Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
El Internet de las Cosas (IoT)

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10033-161104*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*04/11/2016*
N° de Páginas	*1 de 11*

1 TABLA DE CONTENIDOS

2 OBJETIVO

El objeto de este documento es introducir a los usuarios en las nuevas tecnologías del Internet de las cosas (Internet of Things – IoT), así como dar una visión de aspectos y nociones básicas de seguridad.

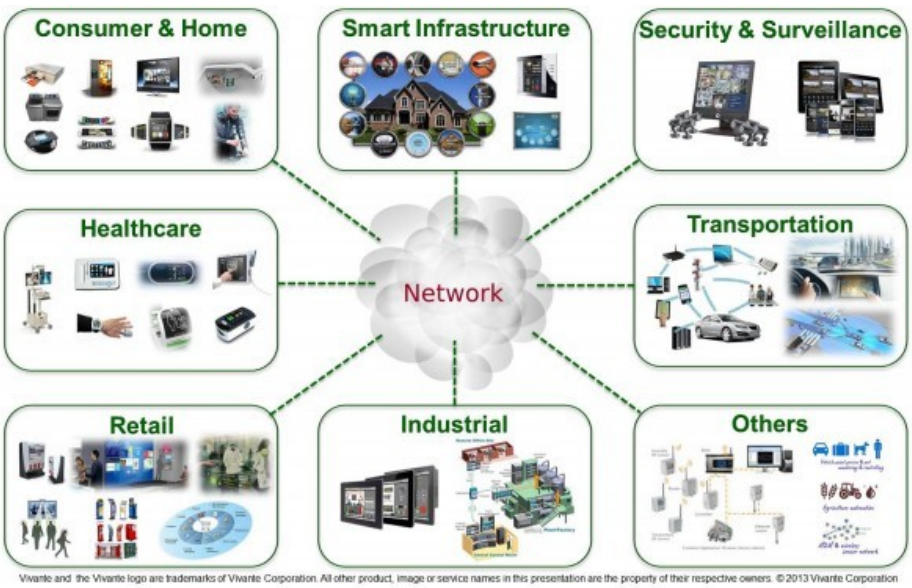
3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Es de carácter divulgativo e informativo, en el cual se pretende dar a conocer las tendencias tecnológicas del IoT y sus ventajas, pero sobre todo, que el usuario sea consciente de las recomendaciones de seguridad que se requieren para que su uso sea un avance global y no un retroceso en la seguridad, confidencialidad y libertad de las personas.

4 INTRODUCCIÓN.

El Internet de las cosas se define como una infraestructura de red global, dinámica, con capacidad de auto-configuración, basada en protocolos de comunicación estándar e interoperables, donde objetos físicos y virtuales poseen identidades, atributos físicos y personalidades virtuales que utilizan interfaces inteligentes y están perfectamente integrados en la red de la información. Las redes de ordenadores junto con IoT y otros desarrollos emergentes de Internet constituirán el Internet del Futuro: una plataforma global de redes a medida y objetos inteligentes conectados en red.

Lo que vagamente consiste en que las cosas tengan conexión a Internet en cualquier momento y lugar.



4.1 Tendencias tecnológicas y las ventajas de su aplicación

Las posibles aplicaciones de IoT son numerosas y diversas, tocando prácticamente todos los ámbitos de la vida cotidiana de las personas, las empresas y la sociedad en su conjunto. A continuación se muestran aplicaciones específicas en algunas áreas a modo de ejemplo.

Ciudad:

- Parking Inteligente: Monitorización de la disponibilidad de plazas de aparcamiento en la ciudad, aparcamientos privados, centros comerciales.
- Controladores de tráfico Inteligentes cuya función es monitorizar vehículos y peatones con el objetivo de optimizar la conducción y las rutas peatonales.

Seguridad y Emergencias :

- Control de acceso perimetral: Control de acceso en áreas restringidas y detección de personas en zonas no autorizadas.

Domótica y Automatización del hogar:

- Monitorización y seguimiento del consumo de agua y energía para ahorrar costes y recursos.
- Aparatos de control remoto para la conexión y desconexión de electrodomésticos para evitar accidentes y ahorrar energía.
- Sistemas de Detección de Intrusos: Detección de la apertura de ventanas y puertas para prevenir intrusos.

Salud:

- Dispositivos detectores de caídas como método de asistencia a personas mayores o discapacitadas que viven solas.
- Neveras sanitarias que controlan las condiciones de almacenamiento de las vacunas, medicamentos y órganos.

5 SEGURIDAD EN EL IoT.

El Internet de las cosas abre una gran ventana al futuro donde podemos disponer de infinidad de nuevos servicios y aplicaciones para muchos de los ámbitos de nuestra sociedad, tal y como se ha mencionado anteriormente. Sin embargo, su seguridad es un punto de especial interés, ya que por un lado supone un foco importante de riesgos y problemas, pero que al mismo tiempo abre la posibilidad para la generación de nuevas soluciones tecnológicas.

5.1 Seguridad en el IoT: Riesgos.

Una vez mencionadas las ventajas que suponen a nivel social la nueva generación tecnológica, también se va analizar los riesgos asociados a la evolución del IoT, ya que tales riesgos pueden variar en función del tipo y la criticidad del dispositivo.

Las amenazas en las cuales pueden verse afectados nuestros dispositivos son las siguientes:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Para determinar el nivel riesgo que produce la materialización de estas amenazas vamos a concretar algunas situaciones que se pueden producir en determinados dispositivos. Se acompañará la exposición con algunos casos de incidentes reales.

Un factor a tener en cuenta y directamente relacionado con la información es la confidencialidad de los datos, que se debe garantizar tanto la información almacenada en el dispositivo, como a la transmitida en las comunicaciones que éste realice, más si son a través de Internet.

Los dispositivos IoT son especialmente vulnerables cuando la comunicación se distribuye por medios inalámbricos o redes publicas.

Otro de los riesgos al que nos enfrentamos, son los ataques que pueden llegar a tomar el control de los dispositivos que utilizamos. Dispositivos que después de un ataque, aprovechando una posible vulnerabilidad, son controlados por terceros de forma remota.

A continuación mostramos diversos ejemplos de casos en los cuales se aprovechó una vulnerabilidad para poder conectar de forma remota a los dispositivos y poder ser controlados.

- Incidente Tesla 11

Se trataba de un modelo de coche pionero en el campo de los eléctricos, que destacaba por su conectividad, funcionalidad y acceso a Internet.

En este caso pudo ser controlado de forma remota por un atacante y tomó el control de este dispositivo a través de la red, controlando toda su funcionalidad.

- Incidente DYN

Este caso, del pasado 21 de octubre de 2016, de ataque por denegación de servicio distribuido (DDoS), se realizó contra el proveedor DYN de servicios DNS (e indirectamente sus clientes).

El ataque hizo uso de varias botnets, principalmente de la botnet Mirai, y generó un tráfico superior a 1 Tbps, imposibilitando la resolución de nombres de algunos clientes importantes de DYN, como Amazon y Twitter.

La botnet Mirai se propaga a través de dispositivos IoT vulnerables, que utilizan contraseñas por defecto del fabricante o con credenciales de acceso embebidas en su firmware. El compromiso es tan simple como conectarse al servicio telnet del dispositivo IoT con las credenciales por defecto (el código hace uso de unas 70 credenciales) e instalar el código malicioso de Mirai. Los cientos de miles de sistemas infectados (como cámaras de seguridad y router) son principalmente de usuarios domésticos y pequeñas empresas. Cuando el malware toma el control de estos dispositivos, los convierte en zombies o bots, forzándolos a conectarse a un centro de mando y control gestionado por los ciber-delincuentes, los cuales son controlados y usados para realizar ciertas acciones maliciosas, como la de lanzar ataques DDoS masivos a otros dispositivos, como en este caso.

- Vulnerabilidad Smart Rabbit.

Este caso se dio a conocer en los medios públicos entorno al año 2013, fue un producto de la empresa Karotz, denominado "*smart rabbit*".

Un conejo interactivo con acceso a Internet y que permitía el control por voz, pensado en su diseño para interactuar con niños y que incorporaba, micrófono y cámara.

En este caso se descubrieron vulnerabilidades que podían llegar a permitir a un atacante tomar el control del dispositivo, pudiendo obtener por ejemplo imagen y audio en tiempo real del mismo.

- Vulnerabilidad reloj Pebble

Se trata de un smartwacth que puede conectarse a cualquier dispositivo móvil e interactuar con las aplicaciones. Fue desarrollado por la Empresa "*Pebble Technology Corporation"* en 2013.

El dispositivo es vulnerable a situaciones estresadas. El ataque DDoS, consistía en enviar 1500 mensajes de Whatsapp al dispositivo en un periodo de 5 segundos, lo que provocaba el bloqueo del dispositivo y este ejecutaba de manera automática el reseteo de fábrica, con la consiguiente pérdida de información del usuario.

Las amenazas a las que pueden enfrentar en cuanto a la disponibilidad es quizás de los aspectos que mas problemas puede general, sobre todo si nos centramos en el entorno industrial, donde una parada de un servicio producido por un ataque puede provocar numerosas perdidas económicas.

- Incidente Planta Nuclear Natanz

Este caso se consideró como el primer ataque cibernético que logró dañar infraestructura, fue diseñado con mentalidad bélica.

Considerado uno de los ataques más importantes, se produjo en torno al 2010 en la central nuclear de Natanz (Irán).

Se trataba de un ataque cibernético provocado por el gusano Stuxnet, que tomó el control de mil máquinas de producción de material nuclear y les dio instrucciones de auto-destruirse.

En este caso, el Controlador Lógico Programable o PLC fue el blanco del ataque. Estos dispositivos eran los encargados de controlar la velocidad específica de las centrifugadoras de uranio. La alteración de la velocidad de las centrifugadoras causó que unas mil máquinas se desintegraran.

6 DEFICIENCIAS DE SEGURIDAD

Los principales vectores de ataque a las IoT, van desde deficiencias de seguridad a la hora de implementar los sistemas, el mantenimiento de sus correspondientes actualizaciones, una deficiencia en el hardware y en la mas importante, las deficiencias en la cultura sobre seguridad de los usuarios.

Las principales deficiencias definidas son:

- Deficiencias de la seguridad en la transmisión de datos: Debido al enfoque de los IoT a la interconexión y el envío/recepción de datos entre dispositivos, una de las medidas fundamentales será la protección de la información en el tránsito. El no proteger adecuadamente el canal de comunicación mediante el cifrado de datos puede ser sencillo, para un intruso, realizar ataques aprovechando la vulnerabilidad.

- Deficiencias en la seguridad de la plataforma software: Cuando un atacante detecta vulnerabilidades sobre dichas plataformas tanto software como hardware, estas pueden ser explotables sobre todos los dispositivos asociados, facilitando a los potenciales atacantes una puerta de entrada para infinidad de dispositivos.

- Deficiencias en la cultura de seguridad de los usuarios: Como ultimo punto a tener en cuenta y de los más importante es el producido por el propio usuario y su experiencia. A pesar de que los sistemas estén bien configurados y bastionados, una negligencia de un usuario podría comprometer el servicio.

7 ESTRATEGIAS PRINCIPALES DE SEGURIDAD EN IOT

Las principales estrategias a tener en cuenta para mantener la seguridad en el IoT son las siguientes:

- Incorporar la seguridad en la fase de diseño: La seguridad debe evaluarse como un componente más integrado en el diseño de cualquier dispositivo conectado a la red.
- Actualizaciones de seguridad avanzadas y gestión de vulnerabilidades: Incluso cuando se considera la seguridad en la fase de diseño, es común que las vulnerabilidades se descubran en los productos después de que se hayan implementado. Estos defectos se pueden mitigar mediante revisiones y actualizaciones de seguridad y estrategias de gestión de vulnerabilidades.
- Basarse en prácticas de seguridad probadas: Muchas de las prácticas probadas utilizadas en la seguridad tradicional pueden utilizarse como punto de partida para mejorar la seguridad de IoT. Estos enfoques pueden ayudar a identificar vulnerabilidades, detectar irregularidades, responder a incidentes potenciales y recuperarse de daños o interrupciones en dispositivos IoT.

- Priorizar medidas de seguridad de acuerdo con el impacto potencial: Los modelos de riesgo varían sustancialmente en el entorno de IoT, al igual que las consecuencias de los fallos de seguridad. Enfocarse en las consecuencias potenciales de la interrupción, el incumplimiento o la actividad maliciosa, es por lo tanto crítico para determinar donde realizar un mayor esfuerzo en la seguridad.
- Promover la transparencia en todo el IoT: Siempre que sea posible, los desarrolladores y fabricantes deben conocer su cadena de suministro, es decir, cuáles son sus componentes de software y hardware y si existen vulnerabilidades asociadas. Un mayor conocimiento puede ayudar a los fabricantes y consumidores industriales a identificar dónde y cómo aplicar medidas de seguridad.
- Conectar de manera cuidadosa y deliberada: Los consumidores de IoT, especialmente en el contexto industrial, deberían considerar si se necesita conectividad continua dada la utilización del dispositivo IoT y los riesgos asociados con su interrupción.

7.1 Conexión cuidadosa y deliberada

Debido a la importancia a tener en cuenta de esta estrategia de seguridad, vamos a profundizar y desarrollar este último punto.

Los consumidores de IoT pueden ayudar a contener las amenazas potenciales que plantea la conectividad de red y ponderar los riesgos de un agujero o fallo de seguridad de un dispositivo IoT, considerando la necesidad de conexión . Con lo que surge la pregunta: ¿Cada dispositivo necesita una conectividad continua y automatizada a internet, tiene las medidas de seguridad necesarias?.

El llevar a cabo unas recomendaciones básicas de seguridad conlleva a unas buenas practicas que los usuarios deben tener en cuenta a la hora de las conexión de sus dispositivos IoT.

A continuación destacamos las siguientes recomendaciones:

- Asesorar a los usuarios de IoT sobre el propósito de cualquier conexión de red.
- Las conexiones directas a Internet pueden no ser necesarias para operar funciones críticas de un dispositivo IoT, especialmente en el entorno industrial.
- La información sobre la naturaleza y el propósito de las conexiones puede asesorar en las decisiones de los consumidores.
- Hacer conexiones intencionales. Hay casos en los que el consumidor no desea conectarse directamente a Internet, sino a una red local que puede agregar y evaluar cualquier información crítica.
- Incorporar controles de seguridad que permitan a los fabricantes, proveedores de servicios y consumidores desactivar las conexiones de red o puertos específicos cuando sea necesario o deseado, para permitir la conectividad selectiva.

- Dependiendo del propósito del dispositivo IoT, proporcionar a los consumidores orientación y control sobre la implementación final puede ser una práctica sólida

8 CONCLUSIONES

Aunque el IoT cambie por completo nuestro entorno socio-económico y tales tecnologías nos abran un mundo cada vez más amplio a la hora de obtener información en todo momento, hay que tener en consideración lo que constituye su seguridad en sus múltiples y variadas vertientes.

Si bien la naturaleza de la IoT presenta unos desafíos novedosos (debido principalmente a las restricciones y/o características que comporta su diseño) en ocasiones incompatibles con la seguridad tradicional, sigue siendo necesario adoptar medidas de seguridad tradicionales; medidas tan elementales como el uso de claves robustas del router o de la wifi, y el bloqueo de pantalla, siguen siendo básicas.

El papel de la industria en su conjunto es esencial para abordar el problema de la seguridad desde la concepción de los protocolos empleados y el diseño de los dispositivos. No obstante, el usuario tiene la última palabra en la decisión de adquisición del dispositivo y el modo de uso. A lo largo del documento hemos visto casos en los que el compromiso en la seguridad en el IoT puede ir orientado contra el mismo o utilizado contra terceros. Evaluar los riesgos que genera el dispositivo IoT, aparentemente inocuo, y tomar las medidas de seguridad apropiadas redundará en el bien de todos.

9 GLOSARIO

IoT: (Internet of Things) En su traducción "El internet de las cosas".

FTP: (Protocolo de transferencia de datos) Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

Botnets : Conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

Ataque DDOS (Denegación de servicio) : Ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Sistemas SCADA: acrónimo de Supervisory Control And Data Acquisition (Supervisión, Control y Adquisición de Datos) es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia.

Gusano Stuxnet : Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales.

SkyGrabber : Herramienta tecnológica que intercepta los datos de satélite (películas, música, imágenes) que los usuarios podrán descargar para guardar en su disco duro.

Drones: Vehículo aéreo no tripulado (VANT), y UAV (Unmanned Aerial Vehicle) o aeronave que vuela sin tripulación.

10 DOCUMENTACION DE REFERENCIA

- Security ArTwork: Mirai Strikes Again
- Security ArTWork: Linux.Mirai: Atacando sistemas de videovigilancia
- MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled..
- MuySeguridad.net: El troyano Mirai tiene una vulnerabilidad que permitiría detener sus ataques
- Consiguen hackear un Tesla Model S y controlarlo a distancia
- elEconomista.es: Hackean el Autopilot de un Tesla Model S para que no detecte los obstáculos al circular
- Smart Rabbit:
- Pebble smartwatch está afectado por una vulnerabilidad con la que un atacante remoto puede borrar todo su contenido
- Un atacante remoto puede borrar todos los datos del reloj Pebble
- Planta Nuclear (Stuxnet)
- BBC: Gusano Stuxnet
- The Register: Israel and US fingered for Stuxnet attack on Iran
- Noticias: Piratean aviones no tripulados de EE.UU
- Piratean los aviones espías norteamericanos
- Guia Comite Federal de comisión 2015
- Guía de seguridad: Sistemas de Control Industrial
- Guía CSIRT-CV: Seguridad en el Internet de las Cosas
- Homeland Security: Strategic Principles for Securing the Internet of Things
- Homeland Security: Seguridad IoT