dispositivo electrónico, que puede ser un sensor o recibe órdenes que le hacen cambiar -como el termostato- o es un elemento que pone en común a ambos”, ha explicado Siles que también ha explicado que los vectores de ataque pueden ser físicos -puertos o interfaces de conexión o el firmware de los dispositivos, el software con el que funciona-. Esto permite abrir el dispositivo, analizar su placa y ver cómo funciona. En los vectores de ataque es importante tener en cuenta los solapamientos. “Se puede saber del dispositivo tanto accediendo a él como a través de la web de su fabricante”.

En segundo lugar otro vector de ataque son las comunicaciones entre el dispositivo y la nube, entre el dispositvo y otros dispostivos o aplicaciones móviles y en conunicaciones inalámbricas -wifi o blutetooth- En tercer lugar

el interfax web y otros interfaces de gestión también son vulnerables y permiten aceder al dispositivo. Por ejemplo, hace poco un fabricante conocido puso en venta unas cámaras de vigilancia a las que se podía acceder e incluso tomar su control a través de Telnet. Por último, el cuarto vector de ataque es que los servicios o datos que usan los dispositivos también permite acceder a él a través de servicios de red o de almacenamiento de datos e información en el dispositivo. Paloma Llaneza ha destacado que en el mundo de los abogados está llegando "el momento de la responsabilidad". Está claro que hay que educar al consumidor y pedir sellos de garantía "pero yo como abogado no voy a buscar la culpa del lado del consumidor sino de parte del fabricante, el que desarrolla el software. Por ejemplo, que tu frigorífico no haya calculado bien la caducidad de tus alimentos".

¿Quién va a ser responsable de los fallos en tus dispositivos conectados?

"Tenemos actualmente una obligación de recoger la autorización de los clientes para gestionar sus datos de forma expresa. El nuevo reglamento de protección de datos va a obligar a desarrollar dispositvos IoT de forma segura porque vamos a tener que responder a los daños. Y hablamos de lavadoras, de coches…. ¿qué inteligencia tiene que tener para ser seguro? ¿Cuantos datos de nuestra vida y entorno va a gestionar? Casi cualquier cosa va a entrar en el Internet de las Cosas.

La UE considerada, en el tema de la robótica, que hace falta unas nuevas normas y ya ya avanzado que su ADN va a ser la doctrina del riesgo. El que tenga la obligación de evitarlo tiene que pagar por el riesgo que causa. En un coche está claro: si un automóvil autónomo causa un accidente se puede echar la culpa al fabricante de los sensores, a la marca del coche, a un criminal….pero lo que dice la UE que la responsabilidad será de la marca de coches y está tendrá que demandar a quién considere responsable. Aquí ya no hay causa efecto. Por no evitar el riesgo puedes ser responsable como empres. Así que si no se hace por amor al arte o por salvar el mundo hay que hacerlo por el dinero que te vas a ahorrar. Hay que poner en práctica nuevas normativas para minimizar el riesgo.

Jorge Hurtado ha explicado el grupo de trabajo del ISMS Forum sobre el estudio que ha presentado hoy y que intenta ser una guía de buenas prácticas para la construcción de dispostivos conectados. “Hay que formar a la gente y a las empresas pero también hay que dar herramientas para que los consumidores puedan exigir unos mínimos y las marcas saber que los cumplen”, ha destacado.

¿Qué apartados tiene que tener en cuenta una marca de dispositivos conectados? Pues la ciberseguridad por diseño y por defecto, la protección del hardware y firmware, la seguridad en sistemas, la seguridad en comunicaciones, la seguridad en el ciclo de vida comercial y la seguridad jurídica. Así Hurtado ha recomendado para exigir la garantía de seguridad es que la responsabilidad de seguridad esté identificada, que permitirá al consumidor preguntar sus dudas en caso de fallos. También hay que exigir que los dispositivos tengan actualizaciones de forma automática. “Los productos no acaban en la cadena de producción. Hay que hacer contínuamente análisis de vulnerabilidades que garanticen que durante su tiempo de uso sigue siendo tan seguro como cuando lo compró”.

Otro tema que se ha considerado vital es que los dispositivos se identifiquen cuando se conecten. “No se pueden vender productos que usen el mismo certificado digital… porque eso supone que si alguien conoce la clave de uno podría acceder a millones con la misma clave”, ha dicho Hurtado.

¿Quieres que tus productos tengan un sello como ‘Ciberseguros'?

La mesa ha destacado el trabajo del Grupo de Trabajo que ha permitido crear un identificador de garantía ‘ISMS Confianza IoT’ que permita a consumidor y fabricante saber que un dispositivo es seguro. Para cumplir con el certificado hay que rellenar de forma positiva 88 controles en dos niveles y el ISMS Forum lo certificará. “Entre otras medidas se pedirá un responsable de seguridad, el análisis de riesgos y meidas, el disponer de requisitos de SSDLC, medidas de detección pasiva y activa, la actualización de seguidad atomáticas, identidad de las cosas, responsabilidad civil, privacidad...entre otras muchas”. Además, algunos fabricantes como Orange o Libelium también están participando para

saber si todo lo que se exige es asumible y permite, realmente, comprobar que algo es seguro.

Si quieres conocer al detalle cómo certificar un producto y en qué situación están los dispositivos del **Internet de las Cosas puedes leer el informe completo aquí.**