Blog ECIJA 2.0

20 de Febrero de 2017

Cristina Carrascosa

Abogada de ECIJA

En un mundo *inhackeable*

La semana pasada tenía lugar en Madrid un torneo de debates entornos a los dispositivos conectados (máquinas autónomas) y la posibilidad de implantarles sistemas de decisión éticos. Fue allí donde escuché a un orador afirmar que la solución a las brechas de seguridad que actualmente padece cualquier sistema conectado a la red es "convertirlos en inhackeables". Ojalá.

No es que cambie Internet, lo que cambian son las cosas que están conectadas a él. Hace unos años soñábamos con los coches autónomos, y **hoy hay pacientes que viven gracias a marcapasos inteligentes.** Aumenta el número de dispositivos que pueden o tienen acceso a solicitar un servicio o emprender una acción sin necesidad de intervención humana. Y lo que es peor, la mayoría de usuarios aceptamos los términos y condiciones así como las políticas de privacidad sin apenas prestar atención, como si no tuviesen repercusión alguna sobre nuestra propia intimidad.

Ahora bien, si tal y como expone Cisco, el 95% de empresarios encuestados afirman que **van a lanzar una compañía relacionada con el Internet de las Cosas (IoT) en los próximos tres años,** y el International Data Company estima que un 90% de las empresas que implementen el IoT sufrirán hackeos, podemos concluir que casi cada empresario que decida implantar un sistema de hiperconectivdad terminará enfrentándose a una brecha de seguridad. Descorazonador.

Dentro del esquema expuesto, es claro que el flujo de información de datos es protagonista, no solo entre dispositivos, sino entre estos y servidores. Pero ¿qué tipo de arquitectura hemos elegido para soportar la estructura del Internet de las Cosas? **A priori, debiera ser una que asegure la protección de nuestros datos,** que garantice un nivel adecuado de seguridad y que sea resiliente frente a posibles hackeos. Y ya no sólo porque los consumidores y usuarios tengamos derecho a que se proteja nuestra información, sino porque la regulación relativa a la protección de datos, en fase de inminente cambio, impone regímenes sancionadores cada vez más gravosos. **Exponerse a brechas de seguridad no tiene solo un coste reputacional para las empresas,** sino también económico.

Pensémoslo: si no somos capaces de publicar nuestro número de cuenta en Facebook, ¿por qué sí somos capaces de conformarnos con el nivel de seguridad del IoT actual? **Y lo que es más curioso, detectado un fallo en la seguridad, ¿es volver a lo tradicional la mejor solución?** Hace unos meses conocimos el caso de un hotel austriaco que sufrió el ataque de un Ransomware que bloqueó todas las cerraduras del edificio. La solución que adoptó la empresa fue la de retirarlas, introduciendo de nuevo las antiguas.

Es en este punto del estado de la tecnología del IoT en el que desde múltiples fuentes se plantea el uso de Blockchain. La startup **Chain of Things**, por ejemplo, ha diseñado un Hardware que integra una solución para IoT basada en la Blockchain tras haber identificado los siguientes problemas de arquitectura del mismo: **(i) la escalabilidad del Internet de las Cosas es insostenible, tanto por motivos de seguridad como de interoperabilidad y** (ii) la recogida de datos de miles de dispositivos (se estima que sobre unos 34 billones para 2020) plantea problemas serios en torno a la seguridad de la información y la protección de datos.

Muy interesante es también el proyecto de **Chain of Security de Cisco,** una aproximación a cómo Blockchain ayuda a reparar y solucionar algunos de los mayores problemas del IoT. Y es que, tal y

como afirman desde la empresa, debemos tener en cuenta que la Blockchain de Bitcoin ha sido capaz de mantener su completa integridad sin un solo hackeo durante casi 9 años. Luego, algo podrá aportar. Dicho esto, plantean las siguientes propuestas concretas:

i. Hashing Firmware

El Firmware (programa informático que establece la lógica de más nivel que controla los circuitos electrónicos de un dispositivo) puede registrarse en la Blockchain utilizando el correspondiente hash. **El hash es una función criptográfica, basada en un algoritmo que transforma información legible por ti y por mí**, en una combinación de caracteres de longitud fija (ej: d67H7gJK9s8fhYs6c9asDJ). Básicamente, el hash actúa como certificador de un contenido concreto, como pudiera ser el del Firmware. Por lo tanto, si el estado del mismo cambia en cualquier sentido, por ejemplo a causa de un Malware en el código, el fallo en el hash advertirá de dicho ataque.

ii. Seguridad de la información

Chain of Security aborda también la seguridad de los mensajes enviados entre dispositivos. Su propuesta es la siguiente: el contenido que se envía de uno a otro, se hashea con carácter previo, registrando dicho hash en Blockchain. **La persona que debe recibir esa información, puede igualmente registrar el hash con el que la recibe en la cadena de bloques** de forma que, si coincide, significará que no se ha alterado por el camino. En este punto cabe puntualizar que el tiempo que tarda en generarse un hash es muy reducido, por lo que introducir esta función dentro del sistema de envío de mensajes de cualquier sistema IoT mejoraría la seguridad sin perder eficiencia.

iii. Identidad de dispositivos

El uso de Blockchain para el control de identidad de dispositivos conectados no es nuevo. El propio Gobierno de Estados Unidos invirtió en 2016, 199.000 dólares en Inc, una empresa que utiliza la cadena de bloques para autenticar dispositivos **con el fin de evitar usurpación de identidades y garantizar la integridad de los datos de los usuarios.** Se describen a sí mismos como un motor que audita contenidos y elimina la necesidad de que exista confianza entre las partes.

Una propuesta que ya **defendieron en su día Consensys, Blockstack o KYC-Chain** y con la que la segunda de ellas ha recaudado hasta ahora cuatro millones de dólares.

Puede que, como dijo el orador al que tuve el placer de escuchar, la solución sí sea convertir nuestros dispositivos en "inhackeables". Para ello, tenemos dos opciones: **volver al correo lacrado, o asumir que necesitamos un nuevo estado de la tecnología** y adoptar una diposición dinámica frente a estas nuevas propuestas.

"Los que no puedan mantener el ritmo de la revolución tecnológica se encontrarán con que ellos mismos han quedado obsoletos" ("Riesgo calculado", 1992)