Controlando nuestro alrededor

Como ya hablé en el post anterior, IoT es capaz de poner en riesgo partes muy importantes de nuestras organizaciones o vidas privadas. Es por esto, que las empresas, ya sean grandes, medianas o pequeñas, deben hacer el ejercicio de revisar los sistemas que tienen implantados para detectar los riesgos que pueden llegar a tener, de esta manera, podrán implementar un sistema de controles que les permita mitigar el daño que dichos riesgos puedan llegar a causar. Es en este punto en el que el trabajo del auditor se convierte en vital.

Lo primero que debe hacer la compañía al implantar nuevos sistemas que incluyan dispositivos de IoT es revisarlos de manera que se puedan identificar los riesgos que se van a añadir a la organización y posteriormente implantar un plan de migración de los mismos para minimizar los daños. Entre medias de este proceso entra en juego el papel de la auditoria de seguridad. En esta, los auditores deberán identificar los riesgos que existan y crear unos controles para revisar y mitigar dichos riesgos.

Es en este momento cuando los auditores pueden crear un cuadro de controles a aplicar. En este cuadro se listan los riesgos que se han detectado y los controles que se pueden aplicar a estos. En estos cuadros también se pueden añadir los ámbitos de impacto de dicho riesgo, los responsables de realizar los controles o los puestos/empleados a los que puede afectar de ocurrir. A continuación, tenemos un cuadro en el que se han listado unos de los riesgos más críticos en IoT y los controles que se pueden aplicar: [1]

Riesgo	Control
Ataques físicos al dispositivo	• ¿Es el dispositivo accesible físicamente a cualquier persona? • ¿Está el dispositivo vigilado? • ¿Está el dispositivo monitorizado contra alteraciones hardware?
Manipulación de datos en el dispositivo	• ¿Está el dispositivo cifrado? • ¿Cuenta el dispositivo con un código de autenticación de mensajes o firma digital?
Ataques de interceptación (Man-in-the-middle)	• ¿Está el dispositivo protegido a nivel de protocolo? • ¿Está el dispositivo emparejado?
Manipulación del sistema operativo	• ¿Está el sistema operativo en modo lectura solo? • ¿Está el sistema operativo firmado? • ¿Está el sistema operativo cifrado?
Acceso no autorizado al dispositivo	• ¿Tiene contraseña el dispositivo? ¿Es segura? • ¿Qué puertos están abiertos?
Accesos de terceros	• ¿Tiene el dispositivo programas de terceros instalados? ¿Son seguros? • ¿Tenemos contacto con los desarrolladores de los programas instalados?

Una vez realizada esta tabla la organización será la encargada de asegurarse que dichos controles se van realizando periódicamente y que se reporta si se encuentra alguna anomalía. También tendrá que preparar a los responsables de llevarlos a cabo de manera que sepan realizarlos correctamente.

En este ámbito nos podemos encontrar con frameworks que usan tecnologías muy innovadoras, como blockchain, que prometen crear un sistema de fiabilidad para los dispositivos IoT. En el reto que es crear este framework, se proponen solucionar el problema que existe a la hora de gestionar el acceso a los dispositivos. El framework propone una solución para crear un sistema que conceda y revoque el acceso a los dispositivos mediante una blockchain descentralizada, anónima y segura. Dicho framework, que esta recién sacada del laboratorio, es la prueba de que el campo de IoT está en auge y que se

están utilizando tecnologías muy innovadoras para tratar de crear nuevos sistemas que permitan controlar y hacer más seguros nuestros dispositivos más personales. [2]

Por otra parte, también existen «frameworks» o guías más experimentadas que nos brindan buenos consejos para la compra, implantación e instalación de dispositivos IoT en nuestras empresas, como es el caso de OWASP IoT Project. Mediante este proyecto se quiere ayudar a los fabricantes, desarrolladores y compradores de IoT a prestar atención a los problemas de seguridad más importantes que presentan los dispositivos y como se pueden mitigar o controlar. [3]

El rol del auditor en todo este proceso es vital ya que él o ella será el encargado de crear un sistema preventivo para que la organización a la que ha auditado no tenga ningún problema o sea capaz de controlarlos. Es por esto por lo que los auditores tienen una gran responsabilidad dentro de la empresa ya que su juicio es vital para impedir que ocurran problemas que le cuesten grandes cantidades de dinero a las organizaciones.

Referencias:

[1] <<Cyber risk in an Internet of Things world>>, Deloitte, acceso el 27 de Noviembre de 2017, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html#

[2]<<Internet of Things: Risk and value considerations>>, LinkedIn, acceso el 27 de Noviembre de 2017, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

[3]<<Fairaccess>>, LinkedIn, acceso el 27 de Noviembre de 2017, https://es.slideshare.net/mimolik/fairaccess

<<FairAccess: a new Blockchain-based access control framework for the Internet of Things>>, Oscars Laboratory, acceso el 27 de Noviembre de 2017, http://download.xuebalib.com/xuebalib.com.31639.pdf

<<Internet of Things: Risk and value considerations>>, Isaca, acceso el 27 de Noviembre de 2017, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

<<OWASP Internet of Things Project>>, OWASP, acceso el 27 de Noviembre de 2017, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

IoT, ¿más riesgos que beneficios?

Hace un año presenciamos como la red Mirai[1] formada por dispositivos IoT fue utilizada para realizar un ataque DDoS que dejo sin servicio a un gran proveedor de servicios y de esta manera afecto a grandes páginas web como Reddit o Spotify. Este es solo un ejemplo de las maldades que se pueden conseguir al aprovecharse de las vulnerabilidades que los dispositivos IoT tienen. Estos dispositivos, en algunos casos, están todavía en un estado de madurez muy temprana por lo que crean algunos riesgos en las empresas en las que son colocados. Por ejemplo, tanto en una empresa como en una casa, el nivel de seguridad con el que cuenta un ordenador de sobremesa no se puede comparar con el que dispone un termostato. Esto hace que estos dispositivos se sitúen en una posición muy anterior a los ordenadores tradicionales de hoy en día y que les sea mucho más fácil de vulnerar a las personas que deseen hacerlo. ¿Y cuáles son estos riesgos?

En esta sociedad en la que la información es la moneda de cambio, el primer miedo que tienen las empresas es que esta pueda ser robada, es aquí donde los IoT pueden jugarles una mala pasada. Podemos encontrarnos enemigos en dispositivos de los que nunca sospecharíamos, como puede ser el caso de las impresoras multifunción[2]. Desde hace ya bastantes años, estos dispositivos están conectados a la red de manera que, las personas autorizadas para ello puedan imprimir desde su puesto de trabajo sin que la impresora este físicamente conectada a su ordenador. Si nos paramos a pensar un poco ya podemos deducir un gran problema en este modelo, el robo de información en el proceso de enviar los documentos a la impresora. Los empleados de una empresa tendrían muy sencillo acceder a la configuración de la impresora, si conocen de las credenciales, par de datos que en muchas organizaciones y hogares sigue siendo el predeterminado, y añadir una redirección a su carpeta de los documentos que se envían a la impresora.

Por otra parte, también podemos temer de los vehículos de empresa. Si nuestra empresa subcontrata a otra para adquirir los vehículos durante un tiempo específico y tienen algún tipo de sistema inteligente, el robo de datos puede darse de varias maneras. Los coches, al conectarnos a ellos mediante nuestro smartphone, nos solicitan varios permisos para que puedan desarrollar sus funciones. Es muy bonito pensar que nuestro coche es totalmente seguro y que no va a escuchar las llamadas que realizamos por las manos libres ni guardar un registro de los mensajes y puntos GPS en los que nos hemos detenido.

Tampoco podemos olvidarnos del riesgo que existe de que las personas y los equipos sufran daños físicos. En este ejemplo nos encontramos con un termostato controlado por una aplicación que es vulnerada y cae en manos de gente que no debería. Si el aire acondicionado está colocado en un armario de servidores es muy fácil apagarlo, o activar el modo de calor para que los servidores se quemen y queden inhabilitados. Ahora, si cambiamos el armario de servidores por un despacho con cerradura controlada vía wifi, que también

es vulnerada, el daño puede ser aún mayor.

También nos podemos encontrar con otros riesgos como la posibilidad de que nuestros dispositivos sean controlados desde fuera de nuestra organización como fue el caso de R. Martin[3]. Martin compro un dispositivo que le permitía controlar la puerta del garaje a demanda desde su smartphone. Al ver que la aplicación no le funcionaba, decidió colocar comentarios en la página de Amazon y el foro de la herramienta. Al ver la mala educación de este usuario el creador de la herramienta decidió bloquear ese dispositivo de los servidores, por lo que quedó inutilizado.

Para terminar, nombrar un par de usos más que se han hecho de los dispositivos IoT para fines no correctos. Como ya he nombrado al principio, los dispositivos se pueden utilizar para ser añadidos a redes zombis desde las que lanzar posteriormente ataques DDoS. También se pueden crear puertas traseras a otros dispositivos al conseguir acceder a uno de los que está dentro de la organización, en este caso, el eslabón mas débil de la cadena, el dispositivo IoT menos experimentado.

---

[1] <<El Internet de las Cosas fue usado para el último gran ataque DDoS y no podemos hacer nada para impedirlo>> HiperTextual, acceso el 12 de Noviembre de 2017, https://hipertextual.com/2016/10/mirai-ddos-internet-cosas

[2]<<¿Sabías que hasta las impresoras necesitan medidas de ciberseguridad?>>, Incibe, acceso el 12 de Noviembre de 2017, https://www.incibe.es/protege-tu-empresa/blog/sabias-las-impresoras-necesitan-medidas-ciberseguridad

[3]<<Los riesgos del IoT: un vendedor inutiliza la puerta del garaje de un cliente por una opinión negativa en Amazon>> Gizmodo, acceso el 12 de Noviembre de 2017, http://es.gizmodo.com/los-riesgos-del-iot-un-vendedor-inutiliza-la-puerta-de-1794002365

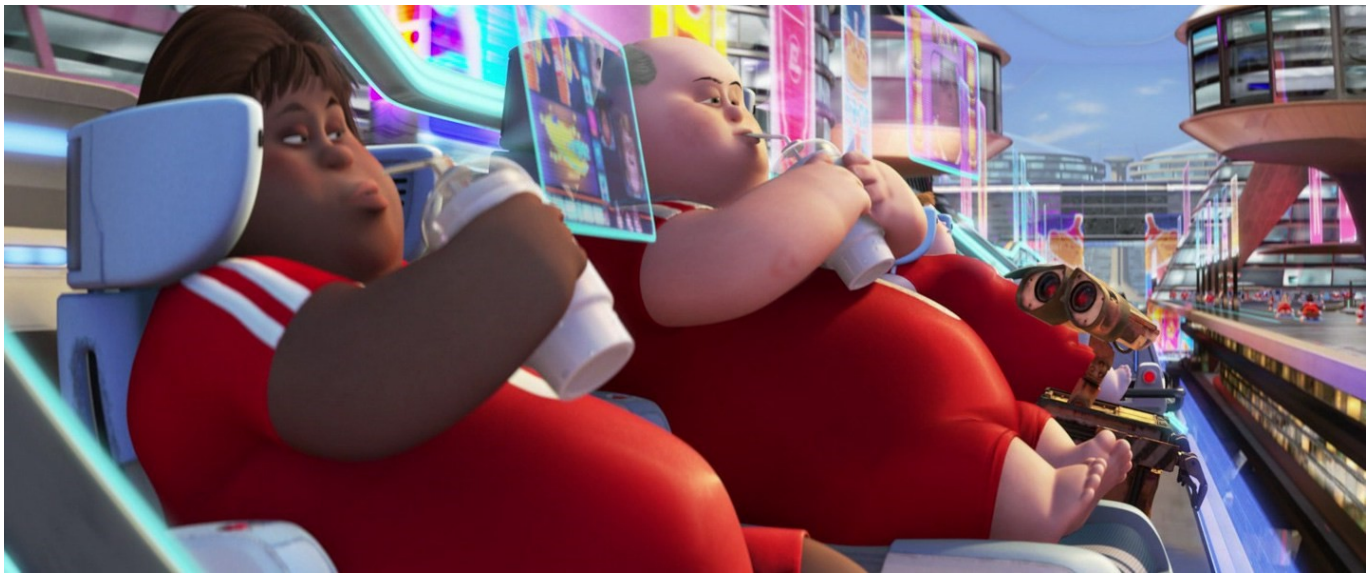
<<La internet de las cosas llega a las empresas: estos son los riesgos que la acompañan>> Panda Security, acceso el 12 de Noviembre de 2017, https://www.pandasecurity.com/spain/mediacenter/seguridad/la-internet-las-cosas-llega-las-empresas/

<<IoT: riesgos del internet de los trastos>>, Incibe, acceso el 12 de Noviembre de 2017, https://www.incibe.es/protege-tu-empresa/blog/iot-riesgos-del-internet-los-trastos

Internet of Things, ¿un concepto tecnológico con un futuro terrorífico?

Pensando lo que escribir en esta última de entrada de este blog, se me pasaban por la cabeza algunos de los términos que hemos nombrado durante las últimas semanas: IoT, BI, Big Data, etc… Palabras que quizás, hace 5 o 10 años ningún profesional de las tecnologías tenía en mente y mucho menos el resto de la población. Pero si nos venimos al día de hoy, ¿quién no sabe de qué van estos temas? Al menos, todo el mundo ha oído algo sobre ellos o los han sufrido cuando han ido al supermercado y les han devuelto 20 tickets con descuentos para colchones (sí, yo tampoco entiendo por qué me ofrecen siempre descuentos en colchones). No voy a ser yo quien me ponga a explicarlos en este momento lo que son estos términos, pero sí que me gustaría hablar acerca de lo que puede llegar a convertirse todo esto, sobre todo en lo que engloba al Internet de las Cosas o *Internet of Things*.

Vivimos en una sociedad en la que podemos encontrar cualquier objeto conectado, desde los teléfonos móviles que todos llevamos en nuestros bolsillos a incluso los electrodomésticos de nuestro hogar (nunca entenderé para que quiero una nevera con wifi). Poco a poco, nos vamos haciendo más dependientes de ellos, nos compramos pulseras o relojes que nos monitorizan, nos gusta actualizar continuamente nuestras redes sociales, ¡e incluso soñamos con un coche autónomo! Y muchas veces, esta dependencia puede llegar a ser muy peligrosa, no dándote cuenta hasta que ya es demasiado tarde. Al pensar en dependencia me viene a la cabeza esta escena de la película Wall-E:



En esta, los humanos se han convertido en algo inútil y totalmente dependiente de las tecnologías y las máquinas que lo rodean. Sé que es algo muy exagerado, al final es una película para niños, pero, ¿no creéis que en parte tendemos a algo similar a eso? Cada uno tenemos nuestros dispositivos personalizados a nuestros gustos y cada vez nos conocerán más, solo habrá que

juntar muchos cabos y dejar que el tiempo pase para que esto suceda.

Nosotros, que somos más técnicos vemos todo esto del BI o el IoT como algo que va a acabar instaurándose en nuestras vidas como algo común antes o después y con lo que vamos a tener que convivir. Pero, ¿alguno os habéis planteado como ven el resto de las personas estas temáticas? Ayer estuve con un amigo cenando y se me ocurrió la brillante idea de sacar este tema de conversación. ¿Os imagináis cual es la sensación que el resto de la gente tiene de todo esto? Lo podría describir con una sola palabra: **Miedo**. A mucha gente le da miedo pensar en lo que se puede convertir la sociedad con los avances que hay actualmente. ¿Sería posible una rebelión de las máquinas emulando aquella película de *Terminator*? ¿Veremos alguna vez una inteligencia artificial con el poder de *Skynet?* Creo que estamos aún lejos de eso, pero no creo que vayamos mal encaminados.

Os quiero contar una pequeña anécdota que me ocurrió durante la cena de ayer. Fuimos a un restaurante de un centro comercial. A la hora de pagar, como yo tengo un Apple Watch, le dije a la camarera que pagaría con tarjeta utilizando el reloj que se encontraba en mi muñeca. En ese momento, el simple hecho de no entregarle una tarjeta para pagar la dejó tan bloqueada que no sabía lo que hacer. Yo intenté explicárselo, pero ella tuvo que preguntarle a una compañera si eso era posible realmente, ya que, no se creía que eso se pudiera hacer. Finalmente, al acercar mi muñeca al dispositivo de pago se quedó sorprendida, como si de una brujería extraña se tratase. Este es realmente uno de los problemas del IoT. Por mucho que se evolucione tecnológicamente, si la sociedad no evoluciona en paralelo, va a ser mucho mas complicado encontrar nuevos avances para nuestro día a día.

Para ir finalizando este último post, yo no acostumbro a recomendar cosas normalmente, pero en esta ocasión voy a hacer una excepción. Creo que hay una serie en la que podemos ver perfectamente las consecuencias que puede tener esta inclusión de la tecnología en nuestras vidas y realmente, las historias que se cuentan puede llegar a dar miedo. Esta serie, que quizás muchos de vosotros habréis visto, es **Black Mirror.** En cada capítulo de esta, se realiza una crítica a como la tecnología puede llegar a sacar lo peor de nosotros desde enfoques como la rapidez en la que se difunde la información, los medios de entretenimiento y su deshumanización o las redes sociales .

Como conclusión, me gustaría decir que creo que somos muy afortunados de vivir en estos tiempos, hemos visto con nuestros propios ojos una evolución brutal en la tecnología y además somos los encargados de que esto siga adelante. Creo que uno de los primeros pasos que se deben hacer es el concienciar a la gente de que las tecnologías están ahí para facilitarnos la vida, y en ningún caso para perjudicarnos. Estoy seguro que nada será en unos años tal y como lo conocemos actualmente, por lo que solo podemos disfrutar del camino que vamos a hacer y seguir soñando con lo que vendrá, que no dudo que al menos, nos sorprenderá.

IoT sí, pero IoT segura

Y llegamos al último Post de la asignatura. Que rápido han pasado estos meses. *¿Y de que puedo hablar en este Post?* Bueno pues me parece apropiado tratar algunos aspectos, que a mi entender son esenciales en el mundo de Internet of Things (**IoT**). Por supuesto que IoT trae consigo grandes avances y aspectos positivos que seguramente cambien nuestro concepto de las cosas, pero debemos estar alerta y no dejar a un lado todo el universo de riesgos que esto implica. Con esto no quiero ser alarmista pero es algo que creo que es importante tratar y que seguramente nos ayude a visualizar nuevos enfoques de la materia y a nuestro aprendizaje, que para eso estamos cursando un máster.

Bueno pues IoT es un concepto que nos rodea, pero que ha surgido sin hacer demasiado ruido. Desde luego la prensa y los medios de comunicación están haciendo eco actualmente, a pesar de ser un concepto con relativa antigüedad (los expertos datan su aparición entre los años 2008 y 2009). Podemos leer noticias relativamente recientes que señalan que, en los próximos años, será algo esencial en la sociedad y nos hablan de porcentajes y porcentajes de implantación en las empresas y en la industria. Y seguramente tengan toda la razón, pero como esto se descontrole… se puede liar una muy gorda.

IoT implica una sociedad hiperconectada, en la que cualquier dispositivo estará conectado a través de Internet, de manera que convertirán nuestra actividad diaria en información, se distribuirá dicha información por la red e interactuaran con ella. Esto implica un incremento del número de dispositivos interconectados, por ello es necesario considerar la necesidad de establecer acciones de seguridad que prevengan de intrusiones no autorizadas y el uso de ellos como origen de ataques. *¿Qué tipo de riesgos implica IoT?* Fundamentalmente estos:

- Interferencia en la privacidad ya que la información recogida, procesada y almacenada puede tener un fin ilícito.
- Proliferación de tecnologías que traen consigo un incremento de fallos

al interconectar dispositivos con tecnológicas incompatibles y en consecuencia incremento de costes para las organizaciones.
- Inexistencia de estándares de fabricación segura.
- Recogida de datos no autorizada que pone en riesgo los derechos de los ciudadanos en cuanto al acceso y uso de sus datos debido a que no siempre se usan de forma autorizada y consentida.

Junto con estos riesgos, debemos ser conscientes de los escasos mecanismos de protección disponibles en estos entornos. Debido a esto, el rol de los reguladores actualmente es fundamental. La complejidad del ecosistema IoT hace necesario el establecimiento y cumplimiento de una normativa que vele por los intereses tanto de las organizaciones como de los usuarios que, ya sea voluntaria o involuntariamente, participan en la recopilación y tratamiento de información de todos estos dispositivos. Pero bien es cierto, que la implantación de esta regulación debe afectar lo menos posible al desarrollo y avance de dichas tecnologías.

Además, la participación de cada uno de los gobiernos será clave, ya que puede generar una mayor sensación de seguridad y confianza a los consumidores. El usuario debe percibir que la información personal extraída por cada dispositivo conectado, será utilizada en su favor y no en su contra, además de aportarle valor. Esta claro que si los usuarios no ofrecen la confianza a este tipo de tecnologías por los riesgos que conllevan, todas las previsiones relacionadas con IoT probablemente no se cumplirán y desde luego su implantación en la sociedad será mucho más lenta y costosa.

En conclusión y para finalizar este Post, es importante destacar que el desarrollo de IoT supone un avance en la sociedad bastante notable. Algunos se atreven a decir que probablemente sea la cuarta revolución industrial. Lo que no cabe duda es que las posibilidades de IoT son inimaginables ya que tendremos a nuestro alcance información de prácticamente todo. Y la información como bien es sabido, es poder. Pero no podemos dejar a un lado todos los riesgos que ello conlleva. Sin una regulación apropiada, el usuario no sentirá la confianza necesaria para aceptar estas nuevas tecnologías. Tanto la privacidad como la seguridad, afectan directamente en este aspecto, y sin confianza, el usuario no está dispuesto a ofrecer su información, y sin información IoT deja de tener sentido. Por lo tanto, desarrollemos tecnologías IoT, pero que sean IoTs seguras y generen una sensación de seguridad en cada uno de los usuarios que las utilicen.

Ha sido un placer escribir estos Posts para la asignatura. Saludos amigos.

La seguridad en el Internet Of Things

El IoT es el siguiente paso en la tecnología, asimilar esta en la sociedad

proporcionando servicios puntuales allí donde se necesitan. Esto requeriría de una masificación de los dispositivos conectados a internet, directamente conectado al wifi, con zigbee, usando bluetooth, beacons o de otras muchas formas.

Pero tenemos un problema al respecto de esta masificación. Si ya hay graves fallos de seguridad a día de hoy en empresas cuya responsabilidad es cuidar de esos datos y que no se divulguen, hasta que punto puede llegar si creamos un montón de dispositivos, sin garantía de calidad y los conectamos a lo largo de toda nuestra ciudad. El ejemplo más reciente del riesgo que supone lo tenemos con Yahoo y la filtración masiva de las cuentas de sus usuarios. Ahora supongamos que una persona, empresa o institución pública decide ahorrar dinero a la hora de comprar estos aparatos para su entorno comprando productos de un precio muy bajo y sin garantía de seguridad. La amenaza puede ser importante, cualquier dispositivo que no tenga una correcta implementación puede ser susceptible de ser atacado ya no solo por hackers malintencionados profesionales, sino por cualquiera que estando un poco metido dentro del mundillo siga los defectos de los diversos productos.

La pregunta que surge es como podemos garantizar la seguridad. Bueno pues la responsabilidad no va a ser solo del que hace el producto, también es nuestra responsabilidad a la hora de comprar un dispositivo que vamos a conectar a la red asegurarnos que tiene unas correctas garantías de seguridad y pensar en si confiamos de verdad en el. ¿Confiamos en esa cámara de seguridad conectada a internet comprada en Alliexpress? Yo personalmente no.

Como desarrolladores de estos dispositivos tenemos una responsabilidad con nuestros clientes. Tenemos que garantizar que sus dispositivos no sean vulnerables. Una forma de garantizar las comunicaciones seguras es implementar un cifrado en dichas comunicaciones. Entre los algoritmos de cifrado tenemos el PRESENT, que es un algoritmo ligero de cifrado, se considera que no hace falta en el IoT el cifrado de grandes masas de datos. Otro ejemplo es TRIVIUM, también un algoritmo de cifrado ligero. En este caso se basa en un registro de desplazamiento cíclico para su funcionamiento, tiene el propósito de ser eficiente y de dar un buen resultado de seguridad.

La seguridad de nuestro sistema también se puede ver vulnerada por el hardware que adquirimos, en un artículo interesante de IEEE se analiza un caso en el que se reemplazo una pieza por otra no autorizada para detección de hielo en un avión P-8 Poseidon. Analizando el problema se descubrió que esta pieza provenía de China. Este caso es especialmente interesante porque se centra en la seguridad en el ámbito militar donde la incorporación de una pieza no autorizada puede provocar fallos de seguridad y brechas que pueden ser aprovechadas por el enemigo.

Pero este es un ejemplo orientado a la industria militar con una serie de requisitos que no todos tenemos, aunque no es la primera vez que en nuestro día a día podemos tener brechas de seguridad que desconozcamos por culpa de haber adquirido un producto cuyas medidas de seguridad no eran lo suficientemente estrictas. Un ejemplo es el caso de los primeros lectores de huellas para móviles samsung que tenían una brecha de seguridad que permitían a otras aplicaciones acceder a ellas.

Homekit

Por último vamos a volver al foco del IoT y la seguridad, pero en el ámbito domestico. Personalmente, una de las apuestas que me resulta más interesante en el IoT es Apple Homekit, sin embargo, este parece estar retrasándose a la hora de surgir productos compatibles con el estándar por un motivo. Según se dice tiene unos requisitos de seguridad tan fuertes que está dificultando el desarrollo de fabricantes no acostumbrados a estos niveles de seguridad. Homekit hace uso de unas claves de cifrado de 3072 bits, curve25519, firmas digitales e intercambio de claves cifradas. Tanto para su conexión por WiFi como por Bluetooth LE. Según parece el problema surge en algunos dispositivos Bluetooth LE que genera un retardo demasiado grande, esto se ha conseguido solucionar incorporando más RAM, pero encareciendo el producto. Sin embargo en un mundo tan inseguro, la existencia de un protocolo que nos de estas garantías y sustentado por un gigante como apple es evidentemente una buena noticia.

IEEE, Pass-IoT: A Platform for Studying Security, Privacy and Trust in IoT, 25/10/2016

IEEE, Defense Systems and IoT: Security Issues in an Era of Distributed Command and Control, 25/10/2016

Xataka, http://www.xatakandroid.com/seguridad/se-encuentra-un-bug-con-el-que-se-pueden-clonar-las-huellas-dactilares-en-los-galaxy-s5, 25/10/2016

Ipadizate, http://www.ipadizate.es/2015/07/26/homekit-fabricantes-accesorios-quejan-seguridad-apple/, 25/10/2016

Internet of the things: Interactividad sí, pero solo con mis amigos.

Cada vez se oye hablar más del Internet of Things (IoT) y de las bondades que trae consigo el uso de esta tecnología. Teléfonos, televisiones, relojes, casas… todos estos y más elementos han cambiado mucho en los últimos 10 años pero el cambio más revolucionario que han tenido en común ha sido sin lugar a dudas la posibilidad de conectarlos a la red y poder así interactuar entre otros dispositivos, ofreciendo nuevos servicios y ventajas.

Cada vez existen nuevas tecnologías y protocolos que facilitan y mejoran la conectividad entre dispositivos tales como el Bluetooth LE, WiFi Direct, Zigbee, etc. Sin embargo, los fabricantes han decidido crean un "ecosistema" de dispositivos en los que solo puedan interactuar entre ellos éstos están limitados por plataforma. Aún hoy en día si un usuario de Android quiere enviar un fichero a otro usuario de iOS tiene que utilizar herramientas de terceros para realizar dicha función, dado que el sistema operativo corta la conexión cuando detecta que dicho dispositivo no pertenece a la "familia".

Este ejemplo no es un saco aislado en telefonía, también ocurre con los "wereables", sistemas de domótica, etc. La raíz del problema está en que no existe un estándar para entablar comunicaciones entre los distintos dispositivos es por eso que los fabricantes realizan implementaciones baratas de un protocolo de handshaking propietario y lanzan sus productos al mercado, al fin y al cabo, no hay mejor forma para entablar un estándar que adquirir la mayor cuota de mercado.

Lamentablemente esta es la etapa que nos toca vivir. Cabe destacar que las grandes empresas del sector como Intel, Qualcomm, Samsung, Microsoft, entre muchos otros ya han entablado conversaciones y han generado asociaciones que tienen como objetivo la creación de estandares que solventen este y muchos otros problemas.

Una vez concluyan se definan las especificaciones y se lancen estos nuevos dispositivos bajo la certificación del estándar se podrán llevar a cabo proyectos de gran envergadura como las Smart Cities y solventar las limitaciones a las que se enfrentan a día de hoy.

Sin lugar a dudas esta tecnología supondrá una revolución y supondrá un cambio drástico en la forma con la que interactuamos con las "cosas".

Internet of Things

El Internet de las cosas o Internet of Things es un término del que cada vez se oye hablar más, pero a pesar de ser un concepto abstracto, su propio nombre nos deja bastante claro su significado: objetos cotidianos que se conectan a internet. Sin embargo, este concepto llega mucho más allá.

¿En qué consiste el Internet of Things?

Como idea base, el objetivo que se persigue es hacer más interactivos los objetos que utilizamos en nuestra vida diaria. Un ejemplo de los avances que se han logrado hasta hoy, sin darnos cuenta, serían los hogares inteligentes, en los que muchos objetos ya cuentan con conectividad y hacen nuestras vidas más fáciles.

El Internet de las cosas potencia objetos que antiguamente se conectaban mediante circuito cerrado, como comunicadores, cámaras, sensores, y demás, y les permite comunicarse globalmente mediante el uso de la red.

Estos objetos se valen de sistemas embebidos, es decir, hardware especializado que les permite no solo la conectividad al Internet, sino también programar eventos específicos en función de las tareas que le sean dictadas remotamente.

A la hora de clasificar los objetos conectados a internet, vemos que no hay un tipo específico de objetos que cuenten con esta característica, pero podrían clasificarse como objetos que funcionan como sensores o como actuadores. Sin embargo, vemos que hay objetos que cumplen ambas características simultáneamente.

La clave de estos objetos es la operación a distancia, de esta forma se puede acceder a ellos y ordenarles tareas determinadas. Por otro lado, también pueden contactar con un servidor externo y enviar los datos que recoja.

¿Cuándo estará entre nosotros?

Cuando hablamos de este concepto, que aparentemente es nuevo, nos preguntamos cuándo estará integrado en nuestras vidas diarias, cuando sin darnos cuenta, ya lo está desde hace un tiempo.

Para dar evidencia de esta afirmación, vamos a nombrar ejemplos en diferentes industrias que ya cuentan con esta tecnología:

- **La industria 4.0:** Este punto hace referencia a la industria de

producción en masa, en la que toda la maquinaria y los procesos de fabricación están conectados a Internet e interconectados entre sí, lo que permite centralizar el control del proceso, así como obtener una visión global del mismo.

- **Control de infraestructura urbana:** Algunos ejemplos sobre este sector serían el control de semáforos, de puentes o de vías de tren, o la instalación de cámaras urbanas. Cada vez más ciudades implementan este tipo de infraestructuras basadas en el Internet de las Cosas que permiten monitorear el correcto funcionamiento de sus estructuras, además de adaptar más flexiblemente su funcionamiento ante nuevos eventos.

Big data o Big….Brother

Hace unos días leía en la revista **XLSemanal** un artículo relacionado con un tema que nos viene como anillo al dedo. El titular era:

> **¿Se dejaría vigilar todo el tiempo en el trabajo?**

Pensémoslo 5 segundos. [. . . . .] Seguramente nuestra respuesta, así a bote pronto sería **NO**. En el trabajo o en cualquier lugar, lo de sentirnos «

espiados» no termina de resultarnos cómodos. Pero… ¿tampoco nos sentimos así en las **redes sociales**, **asistentes personales**, **pulseras de actividad**, diferentes **aplicaciones móviles** y otras fuentes de captación de nuestra información? Puede parecer que no pero parándonos a pensar un momento nos daremos cuenta de que estamos **bastante más vigilados** de lo que seguramente nos gustaría…

Sin embargo, también es cierto que debido a todos los **patrones** que se identifican con los análisis de **Big Data**, se pueden llevar a cabo muchísimas **prácticas beneficiosas** para muchas organizaciones, desde hospitales con sus pacientes hasta **recomendaciones personales** de cualquier cosa que nos imaginemos. El caso que mostraba el artículo

 de la revista anteriormente nombrada era precisamente un hospital estadounidense en el que los profesionales están **monitorizados** en **toda** su **jornada laboral**. Todo con unos **objetivos** claros: minimizar costes. Cada persona lleva un **receptor** en el que se puede saber en todo momento **dónde está, cuánto tiempo pasa en el baño, en la sala de café,** etc. Por supuesto, el dispositivo no es para nada obligatorio, aunque todos lo llevan.

Otra parte que me ha parecido curiosa es que **Big Data** está (o estará aún más) bastante relacionada con **recursos humanos** de la empresa. A día de hoy, hay aplicaciones que son utilizadas para contratar a los empleados que mediante una **entrevista** hecha por ordenador de unos 15 minutos, la máquina **revela informes** con información de carácter personal: dotes de mando, preocupaciones, aficionado al riesgo, y otros datos muy interesantes para los jefes de personal. El **análisis** es **llamativo** por el hecho de que no se fija en las respuestas dadas, sino en el **volumen de la voz**, la **velocidad del habla**, el **número de negaciones o lo largas que son sus pausas**. Los partidarios del Big Data aseguran que con este tipo de mecanismos y otros parecidos, los despidos y contratos serán **más objetivos**.

Lo que está claro es que nos movemos en una era en la que **Big Data y similares están en auge**. Nuestras ciudades y «artilugios» más comunes se están convirtiendo en inteligentes (Smart cities, IoT, …), nuestra información es recopilada para una mejor experiencia en la red, para predecir acontecimientos, recomendarnos productos, etc. Podemos sentirnos como si realmente viviésemos en un **Gran Hermano global**, pero… si nos hace más mal que bien podríamos desconectar nuestros Smartphones, no tener Facebook, no utilizar tarjetas de crédito, … Todo es opcional.

Para finalizar el **post** y el **año** os dejo con un artículo en el que se muestra cómo cambiará nuestra vida en los próximos años con unos ejemplos.

Network Connected Devices (Internet of Things): Estándares y beneficios

Estándares

Si bien llevamos más de una década conviviendo con el IoT no fue hasta el 2013 cuando se comenzaron a nombrar los estándares. Sin embargo, mientras surgen consorcios y alianzas la industria no permanece a la espera y se genera una lucha entre las organizaciones por establecer cuál de las tecnologías fabricadas por cada casa prevalecerá en el mercado, tal y como pasó en su día con *La guerra de los navegadores* o *La guerra del formato óptico para la alta definición*.

Muchas veces estas guerras se ganan o se pierden antes incluso de que se establezca un estándar. En el 2013 se crearon ciertas alianzas entre los líderes del sector y se comenzaron a producir dispositivos con certificación que avalaba que cumplian con las especificaciones que se había decretado en dichos estandares.

El IoT implica establecer un vínculo entre los dispositivos interconectados, con los que en la mayoría de los casos no hubiera sido posible establecer una conexión. Por otra parte, involucra la gestión de esos dispositivos y la creación de aplicaciones que establecen una relación entre ellos para realizar tareas o funciones que no serían posibles de completar por ellos mismos como individuos. Todos los dispositivos del IoT están destinados a poder comunicarse entre ellos, sin embargo a día de hoy no existe ningún estándar formalizado o universal que permita llevar a cabo esta virtud.

Las Alianzas formadas intentan solventar esta problemática, así como

establecer unas directrices de desarrollo, con el fin de reducir el alto porcentaje de dispositivos vulnerables que se han producido como resultado de no tener definida una lista de buenas prácticas a seguir en función de la tecnología escogida para el desarrollo de los dispositivos.

Las alianzas resultantes que caben destacar son las siguientes:

AllSeen Alliance

Este grupo es uno de los que más adeptos está reclutando, comenzó en Diciembre de 2013 formado por Qualcomm, Cisco Systems, Panasonic y otras empresas relacionadas con el sector electrónico. Desde entonces se ha cuadriplicado con 100 miembros.

El protocolo AllJoyn primero diseñado por Qualcomm ahora gestionado por la fundación Linux, es el estándar que originó la AllSeen Alliance. Alljoy es un *framework open-source* que gestiona la conectividad y las operaciones de la capa de servicio para los dispositivos IoT con el objetivo de "*crear productos interoperables que sean capaces de buscar, conectarse e interactuar directamente con dispositivos, sistemas y servicios cercanos independientemente de la capa de transporte, tipo de dispositivo, plataforma, sistema operativo o marca*" .

Open Interconnect Consortium

Open Interconnect Consortium (OIC) fue fundada por Intel en Julio, apoyada por fabricantes que incluyen a la propia Intel, Samsung y Dell. El objetivo de esta asociación es definir un conjunto de especificaciones que ayuden a los dispositivos a buscarse y a trabajar entre ellos.

El *framework open-source* cubre las funciones tales como la búsqueda, comunicación y intercambio de datos. Este *framework* hace competencia directa al propio desarrollado por AllSeen Alliance, AllJoyn que ha resultado en disputas entre los grupos por asuntos de propiedad intelectual.

Thread Group

Fue fundada por compañías como ARM, Samsung y por la reciente adquisición de Google en termostatos y alarmas de incendios, Nest, al mismo tiempo que el OIC. El objetivo de esta alianza es crear un *framework* ambicioso centrado en la comunicación inalámbrica que gestiona la red, consumo energético, la seguridad y la compatibilidad de productos. Cabe destacar que cada dispositivo con certificación Thread dispone de una dirección IPv6, facilitando así muchos problemas de redes.

La ZigBee Alliance se unió recientemente a este grupo, lo que supone que ofrecerá una mayor visibilidad del protocolo para el estándar.

En lo que respecta a su relación con el protocolo AllJoy y el estándar de OIC, a diferencia de estos últimos Thread es un protocolo de radio, lo que posibilita la coexistencia de estas alianzas pacíficamente.

Industrial Internet Consortium

The Industrial Internet Consortium (IIC) fue fundada en Marzo de 2014, su labor se centra en el desarrollo de buenas prácticas relacionadas con las aplicaciones industriales del IoT. Le apoyan principalmente grandes empresas como GE, IBM, Cisco, AT&T e Intel.

La IIC ha comunicado que no está desarrollando un estándar por sí misma, sino que está trabajando en agrupar a las organizaciones y la tecnología necesaria para acelerar el crecimiento del Internet industrial mediante la identificación, agrupación y promoción de buenas prácticas.

IEEE P2413

El Institute of Electrical and Electronics Engineers (IEEE) ha formado un grupo para establecer un poco de orden en lo que se refiere a las especificaciones del IoT, siendo estas desarrolladas por el consorcio. Actualmente además de existir 350 estandares que pueden aplicarse al IoT, existe un borrador del estándar aunque se estima que el estándar se finalice a lo largo del 2016. Mientras tanto, el grupo está estableciendo relaciones con otros fabricantes y otros organismos relacionados con el IoT como el IIC y oneM2M entre otros.

ITU-T SG20

Grupo establecido en Junio de 2015. La International Telecommunication Union está en proceso de desarrollar un estándar que no solo cubre al IoT, sino tambien a las Smart Cities and Communities (SC&C). El estándar SG20 tiene el objetivo permitir el desarrollo coordinado de las tecnologías de IoT, incluyendo las comunicaciones maquina a maquina y las redes ubicuas de sensores.

OneM2M

Formada en 2012 y con el apoyo de siete de las organizaciones de desarrolladoras de estándares más prestigiosas del mundo, oneM2M es una organización global que tiene como objetivo crear un estándar escalable e interoperable para la comunicación de dispositivos y servicios usadas en aplicaciones M2M y el IoT. Ofrece un estándar que da soporte a aplicaciones y servicios tales como la red eléctrica inteligente, el coche inteligente, domótica, seguridad pública y salud.

Apple

Apple ha desarrollado su *framework* HomeKit, para comunicarse y controlar los acessorios conectados en el hogar del usuario. Como es de esperar, no es un estándar sino la “forma de hacer” que tiene Apple. Los desarrolladores pueden decidir si usarlo o mantenerse al margen.

Aunque el *framework* ya está disponible, no está teniendo el éxito esperado

debido a la insistencia de Apple por usar una encriptación de 3072 bits y chips certificados por ellos mismos en los dispositivos que usen WiFi o Bluetooth. Esto supone que los desarrolladores tengan que rediseñar su línea de productos si quieren soportar el HomeKit.

Por otra parte, ya están saliendo al mercado dispositivos que soportan el HomeKit y nada fomenta más un estándar que productos en las estanterías de una tienda.

Beneficios

Hemos visto como el uso del IoT supone nuevos riesgos, el objetivo de las organizaciones consiste en definir los escenarios en los que los beneficios de la implantación sean mayores a estos nuevos riesgos o al menos alcancen un equilibrio.

Es innegable que el IoT ofrece beneficio y valor añadido a las organizaciones, y estas no pueden ignorar estos hechos. Entre todos los beneficios que otorga el IoT caben destacar los siguientes:

- **Reducción de costes: Los costes pueden reducirse debido a un aumento en la eficiencia de los activos, procesos y mejoras de servicio. *General Electric* estima que la mínima mejora en los procesos que permitan una reducción en el consumo de energético, puede suponer un ahorro de miles de millones.**
- **Aumento de la eficiencia de uso de los activos:** Con la mejora de los procesos y la monitorización de los recursos, la industria se puede beneficiar de las ventajas de la visualización en tiempo real de sus activos pudiendo localizarlos o realizar mantenimientos preventivos de piezas críticas mejorando el procesamiento de los productos.
- **Aumento de la eficiencia de los procesos:** La introducción de los procesos de monitorización en tiempo real mejora la toma de decisiones, minimiza la intervención humana y reduce, por ello, los costes operativos y totales.
- **Aumento de la productividad:** Mejora la productividad de la organización gracias a los entrenamientos *just-in-time* solventando la escasez de habilidades disponibles frente a las necesitadas, mejorando la eficiencia laboral.

Network Connected Devices (Internet of Things): Riesgos (parte 2, Final)

Mitigación y Priorización

En este apartado se analizará y se profundizará más en cada uno de los riesgos descritos en la subsecciones anteriores, finalizando con una tabla que contendrá un resumen con el impacto del riesgo y su probabilidad.

Salud y Seguridad

Los riesgos de salud y seguridad están relacionados estrechamente con el negocio. El impacto en todos los casos es alto, dado que involucra vidas humanas o repercute en el medio ambiente. La probabilidad de que se dé depende del negocio en cuestión y de las funciones de las que se encargue el dispositivo IoT.

Este riesgo está sensiblemente relacionado al resto de los riesgos de negocio, operacionales y técnicos ya que cualquiera de estos puede comprometer tanto a la salud como a la seguridad.

Para mitigar este riesgo es necesario realizar un modelo holístico para prevenir, detectar y corregir las posibles vulnerabilidades del dispositivo. Este modelo consiste en identificar a los *Stakeholders* para poder definir el ámbito de uso. Una vez definido esto, se realiza una evaluación de los riesgos para identificar las posibles vulnerabilidades y determinar el impacto de negocio que supondría que ocurrieran dichos riesgos. A continuación, es necesario desarrollar un plan de contingencia que garantice la seguridad y el buen funcionamiento del dispositivo. Por último, y no menos importante, se requiere realizar un proceso de monitorización continua para salvaguardar y/u obtener evidencias de que todo va según lo establecido y realizando siempre un análisis actualizado de las posibles vulnerabilidades que pudieran comprometer la seguridad del dispositivo.

Cumplimiento de la regulación

Los riesgos de cumplimiento de regulación dependen del país en el que resida la sede de la organización y de la legislación de los países en los que ofrezca servicio.

Una organización se enfrenta a estos riesgos, mayormente, cuando se producen cambios en la ley o la regulación que afectan a la industria o un negocio, que pueden implicar cambios en los procesos, *frameworks* y costes. Dependiendo del negocio, estos cambios pueden suponer el cierre del mismo por lo que supone un impacto alto, aunque, con una buena gestión, es dificil que esto ocurra por lo que la probabilidad resultante es media.

Para mitigar los posibles riesgos referentes al cumplimiento de la regulación es necesario hacer una gestión de la misma. Ésta casi siempre va de la mano

de una auditoría, ya sea externa o interna, en la que se definirá qué rasgos de la regulación afectan más a la empresa. Con esto, se exigirán las evidencias que demuestran que se cumple con la regulación para asegurarse que todo funciona como lo exige la ley. Este proceso requerirá realizar una monitorización periódica para controlar los posibles cambios jurídicos que puedan surgir.

Privacidad del usuario

La privacidad del usuario está ligada a las vulnerabilidades del dispositivo, leyes de los países en los que se opere y de cómo la organización gestione los datos de carácter personal. Teniendo en cuenta que más del 90% de dispositivos contiene información sensible y de que de éstos el 70% presenta algún tipo de vulnerabilidad, la probabilidad de este riesgo es alta. El impacto representa una sanción económica por parte del órgano judicial, así como una pérdida de confianza de los usuarios, por lo que supone que el impacto sea alto.

Para mitigar estos riesgos, por una parte el usuario ha de estar concienciado y entender lo que suponen los siguientes factores del IoT:

- La interoperatividad entre dispositivos y tecnologías.
- Como la información se transmite entre dispositivos y aplicaciones.
- Los términos “privacidad” y “condiciones de uso” de los dispositivos.
- El riesgo de compartir información entre los dispositivos y las redes sociales.
- La implicación de vincular cuentas presentes en las redes sociales.

Conociendo estos factores el usuario entenderá cuales son sus derechos y se pensará dos veces qué tipo de contenido comparte en la red.

Por otra parte, la organización debe cumplir según la regulación de los países en los que opere. Se establecerán las responsabilidades de las organizaciones externas que tengan acceso a dicha información y se llevarán a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Costes inesperados

El hacer uso de esta nueva tecnología supone una implantación y un desarrollo más lento. Por otra parte, un cambio en los estándares exigiría una nueva planificación, modificación de fechas de entregas y una inversión de fondos adicionales. De todas formas, haciendo un análisis de los riesgos, no serán tan arriesgados como para poner en peligro la organización. Es por ello que la probabilidad de este riesgo es media y el impacto es bajo.

En estos casos, es aconsejable seguir las novedades que realizan los organismos responsables del estándar para poder planificar de antemano cualquier imprevisto y asignar un margen de costes para solventar o mitigar dichos imprevistos.

Acceso inadecuado

Una vulnerabilidad en el dispositivo, puede implicar un acceso inadecuado al mismo. Por otra parte, con la reducción de coste de los dispositivos, cada vez son más los que se sitúan en áreas desprotegidas exponiendo, físicamente, la integridad del sistema. Debido al alto número de dispositivos que presentan vulnerabilidades y a la creciente disposición de dispositivos sin monitorización, la probabilidad de acceso inadecuado es alta, siendo su impacto alto dado a que pueden afectar tanto a la salud y seguridad como a la privacidad de la información del usuario.

Para mitigar este riesgo, es necesario restringir el acceso al dispositivo, bien físicamente o mediante un sistema de autenticación y autorización lo suficientemente robusto. Por otra parte, será necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Uso inapropiado

Las vulnerabilidades del dispositivo implican que usuarios no autorizados puedan acceder a los procesos de los dispositivos y alterar su funcionamiento. Por otra parte, los usuarios, como tal, pueden utilizar el dispositivo o componentes del mismo con fines para los que no fueron diseñados. En el primer caso el riesgo es alto, dado que pueden comprometer la salud, la seguridad y la privacidad de los datos. Debido al alto número de dispositivos que presentan vulnerabilidades y a la creciente existencia de los mismos, sin monitorización, la probabilidad de que se dé un uso inadecuado del dispositivo es alta.

Para mitigar este riesgo, sobre el uso inadecuado por parte del usuario, es necesario definir una política de uso que exhuma de responsabilidad a la organización de su uso indebido. Por otra parte, será necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Rendimiento

El rendimiento se puede ver alterado por un uso inapropiado de los recursos causado por una vulnerabilidad del dispositivo o por un mal diseño, esta última siendo menos probable. Dependiendo de la funcionalidad que desempeñe el dispositivo, el impacto variará. Como ejemplo, no es lo mismo un sistema de monitorización de aviones que el sensor que monitoriza la temperatura de la calefacción de una vivienda, es por ello que el impacto puede ser alto o bajo. En lo que respecta a su probabilidad, debido al alto número de dispositivos que presentan vulnerabilidades, la probabilidad de una alteración del rendimiento es alta.

Para mitigar este riesgo, es necesario realizar un modelo holístico para descubrir las posibles vulnerabilidades del diseño del dispositivo así como cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Vulnerabilidades del dispositivo

Superar este reto es sin lugar a dudas uno de los retos más duros a los que se enfrenta el IoT dado a la diversidad de vulnerabilidades que se han encontrado en los dispositivos ya existentes en el mercado. Se calcula que cerca del 70% de los dispositivos IoT presentan algún tipo de vulnerabilidad, entre las que cabe destacar:

- El 80% de estos dispositivos tiene una contraseña débil o corta o políticas de seguridad insuficientemente complejas.
- El 70% de los dispositivos falló a la hora de encriptar los servicios de transmisión de datos por la red local e Internet.
- El 60% de los dispositivos con interfaz web permiten realizar ataques de *cross-site scripting*, mantienen las credenciales por defecto o realizaban una mala gestión de la sesión.
- Por otra parte, al no haber un estándar universal definido, seguido de unas buenas prácticas del desarrollo para comunicación entre dispositivos, muchos de ellos realizan conexiones inalámbricas de protocolos que presentan vulnerabilidades, como los que se pueden mostrar en la parte inferior de la figura 2.

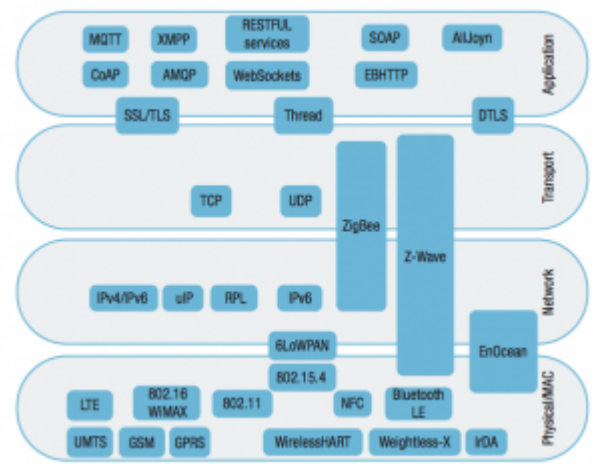


Figura 2: Protocolos más usados en el IoT

Como se deduce, la probabilidad de que un dispositivo presente vulnerabilidades de algún tipo es alta. Por otra parte, tal y como se ha visto en las subsecciones anteriores, este riesgo compromete aspectos tan críticos como la salud, seguridad y la privacidad del usuario, por lo que el impacto que supone también es alto.

Para mitigar algunos de estos riesgos es necesario realizar las siguientes tareas:

- Desarrollar una legislación, políticas, estandares y buenas prácticas.
- Liberar el software propietario no compatible a la comunidad *open-source*.
- Asegurarse de que los sistemas embebidos remotos están monitorizados o su vida útil es finita.
- Integrar la seguridad en los procesos de diseño de los dispositivos.
- Realizar un estudios de los servicios que se utilizan para la

comunicación y puedan crear situaciones inseguras o no deseadas y planear una arquitectura para salvaguardarse de estas vulnerabilidades.
- Definir y habilitar comprobadores de la integridad de los datos en los dispositivos.

Actualizaciones del dispositivo

Este riesgo consiste en no mantener al dispositivo y brindarle actualizaciones que solventen vulnerabilidades. Pero además, incluye las vulnerabilidades propias de dicho proceso:

- La comunicación entre el servidor y el cliente no está cifrada, pudiendo así acceder al contenido del mismo.
- Los clientes que no protegen el espacio de memoria destinado a la actualización, siendo posible la instalación de un código de terceros.

Al igual que los riesgos de seguridad, estos riegos comprometen aspectos tan críticos como la salud, seguridad y la privacidad del usuario, por lo que el impacto que suponen es alto. Por otra parte, debido al alto número de dispositivos vulnerables, la probabilidad de padecer este riesgo también es alto.

Mitigar este riesgo consiste en impedir que los usuarios consigan aprovecharse de las vulnerabilidades de dispositivos no soportados o no actualizados y asegurar los procesos de actualización. Para ello hay que llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos, así como definir un ciclo de vida para los dispositivos, monitorizados y darlos de baja cuando llegue el momento.

Gestión del dispositivo

Este riesgo consiste en salvaguardar los procesos de configuración, supervisión y mantenimiento de los dispositivos, donde entran en juego las vulnerabilidades y el acceso autorizado. Una mala monitorización o la configuración por un usuario no autorizado puede comprometer la salud, seguridad y la privacidad de la información, por lo que el impacto de este riesgo es alto. Por otra parte, debido a la gran cantidad de dispositivos que presentan algún tipo de vulnerabilidad, la probabilidad de este riesgo es alta.

Para mitigar este riesgo, es necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos, así como establecer un control sobre los usuarios que están autorizados para la manipulación del dispositivo sin olvidarnos de una continua monitorización.

Riego	Impacto	Probabilidad
Salud y seguridad	Alto	Bajo-Alto (Dependiente de Negocio)
Cumplimiento de la regulación	Alto	Bajo

Privacidad del usuario	Alto	Alto
Costes inesperados	Medio	Bajo
Acceso inadecuado	Alto	Alto
Uso inapropiado	Alto	Alto
Rendimiento	Bajo-Alto (Dependiente de la función que desempeña el dispositivo)	Alto
Vulnerabilidades del dispositivo	Alto	Alto
Actualizaciones del dispositivo	Alto	Alto
Gestión del dispositivo	Alto	Alto

Priorización de los riesgos