EL PAÍS

Una organización española crea un sello de ciberseguridad para Internet de las Cosas.

La iniciativa es una respuesta a la falta de una regulación que obligue a los fabricantes a proteger al usuario.

10 JUL 2017 - 13:46 CEST
https://elpais.com/tecnologia/2017/07/07/actualidad/1499420748_095668.html#?ref=rss&format=simple&link=guid&utm_content=buffer85e0d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Imagen promocional de una 'smart TV'.

A las 11.00 del día 3 de julio, una página web que funciona como un buscador para piratas informáticos indicaba que por lo menos 2.631 cámaras de seguridad y 15.000 televisores inteligentes eran vulnerables a ataques cibernéticos. Los objetos inteligentes que conforman la domótica o la Internet de las Cosas (IoT) también son susceptibles a ataques que van desde el robo de datos privados hasta la usurpación de transferencias de dinero en compras a través del dispositivo. Los expertos alertan de que las amenazas solo van a

aumentar —en 2020, habrá en todo el mundo 20.000 millones de objetos interconectados, según la consultora Gartner— y no existe una regulación que obligue a los fabricantes a añadir a los productos características para proteger al usuario.

Por eso, la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum), formada por 15 organizaciones del sector tecnológico —entre ellas S21sec, McAfee, HP, además de centros académicos como la Universidad Complutense de Madrid— ha creado un sello de ciberseguridad para IoT, que tiene la forma legal de una marca de garantía. "Es similar a un sello de denominación de origen, con varios dominios que abarcan aspectos técnicos, como seguridad del *firmware*, política de actualizaciones a distancia, inspecciones remotas, además de seguridad en las comunicaciones, seguridad por diseño, privacidad desde un punto de vista legal o la garantía de seguridad a lo largo de todo el ciclo de vida del producto", explica Jorge Hurtado, director de ciberseguridad de la consultora Capgemini y líder de la iniciativa.

Para obtener el sello, el fabricante tiene que autoevaluarse a través de un formulario técnico y después someterse a la auditoria de ISMS Forum. La primera empresa en participar de las pruebas, cuenta Hurtado, será Orange, cuyos productos serán autenticados en septiembre. El objetivo de la iniciativa es trasladar el sello al ámbito europeo en un futuro próximo. La intención del ISMS es contar con el Instituto Nacional de Ciberseguridad (Incibe) como interlocutor ante la Unión Europea. Fuentes del Incibe aseguran que el Instituto colaborará con cualquier iniciativa que contribuya a "extender la cultura de la ciberseguridad a todos los ámbitos".

Hurtado sostiene que ese apoyo es importante para diseminar la importancia de la seguridad en internet de los aparatos que los ciudadanos tienen en sus casas. “El problema es que los gobiernos dejan la regulación para el último momento, los ciudadanos no conocen las medidas de seguridad y, como la seguridad no tiene valor añadido y no existe una ley para eso, los fabricantes no la implementan”, lamenta.

Riesgos

Cualquier aparato que utilice un sistema operativo puede estar sujeto a los mismos tipos de amenazas que los ordenadores y *smartphones.* Fuentes del Incibe señalan que cualquier dispositivo conectado a internet puede ser víctima, por ejemplo, del *ransomware,* el *malware* que provocó un ciberataque global en mayo y que en junio volvió a afectar empresas de todo el mundo. "Ya se han dado casos de televisores inteligentes infectados con un *ransomware*", afirman.

Los dispositivos más vulnerables son los que cuentan con cámara y micrófono

El método de infección más común en cualquier dispositivo inteligente, según el Incibe, procede de la instalación de aplicaciones que no provienen de la tienda oficial. Al igual que sucede en los *smartphones*, las aplicaciones de fábrica han pasado una serie de controles, pero al instalar una *app* de un repositorio distinto, el usuario no tiene garantías de que la funcionalidad sea la que se supone que debe de ser, y por lo tanto, el riesgo de infección aumenta.

Los dispositivos con más probabilidad de sufrir un ataque son aquellos que, además de tener sistema operativo con algún tipo de vulnerabilidad, cuentan con cámara y micrófono, ya que en estos casos los ciberdelincuentes podrían grabar lo que dice el usuario y capturar vídeos sin que el mismo fuera consciente. "Las televisiones inteligentes Samsung, por ejemplo, se reservan el derecho de grabar y escuchar conversaciones. Lo informan en un miniapartado de las condiciones de uso que casi ningún usuario lee", señalan desde el Incibe.

Hurtado defiende que diseñar y fabricar objetos seguros no es suficiente y que las empresas deben garantizar la ciberseguridad durante todo el ciclo comercial del producto. "El objetivo del sello es cuidar garantizar que se

cumplan las buenas prácticas durante todo ese ciclo, porque se puede comprar un móvil o un televisor que hoy por hoy es seguro, pero que dentro de un año deja de serlo. Cada día surgen nuevas amenazas", afirma.

CÓMO EL USUARIO PUEDE PROTEGERSE

- No permitir el acceso remoto a ningún dispositivo

- Asegurarse de que el dispositivo está siempre actualizado con la última versión de *firmware* o *software* proporcionada por el fabricante

- Cambiar las contraseñas de los dispositivos y establecer nuevas contraseñas robustas

- Revisar y desactivar cualquier servicio (interfaz web, compartición de ficheros, etc.) o conexión de red mientras no se esté utilizando o siempre que no se necesite

- En el caso de los *wearables*, como una pulsera para monitorizar la actividad física conectada por Bluetooth al móvil, el usuario debe preguntarse si tiene algún mecanismo de cifrado que garantice la confidencialidad de la información, qué permisos necesita la *app* que va a tratar los datos personales o si esta información se va a almacenar en la nube y quién puede acceder a la misma