CCN-CERT

BP/05

Internet de las Cosas

INFORME DE BUENAS PRÁCTICAS

JUNIO **2021**

centro criptológico nacional

centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Índice

1. Sobre CCN-CERT

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es **contribuir a la mejora de la ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de **conseguir un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional.

2. Introducción

El término "Internet de las Cosas" (Internet of Things) se refiere a redes de objetos físicos: artefactos, vehículos, edificios, electrodomésticos, atuendos, implantes, software... en definitiva, sensores que disponen de conectividad en red que les permite recolectar información de todo tipo.

Un estudio de IOT Analytics[1] recoge que a finales de 2019 había 9.500 millones de dispositivos IoT conectados en el mundo descontando móviles y ordenadores. En los próximos años, la demanda disparará la cifra hasta 28.000 millones en 2024 y 40.000 millones en 2027. No es difícil imaginar como esa ingente cantidad de objetos representa una enorme superficie de exposición social e industrial antes nunca vista.

En ese mismo informe, se muestra una gráfica con el número de plataformas de IoT en el mundo de 2015 a 2019, la cual muestra que a finales de 2019 existían en todo el mundo 620 plataformas de Internet de las cosas (IoT), es decir, más del doble de las contabilizadas en 2015.

Mientras que los medios y los expertos en seguridad están constantemente advirtiendo sobre el riesgo de ataques cibernéticos, rara vez se mencionan los riesgos asociados a la Internet de las Cosas.

La seguridad de la IoT todavía no está en el punto de mira, incluso para las empresas que tienen mucho que perder si se produce una brecha de seguridad. En una encuesta llevada a cabo en 2017 por la consultora estadounidense Altman Vilandrie & Company, casi la mitad (48%) de las empresas de este país que utilizan una red de Internet de Cosas (IoT) habían experimentado, al menos, un problema de seguridad en estos dispositivos.

1. https://iot-analytics.com/iot-2020-in-review/

2. Introducción

Internet ha pasado por cuatro (4) fases distintas en los últimos 30 años (fases académica, comercial, transaccional y social), y ha mantenido una implantación y mejora estable durante muchos años, pero, sin embargo, no se puede decir que haya cambiado mucho desde el punto de vista de su arquitectura. De hecho, es esencialmente la misma entidad que se diseñó en la era ARPANET[2]

En este contexto, IoT es la primera evolución real de Internet, un salto que podría llevar a modificar de forma muy significativa la forma en la que vivimos, aprendemos, trabajamos y nos entretenemos o relacionamos socialmente. Lo más transcendente de la IoT es que le da sensores y sensibilidad a Internet, permitiendo que, de forma autónoma, exista una realidad más allá de ella misma, el mundo físico, y a nosotros y lo nuestro dentro de él.

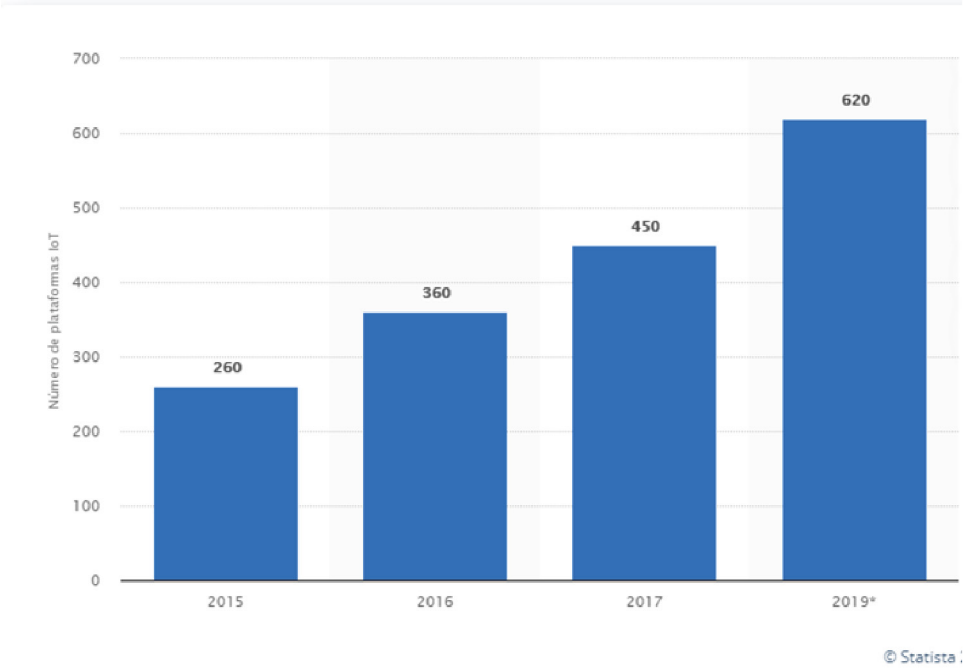


Figura 1 Número de plataformas de IoT en el mundo 2015-2019

Mientras que los medios y los expertos en seguridad están constantemente advirtiendo sobre el riesgo de ataques cibernéticos, rara vez se mencionan los riesgos asociados a la Internet de las Cosas.

2. Ver https://sistemas.com/arpanet.php

2. Introducción

Cuando se habla de la IoT, se hace referencia a todos aquellos dispositivos u objetos cotidianos adaptados, que se encuentran conectados entre sí o a Internet. La IoT es un concepto relativamente nuevo y por este motivo, el ámbito de la ciberseguridad no está todavía preparado para hacer frente a todas las amenazas que representa, que ya han surgido y sin duda surgirán en un futuro cercano.

Una de las mayores ventajas reconocidas a estos dispositivos es su conexión a Internet, pero esa capacidad también es una de sus mayores debilidades, ya que esa conectividad puede amenazar la seguridad de todo el sistema al incrementar notablemente su superficie de exposición a ciberataques.

Por ejemplo, si no hubiese control de acceso en el dispositivo o hubiese algún fallo en el mismo, un atacante podría acceder de forma remota al mismo y alterar su configuración e incluso toda su funcionalidad. Ese acceso podría darse en cualquier momento y desde cualquier lugar, por lo que no se podría confiar en la integridad y funcionalidad del dispositivo IoT que originalmente se instaló y utiliza a diario de forma habitual.

La creciente superficie de ataque está dominada por puntos de control no tradicionales, que van desde algo tan inocuo como un juguete conectado a Internet hasta algo tan crítico como los sensores conectados que controlan la producción de energía en una planta nuclear.

2.1 Tendencias en la internet de las cosas

Una conectividad sin precedentes constituye lo mejor de la Internet de las cosas y a la vez lo peor ya que crea tanto grandes oportunidades como riesgos considerables. En un entorno que se extiende desde sensores hasta aplicaciones y servicios en la nube, un ecosistema de IoT de extremo a extremo es esencial para aprovechar las oportunidades sin arriesgar la seguridad, la capacidad de gestión y la interoperabilidad.

Así, Microsoft está desarrollando encimeras de cocina que pueden reconocer los alimentos y mostrar recetas que los incluyan. Hay colchones inteligentes que monitorizan los patrones de sueño del usuario mediante la medición de su respiración y ritmo cardíaco. Ahora hay disponibles un gran número de cerraduras inteligentes que se abren cuando se camina hacia la puerta y que pueden ser programadas de forma remota para dejar entrar eventualmente a amigos o invitados

Hay un cierto entusiasmo comedido sobre el potencial de una "vida cotidiana asistida", que es especialmente importante para ancianos o dependientes. Hay varios proyectos en marcha que incluyen grandes despliegues de IoT para una mejor gestión de ciudades y sistemas.

Las aplicaciones potenciales de la Internet de las cosas cubren un amplio espectro de industrias multimillonarias que van desde la seguridad y la salud, hasta el estilo de vida y el juego.

2.1 Tendencias en la internet de las cosas

Un ejemplo de ello es Songdo[3], en Corea del Sur, que es el primer ejemplo de **Smart City** completamente equipada. Prácticamente todo en esa ciudad está cableado, conectado y convertido en una fuente continua de datos que podrán ser monitorizados y analizados por multitud de ordenadores y todo ello con escasa o nula intervención humana.

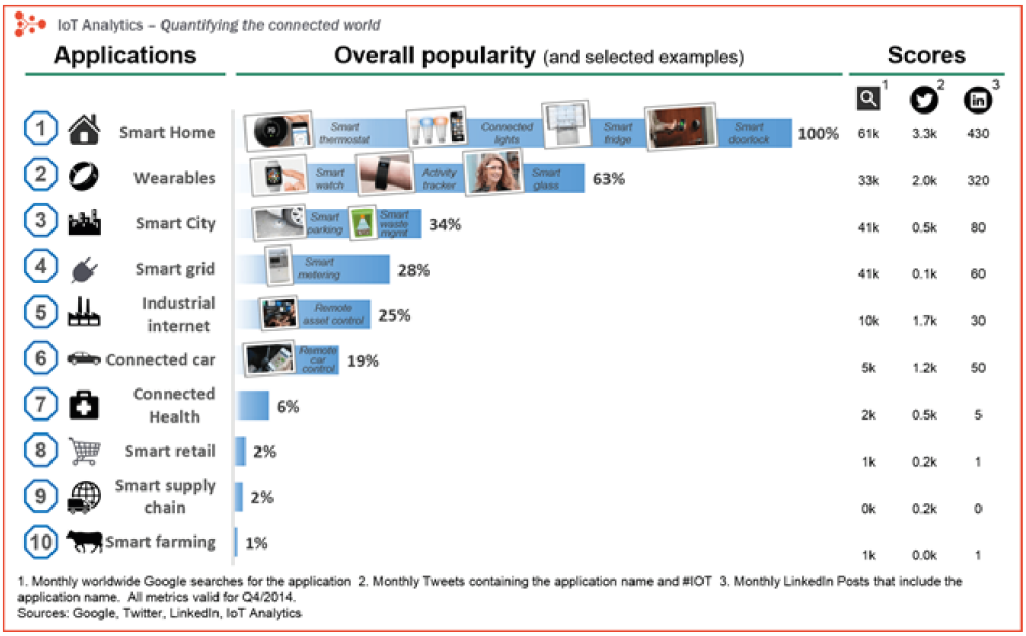


Figura 2.- Popularidad de dispositivos IoT.

Otro aspecto a tener en cuenta son los rápidos **ciclos de actualización y obsolescencia** que son habituales en el mundo de las tecnologías de la información. Si se pretende integrar estas tecnologías con la edificación y la arquitectura, podríamos terminar teniendo edificios, casas y fábricas plagadas de elementos completamente obsoletos, sin soporte y sin mantenimiento posible.

Con la IoT nuestras casas se hacen más "*hackeables*" según aumenta el número de dispositivos conectados. Las pesadillas de los expertos en ciberseguridad son ejércitos de "*botnets*" utilizando las tostadoras inteligentes para desarrollar ataques de denegación de servicio distribuido (DDoS) o para esconder código y ejecutables lejos de la vista de los investigadores.

3. Ver https://www.bbc.com/mundo/noticias-57030345

2.1 Tendencias en la internet de las cosas

Con la Internet de las cosas, la casa y demás entornos inteligentes se convierten en una extensión de nuestro trabajo. Al igual que un dispositivo "*wearable*" cuenta nuestros pasos, nuestro ritmo cardiaco o nuestra respiración, nuestros hogares monitorizarán y medirán todo lo demás.

Las preocupaciones más obvias tienen que ver con la **privacidad**. La recolección masiva de nuestros datos y metadatos puede que sea lo mismo que instalar cámaras de vigilancia, pero es una forma de vigilancia digital incluso más peligrosa para nuestra intimidad y libertad que la mera observación visual.

En el futuro, la Internet de las cosas puede ser una enorme red abierta en la que entidades y objetos virtuales (avatares) interactuarán entre sí de forma independiente según el contexto, las circunstancias y el entorno.

Las empresas necesitarán adaptar sus prácticas de gestión de riesgos y ampliar el alcance de las evaluaciones de riesgo para incluir todos los dispositivos conectados. En este contexto, uno de los desafíos principales para las organizaciones será cómo almacenar, rastrear, analizar y dar sentido a la gran cantidad de datos generados al incluir la IoT en el proceso de evaluación de riesgos.

2.2 Relaciones con la nube

Actualmente, muchos de estos dispositivos domésticos utilizan servicios de respaldo ubicados en la nube para monitorizar su uso y permitir a los usuarios controlar de forma remota dichos sistemas. Gracias a ellos, los usuarios pueden acceder a los datos y controlar el dispositivo a través de una aplicación para su móvil o a través de un portal web.

Dada la importancia que van a tener los proveedores de servicios en la nube en las distintas fases del desarrollo de la IoT, es muy necesario comprobar la seguridad de su interfaz:

Determinar si los valores **por defecto del usuario y de la contraseña** pueden ser **cambiados** durante el proceso de instalación inicial del producto.

Determinar si cualquier **cuenta** se **bloquea** después de varios fallos de acceso[4].

Determinar si se pueden identificar cuentas válidas utilizando los mecanismos de **recuperación de contraseñas.**

Revisar la r**esistencia del interfaz web** frente a ataques de cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection (SQLi) y similares.

Revisar los **interfaces con la nube en busca de cualquier posible vulnerabilidad** (interfaces API e interfaces web de los sistemas en la nube).

2.2 Relaciones con la nube

El hecho de asegurar el interfaz con la nube requiere:

- Cambiar la contraseña e incluso el nombre de usuario durante la instalación del producto IoT.
- Asegurar que las cuentas de los usuarios no pueden ser averiguadas utilizando funcionalidades como, por ejemplo, la de recuperación de contraseñas.
- Asegurar que se bloquea temporalmente el acceso a una cuenta después de varios fallos de acceso[4].
- Asegurar que las credenciales (nombre de usuarios, contraseñas, tokens de acceso, cookies, etc.) no están expuestas a Internet mientras transitan a través de ella. Hay que utilizar siempre conexiones cifradas con autenticación TLS.
- Implementar, si es posible, la autenticación mediante la verificación de dos o más factores.
- Detectar y bloquear peticiones o intentos anómalos de conseguir entrar en el sistema/dispositivo.

4. Por ejemplo, ver https://bitacoralinux.es/fail2ban-o-como-prevenir-ataques-de-fuerza-bruta/

2.3 Infraestructuras críticas y la internet de las cosas

En los últimos años, la electrónica industrial y su informática eran cosas muy específicas y sólo presentes en sus cerrados ámbitos de actuación. Los sistemas SCADA[5] son un tipo de Sistema de Control Industrial (ICS)[6] al igual que lo son los denominados Sistemas de Control Distribuido (DCS)[7].

En los sistemas industriales, los datos se reciben desde estaciones remotas y estos generan reacciones que, de forma automática o con ayuda de operadores, se plasman en acciones ejecutivas que se envían a dispositivos de campo, controlando así todo el sistema. Estos artefactos son los que realmente controlan las operaciones locales (abrir o cerrar válvulas, poner freno o quitarlo, recoger datos proporcionados por sensores, monitorizar el entorno, establecer el nivel de alarma, etc.).

Las tecnologías SCADA son las que controlan los procesos industriales y todas estas instalaciones tienen como característica esencial que no pueden detenerse sin causar un gran perjuicio a las poblaciones y sistemas a los que sirven, ni sin causar grandes pérdidas económicas difíciles de asumir.

Los protocolos de comunicación SCADA son específicos de un fabricante, pero muchos de ellos se utilizan con profusión sobre redes TCP/IP gracias a extensiones posteriores de los protocolos originales. Este hecho difumina peligrosamente la frontera que hay entre redes industriales y redes de propósito general como Internet. En cualquier caso, esta migración a redes TCP/IP es un riego en sí, ya que no tiene en cuenta las importantes diferencias que hay en una red industrial y otra generalista.

5. SCADA (Supervisory Control And Data Acquisition). Ver https://www.wonderware.es/hi-scada/que-es-scada/
6. Ver https://www.industriasgsl.com/blog/post/que-es-un-sistema-de-control-industrial
7. Ver https://www.cursosaula21.com/que-es-un-sistema-de-control-distribuido/

2.3 Infraestructuras críticas y la internet de las cosas

Todos esos escenarios y muchos más, que componen el catálogo de **Infraestructuras Críticas**, dependen, en mayor o menor medida, de redes de control y monitorización que están siendo migradas para operar sobre redes TCP/IP y así utilizar la misma electrónica de red que Internet, todo ello sin una evaluación previa en cuanto a su seguridad efectiva.

La consideración de la seguridad SCADA ha cambiado radicalmente después de que se conociera el ataque Stuxnet[8] a los sistemas de control industrial de una planta iraní de enriquecimiento de uranio en Natanz[9]. De esta manera, la sociedad industrializada ha podido ver claramente lo que la amenaza del código dañino puede suponer en operaciones de sabotaje[10].

8. Ver https://www.businessinsider.es/10-anos-stuxnet-primer-ciberataque-mundo-fisico-657755
9. Ver https://www.bbc.com/news/world-middle-east-56722181
10. Kim Zetter: "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" Crown Publisher, ISBN-13: 978-0770436179

3. Visibilidad en Internet

Gracias al rápido crecimiento de Internet, cada día hay más herramientas al alcance de todos, y una de ellas son los famosos buscadores.

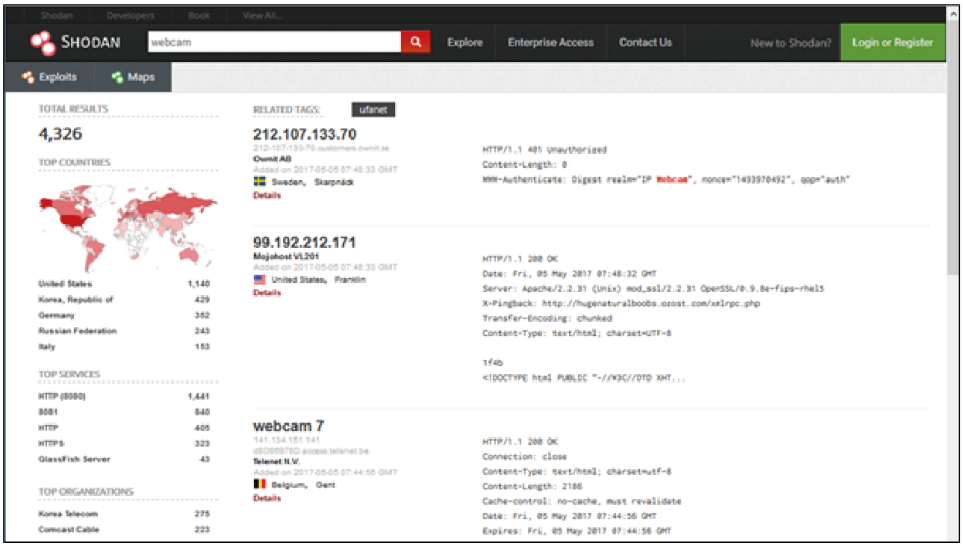


Figura 3.- Búsqueda de dispositivos IoT en Shodan.

3. Visibilidad en Internet

Según han crecido los servicios ofrecidos en la red, también se han especializado los motores de búsqueda, surgiendo algunos como **Shodan**[11] que permite, de forma muy sencilla, encontrar dispositivos IoT conectados directamente a Internet.

Este buscador ofrece al usuario una amplia cantidad de detalles sobre el aparato en sí y le permite hacer búsquedas por tipo de dispositivo, como, por ejemplo, "webcams". Como se observa en la Figura 3, con esta sencilla búsqueda se pueden encontrar hasta 4.326 webcams directamente conectadas a Internet en ese momento.

También se pueden filtrar búsquedas por otros términos como el puerto que tienen expuesto a la red. Por ejemplo, se pueden encontrar todos los dispositivos que permitan conexiones al puerto 22, que es el de los terminales SSH, y el resultado de la búsqueda arroja hasta 8.860.281 elementos directamente accesibles de forma remota con ese tipo de comunicación en Internet.

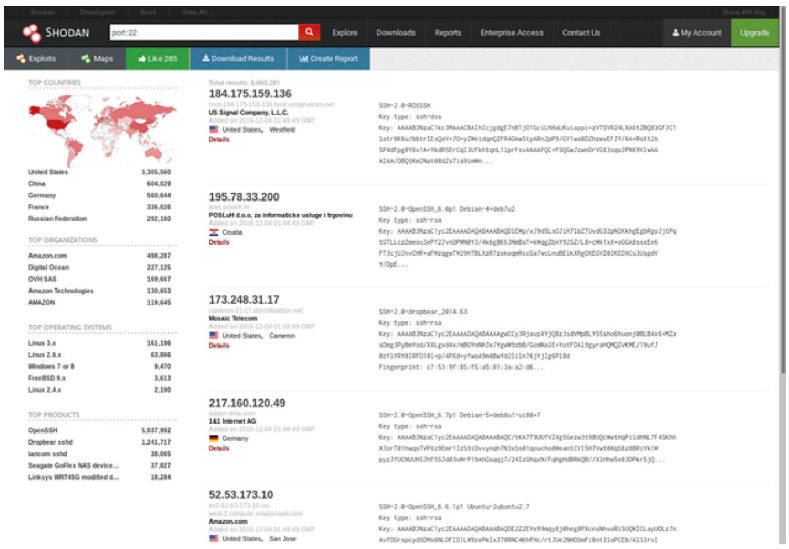
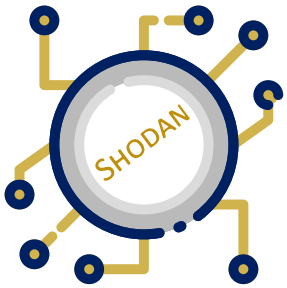


Figura 4.- Búsqueda de dispositivos IoT en Shodan por puerto.

11. https://shodan.io

3. Visibilidad en Internet

Además de Shodan, hay otros muchos métodos de búsqueda de máquinas que están directamente conectadas a Internet. Unos de los más conocidos son Scans.io[12] y ZMap[13] .



No se puede olvidar que los dispositivos IoT también pueden estar conectados entre sí o con otros dispositivos mediante conexiones[14] de radio, de las cuales podemos resaltar las conexiones Wi-Fi, BlueTooth (BT) o, incluso, NFC. En estos casos, el control de los dispositivos también es susceptible de caer en manos de usuarios malintencionados.

En el informe "Combatting the Ransomware Blitzkreig" podemos encontrar un capítulo dedicado a dispositivos IoT relacionados con la medicina que están conectados a otros mediante enlaces Bluetooth, como, por ejemplo, los marcapasos implantados en pacientes, lo cual pone de relieve los riesgos para la seguridad que eso conlleva.

En cualquier caso, se recomienda al usuario realizar búsquedas de sus dispositivos en los buscadores previamente mencionados, ya que son una de las principales fuentes de información para los atacantes que pretenden localizar dispositivos vulnerables.

12. https://scans.io/
13. https://zmap.io/
14. https://www.postscapes.com/internet-of-things-protocols/

4. Cuando los dispositivos son el objetivo

Una vez que el atacante encuentra la manera de automatizar la búsqueda de posibles objetivos a los que pueden acceder y administrar de manera remota, solo falta que lo haga y consiga su control total con el fin de utilizarlos para realizar las actividades ilícitas que le interesen.

A esta red de máquinas y dispositivos que se encuentra bajo el control de una misma persona se la conoce como “botnet”, y a los nodos que la conforman se les conoce como “bots” o “zombis”.

Cuando un atacante tiene acceso a un dispositivo, normalmente instala en el mismo un programa dañino que le permita controlarlo de forma sincronizada con otros, siendo incluso capaces de lanzar órdenes de forma simultánea, de tal manera que todos los equipos infectados actúen de un mismo modo, o de forma coordinada, contra un mismo objetivo.

El ataque de este tipo que más se ha popularizando en los últimos años es el de **Denegación de Servicio Distribuido (DDoS)** que, mediante la realización de conexiones de forma masiva y simultánea desde diferentes orígenes, busca inutilizar un servicio o una web de modo que nadie pueda acceder al sitio atacado.

Es interesante observar que para realizar este tipo de ataques, cada vez se utilizan más los dispositivos IoT comprometidos, siendo en su mayoría grabadoras de vídeo digital (DVR) y cámaras IP.

4. Cuando los dispositivos son el objetivo

Las razones para lanzar campañas de DDoS son múltiples, algunas de ellas tienen motivaciones claramente políticas, reivindicativas, activistas, etc. En otros casos, simplemente se hacen para demostrar el poder que puede tener un grupo de delincuentes informáticos a la hora de inutilizar un sitio web. A veces, se trata de una extorsión en la que a la empresa se le pide dinero para no inutilizarle sus servidores en Internet y afectar seriamente a sus actividades comerciales.

Las "botnets" también se utilizan para realizar campañas de **"spam"**, que consisten en el envío masivo de correos electrónicos no solicitados, o bien para alterar los resultados de votaciones y encuestas realizadas a través de Internet. Por lo general, estas "botnets" se alquilan a terceros como plataforma para llevar a cabo las actividades que el cliente desee y que, normalmente, son completamente ilícitas.

Actualmente, una de las "botnets" más famosas y utilizadas es la "botnet Mirai[15]". Esta "botnet" es de amplio uso ya que, a mediados del mes de octubre de 2016, se publicó su código fuente en forma de código libre para ser utilizado por cualquiera. Además, hay que hacer hincapié que este código dañino muestra características que hacen que infectar los dispositivos y crecer como "botnet" sea realmente fácil.

En primer lugar, Mirai escanea Internet buscando principalmente cámaras y enrutadores. Después, trata de acceder al panel de administración del dispositivo usando una lista de **usuarios y contraseñas por defecto.** Cuando consigue acceder al dispositivo, se aloja en el mismo y comprueba que no se encuentre ya infectado por otro código dañino y, si ese es el caso, se encarga de expulsarlo. Después trata de hacer crecer la infección, y con ello la "botnet", desde ese dispositivo buscando nuevas máquinas vulnerables.

Una vez completado el proceso de infección en una máquina, lo que se obtiene es un equipo zombi que está continuamente preparado para ser utilizado en el ataque distribuido que indiquen sus servidores de mando y control.

Recientemente se ha descubierto una nueva versión de Mirai equipada con más exploits, lo que aumenta su peligrosidad y facilita su expansión. Además, esta nueva versión no se dirige únicamente a sus víctimas habituales (cámaras IP, routers, etc.), sino que también se dirige a los dispositivos IdC de las empresas.

15. https://www.akamai.com/es/es/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf
16. https://www.kaspersky.es/blog/mirai-enterprise/18065/

- **Las “botnets” se pueden crear fácilmente en cuestión de horas sobre la base del creciente número de dispositivos IoT inseguros que están conectados a Internet.**
- **Asegurar que las cuentas de los usuarios no pueden ser averiguadas utilizando funcionalidades como, por ejemplo, la de recuperación de contraseñas.**

4.1 Recomendaciones

El primer paso que se ha de llevar a cabo con todos los dispositivos, particularmente con los IoT, debe ser **el cambio de contraseña, eligiendo una que sea realmente segura** para todos sus perfiles, especialmente en aquellos que administren dicho dispositivo. Si por alguna razón, esto no fuese posible, **ese dispositivo nunca debería conectarse a ningún otro y, en la medida de lo posible, no debería utilizarse.**

Otra posibilidad sería cambiar los puertos TCP de conexión por defecto con el fin de no dar a los buscadores información sobre el servicio que, a través de ellos, ofrece el dispositivo.

Si es posible, también es recomendable utilizar un elemento que haga de intermediario separando la red de dispositivos IoT del resto de Internet. Ese dispositivo podría ser el propio enrutador utilizado para acceder a Internet, en cuyo caso habría que **configurarlo correctamente y activar** las **medidas de seguridad** y de **control de accesos** para asegurar las redes de dispositivos IoT a las que ofrece conectividad.

Utilizar un elemento que haga de intermediario separando la red de dispositivos IoT del resto de Internet.

El primer paso en todos los dispositivos, es el cambio de contraseña y eligiendo una que sea realmente segura

5. Cuando tú eres el objetivo

Aunque en la actualidad el concepto de "ransomware" esté más orientado al secuestro de información y al pago del correspondiente rescate, no cabe duda que con la expansión de IoT surgirán nuevas formas de extorsión a los usuarios.

Mientras la efectividad del "ransomware" en ordenadores personales se basa en aprovecharse del valor sentimental de los ficheros privados capturados y del valor que tiene esa información (entorno empresarial) para el funcionamiento de la empresa, en el caso de los dispositivos IoT, el objetivo no será, en principio, la información que se pueda tener almacenada en ellos, sino la denegación permanente de servicio a la espera de conseguir un rescate.

En algunos dispositivos, reinstalar el firmware original y reiniciar el sistema con los valores de fábrica puede ser suficiente para dar respuesta al ataque y recuperar su funcionamiento original, pero, dependiendo del dispositivo, esto podría ser una tarea complicada y, en algunos casos, dada la naturaleza del servicio prestado, la interrupción del funcionamiento correcto podría ser crucial y llegar a costar vidas.

Tómese como ejemplo el caso de un **marcapasos**. Este dispositivo podría ser utilizado para obligar a la víctima a pagar un rescate bajo la amenaza de desactivarlo, o forzándolo a realizar operaciones que agoten la batería a un ritmo acelerado hasta que se reciba el correspondiente pago.

En los casos de denegación de servicio de los dispositivos o instalaciones IoT, el coste que supondría realizar las operaciones de restablecimiento del servicio podría superar con creces el valor del rescate solicitado,

Dependiendo del dispositivo, la interrupción del funcionamiento correcto podría ser crucial y llegar a costar vidas.

por lo que finalmente se terminaría pagando dicho rescate.

También hay que tener en cuenta que, en algunas ocasiones, ese proceso de vuelta a los valores de fábrica podría ser imposible de realizar en el corto espacio de tiempo que marque el atacante. En estos casos, el pago del rescate podría convertirse en la única opción viable que no ponga en riesgo la vida de la persona afectada.

Otro ejemplo de ataque puede ser la infección del sistema de control general de una **casa domótica**. Haciéndose con el controlador central de esta, el atacante podría determinar en todo momento cuál debería ser el funcionamiento y comportamiento de todos los dispositivos conectados en la casa, y posibilitar diversas acciones contra sus habitantes.

Por ejemplo, las acciones que el atacante podría llevar a cabo irían desde manipular la alarma de un despertador para que suene cuando no debe hacerlo y que se mantenga en silencio cuando tenga que sonar, hasta decirle al regulador de temperatura de un dispositivo que vaya a niveles extremos que puedan poner en peligro su integridad. El atacante también podría, por ejemplo, acceder a cámaras de vigilancia para conseguir imágenes comprometidas de los habitantes de la casa para, posteriormente, utilizarlas para hacer chantaje a sus víctimas.

También podría tratarse de una operación más encubierta, en la que el atacante simplemente quiere conocer los hábitos y los horarios de la víctima para planificar el mejor momento para un robo o un secuestro.

En el caso de los dispositivos IoT, el objetivo no será, en principio, la información que se pueda tener almacenada en ellos, sino la denegación permanente de servicio a la espera de conseguir un rescate.

5.1 Recomendaciones

Esta situación plantea un nuevo conjunto de amenazas ante las que el usuario no tendrá medios para combatir. Por ello, la principal recomendación es **prescindir del acceso a Internet en los dispositivos** IoT, evitando así la posibilidad de ataques remotos y el robo de información privada que pueda causar futuros y serios problemas.

En el caso de que ese acceso desde Internet sea absolutamente necesario, es imprescindible extremar la cautela y las medidas de seguridad a la hora de establecer **quién se puede conectar (control de accesos), desde qué dispositivo** (móvil, tableta, etc.) y **en qué momento** del día, de la semana o del año.

La inercia como usuarios de las tecnologías de la información hace pensar que el aumento en el número de funcionalidades de los sistemas y dispositivos siempre es bueno y bien recibido, pero en el caso de IoT hay que pensar si esas funcionalidades son necesarias y van a ser utilizadas realmente y, sobre todo, si compensan los riesgos que conllevan.

Cualquier funcionalidad no inutilizada es una oportunidad más que tiene el atacante de hacerse con el control de todo el sistema.

La principal recomendación es prescindir del acceso a Internet en los dispositivos IoT, si esto sucede, es imprescindible extremar la cautela y las medidas de seguridad: quién se puede conectar, desde qué dispositivo y en qué momento.

6. Superficies de ataque

Teniendo en cuenta el amplio espectro de soluciones IoT que la industria está proponiendo y que probablemente aumentarán en los próximos años, es interesante ir identificando desde el primer momento los espacios o las ventanas a través de las cuales se pueden producir los ataques.

A continuación, se exponen algunas de las vulnerabilidades que aportan cada uno de los frentes por los que el atacante puede conseguir hacerse con una infraestructura IoT o con los datos que recopila.

Superficie de Ataque	Vulnerabilidad
Control de Acceso al Ecosistema	Confianza implícita entre todos los componentes del sistema. (In)Seguridad en el registro de componentes (*enrollment*). La retirada o jubilación de equipos (*decommissioning*). La pérdida de las credenciales y procedimientos de acceso.
Memoria del dispositivo	Nombres de usuario y contraseñas en claro. Credenciales de terceras partes en claro. Claves de cifrado en claro.

6.1 Superficie de ataque

Superficie de Ataque	Vulnerabilidad
Interfaces físicas del dispositivo	Extracción del Firmware. Interfaz de línea de comando de los usuarios y del Administrador. Posibilidades de escalado de privilegios. Borrado (*Reset*) a un estado inseguro. Extracción de los medios de almacenamiento. (No)Resistencia a las manipulaciones físicas del dispositivo. Presencia de puertos de depuración (p.ej., JTAG[17]). Exposición de número de serie o la identidad del dispositivo.
Interfaz Web del dispositivo	SQL injection, Cross-site scripting y Cross-site Request Forgery. Extracción y listado de nombres de usuarios válidos. La presencia de contraseñas débiles. Posibilidad de bloquear cuentas. Existencia de credenciales por defecto.
El Firmware del dispositivo	Credenciales incrustadas en el código *(hardcoded credentials*). Divulgación de URL e información sensible. Presencia de claves de cifrado en claro. Alteración del cifrado en sí mismo (simétrico y asimétrico). Mostar la versión del Firmware y/o la fecha de la última actualización. Cuentas olvidadas de usuario actuando como puertas traseras. Servicios vulnerables activos (web, ssh, tftp, etc.). Exposición de las API de seguridad del dispositivo. Posibilidad de retornar a una versión anterior insegura.
Servicios de red del dispositivo	Divulgación de información. Interfaz de línea para los usuarios y para el Administrador. Posibilidades de inyección de código. Denegación de servicio. La existencia de servicios no cifrados. El uso de cifrados mal implementados. Presencia de servicios de prueba y/o desarrollo no eliminados o no desactivados en escenarios de producción. Problemas de buffer overflow en el software. UPnP[18] y servicios UDP vulnerables. Las posibilidades de éxito en ataques DoS (*Denegation of Service*). La actualización On The Air (OTA) del Firmware del dispositivo. Las posibilidades de éxito de ataques de Replay. Falta de verificación de las cargas de datos o códigos. Falta de verificación de la integridad de los mensajes, tanto si son datos como comandos

17. Ver https://study.com/academy/lesson/joint-test-action-group-jtag-definition-uses-process.html
18. Ver https://www.redeszone.net/tutoriales/internet/upnp-problema-seguridad-red/

6.1 Superficie de ataque

Superficie de Ataque	Vulnerabilidad
Interfaz Administrativa	SQL injection, Cross-site scripting y Cross-site Request Forgery. Mecanismos de descubrimiento de nombres de usuario válidos. La presencia de contraseñas débiles y credenciales por defecto conocidas. La posibilidad de que se dé el bloqueo de cuentas. La ausencia de opciones de Seguridad/Cifrado y de *logging* seguro. La no autenticación con doble factor. La incapacidad para limpiar de forma segura el dispositivo (*wipe*).
Almacenamiento local de los datos	La presencia de datos no cifrados y/o el cifrado con claves comprometidas. La falta de controles de integridad de los datos. El uso de una misma clave de cifrado/descifrado de todos los datos.
Interfaz Web con la Nube	SQL injection, Cross-site scripting y Cross-site Request Forgery. El descubrimiento de nombres de usuario válidos. La presencia de contraseñas débiles y de credenciales por defecto. El posible bloqueo de cuentas. El no cifrado de lo que se transporta o comunica. La presencia de mecanismo de recuperación de claves y contraseñas que sea inseguro. La falta de autenticación de doble factor.
Backend API de terceras partes	Envío no cifrado de información personal o identificativa. El modo de cifrado de la información personal e identificativa. La divulgación de información interna del dispositivo. La divulgación de la ubicación del dispositivo.
Mecanismo de actualización	El que las actualizaciones se envíen sin cifrar. Que las actualizaciones no vengan correctamente firmadas. Que la URL de las actualizaciones sea modificable. Que no haya o sea ineficaz la verificación de las actualizaciones, o la falta de autenticación de las mismas. La posibilidad de instalar actualizaciones maliciosas. La pérdida temporal o definitiva del mecanismo de actualización. La ausencia de un mecanismo manual de actualización.
Aplicación móvil	La existencia de credenciales por defecto y/o la aceptación o uso de contraseñas débiles. El almacenamiento inseguro de los datos. La ausente o el inadecuado cifrado de lo que se transporta. Un mecanismo inseguro de recuperación de contraseñas y claves. La ausencia de una autenticación de doble factor
Backend API de proveedores	Aceptar como inherente la confianza en las aplicaciones de la nube o móviles. Mecanismos de autenticación débiles. Los controles de acceso inexistentes o débiles. La posibilidad de que tengan éxito los ataques de inyección. La presencia de servicios ocultos y funcionalidades no documentadas.

6.1 Superficie de ataque

Superficie de Ataque	Vulnerabilidad
Comunicación del ecosistema	La ausencia o el abuso de los controles sobre el estado de salud de todo el sistema. Las pruebas de funcionamiento correcto (Heartbeats) del sistema. La (in)seguridad de los comandos que operan el ecosistema. El desaprovisionamiento de recursos o capacidades. El forzado de las actualizaciones.
Tráfico de red	La propia Red de Área Local (LAN). El salto desde la LAN a Internet (enrutador, proxy, cortafuegos, etc.). Las conexiones aéreas de corto alcance. La no estandarización de protocolos y/o procedimientos. Las redes inalámbricas en si (Wi-Fi, Z-wave, Zigbee, Bluetooth). La posibilidad de analizar los dispositivos con técnicas de Protocol fuzzing[19].
Autenticación y Autorización	La divulgación de valores relacionados con la Autenticación/Autorización de claves de sesión, token, cookies, etc. La reutilización de claves de sesión, tokens, etc. La ausencia de autenticación de dispositivo con dispositivo. La nula o débil autenticación del dispositivo con la aplicación y entre el dispositivo y la nube, y viceversa. La no autenticación de la aplicación con la nube, y viceversa. La falta de autenticación de las aplicaciones Web con el sistema en la nube. La falta de técnicas de autenticación dinámica.
Privacidad	La divulgación de datos de usuario. La publicación de la ubicación del usuario a través del seguimiento de su dispositivo. La posibilidad de sistemas con privacidad diferencial, en la que unos pocos monitorizan a todos y nadie les monitoriza a ellos.

La seguridad de la infraestructura IoT frente a los ataques anteriores aumentará con cualquier medida que sirva para mitigar los efectos de cada una de las superficies de exposición. Antes de adoptar cualquier tecnología o implementar una arquitectura basada en IoT, es recomendable hacerse preguntas sobre lo indicado en la tabla anterior.

19. Ver https://www.owasp.org/index.php/Fuzzing

7. Medidas para proteger y/o reducir la superficie de ataque

En el caso de arquitecturas IoT, pocas veces será posible utilizar las mismas medidas de seguridad que se recomienda que estén presentes en los sistemas de las TIC, y con las cuales el usuario está más familiarizado (antivirus, cortafuegos, analizadores de malware, etc.). Sin embargo, hay otras que sí son posibles y que hay que tener muy en cuenta si se pretende trabajar, viajar, vivir, etc. con una infraestructura IoT segura.

7.1 Configuración segura

En general, las características de cada dispositivo IoT variarán bastante de uno a otro, y en algunos casos sí es posible instalar aplicaciones de seguridad (mini cortafuegos, anti-malware, etc.) o al menos modificar el comportamiento del dispositivo (configuración) para hacerlo más seguro. Sin embargo, en otros muchos casos las **limitaciones físicas y lógicas del propio dispositivo harán imposible ese proceso de protección** y en numerosas ocasiones esa imposibilidad está impuesta por el fabricante, en cuyo caso, la única recomendación posible es **renunciar a utilizar ese tipo de tecnología.**

7.2 Actualización

La principal medida de seguridad que se debe seguir con cualquier dispositivo informático, sea IoT o no, es **mantener todo su software y firmware permanentemente actualizado**, ya que esta es la única forma de contar con las últimas correcciones para las vulnerabilidades que hayan sido detectadas. La disminución de vulnerabilidades siempre disminuye el riesgo y la efectividad de las posibles herramientas desarrolladas por los atacantes.

La puntual actualización de los sistemas, además de favorecer su correcto funcionamiento, permite disponer de nuevas características que ofrecen los fabricantes.

En general, el proceso de actualización depende del dispositivo del que se trate. Algunos permitirán la actualización automática mediante conexiones y comprobaciones periódicas en los servidores que tenga activos el fabricante para tal fin, mientras que en otros casos, solo podrán actualizarse manualmente y, por lo tanto, será necesario que el usuario sigua las instrucciones proporcionadas por el fabricante.

7.3 Actualizaciones genuinas

En cualquier caso, la calidad del dispositivo IoT también está relacionada con las medidas de seguridad que ha implementado el fabricante para que el dispositivo solo pueda instalar actualizaciones genuinas y autorizadas por él mismo.

Uno de los procedimientos de ataque más efectivos en los dispositivos IoT es actualizarlos con una actualización falsa, modificada adecuadamente por el atacante. **La integridad y autenticidad de las actualizaciones es un factor a tener muy en cuenta a la hora de adquirir dispositivos electrónicos** de cualquier tipo.

En cualquier caso, **las actualizaciones deben venir firmadas, y dichas firmas deben ser correctamente verificadas antes de proceder** a su instalación. Cabe destacar que **no se debe permitir el retorno a versiones anteriores más inseguras, por lo tanto** la actualización siempre debe ser posterior a la versión que actualiza.

7.4 Cortafuegos y detección de código dañino

Al no ser posible recurrir a la instalación de software antimalware o cortafuegos en el propio dispositivo IoT, la prevención de intrusiones debe hacerse en otras capas interpuestas que se encarguen de gestionar la seguridad de toda la arquitectura.

La medida más recomendable es **configurar correctamente el enrutador que proporciona el acceso a Internet** del dispositivo, de modo que éste filtre las conexiones que pueda haber hacia y desde los dispositivos IoT a los que da conectividad.

El objetivo debe ser restringir el acceso al dispositivo desde redes externas, de forma que, por ejemplo, solo pueda accederse a la configuración de los dispositivos desde un equipo conectado a la misma red local, o bien que las conexiones a Internet y desde Internet se hagan a direcciones IP concretas y verificadas como confiables.

En este escenario hay que **configurar correctamente el enrutador** y establecer **listas de acceso permitido (listas blancas)** para usuarios, dominios y/o direcciones IP concretas.

7.5 Autenticidad e integridad de los comandos

En el caso de que haya que mantener una conectividad exterior para los dispositivos e infraestructuras IoT, lo adecuado es que el sistema disponga de un mecanismo de firma digital que permita verificar criptográficamente la autenticidad de los comandos y las comunicaciones que se establecen.

El sistema IoT debería establecer en todo momento si una conexión remota (Internet) al dispositivo IoT es auténtica o no, y en el caso de que no lo sea, simplemente desestimar la solicitud.

7.6 Conectividad con internet

Es muy aconsejable desactivar cualquier tipo de conectividad remota del dispositivo IoT siempre y cuando no se vaya a hacer un uso inmediato de ella. Tanto los dispositivos Bluetooth, que pueden ser localizados por otros dispositivos cercanos, como los dispositivos conectados a Internet, que pueden aparecer en buscadores específicos, son fáciles de descubrir, y la mejor forma de evitar un ataque es limitar el acceso a ellos.

Hay casos en los que puede parecer que es necesario tener un dispositivo IoT accesible desde el exterior, desde cualquier rincón de Internet, pero siempre conviene responder a la pregunta de si realmente es necesario acceder "¿a mi nevera?" desde cualquier lugar del mundo. Casi siempre la respuesta no es un sí rotundo.

Una solución paliativa del riesgo pasa por establecer cuáles son exactamente las condiciones en las que se necesita permitir esa conexión: ¿desde dónde?, ¿en qué momento?, ¿por parte de quién?, ¿con qué fin?, ¿qué es exactamente lo que se va a permitir hacer?, etc.

7.6 Conectividad con internet

Por ejemplo, si lo que se necesita es poder encender la calefacción de una segunda vivienda para que la temperatura sea confortable al llegar, la conexión con la caldera está perfectamente definida (comando para encender o apagar la caldera), se hará desde dispositivos muy concretos (dirección IP de la residencia principal, teléfonos del propietario o personas autorizadas), realizándose probablemente en fines de semana y períodos de vacaciones (calendario), a unas horas más probables que otras (horario) y en caso de que la temperatura exterior sea inferior a un valor dado, etc. Con esta información se puede limitar la ventana de tiempo y el origen de esa operación remota en la infraestructura IoT.

7.7 Configuraciones de seguridad

Por las exigencias de atender a un mercado más amplio, en la mayoría de los casos, los sistemas IoT incluyen funcionalidades que son necesarias en un momento dado para su puesta en marcha o para su mantenimiento posterior. En este caso, todas las funcionalidades innecesarias deben estar inactivadas en el escenario de explotación.

Para que esto sea posible, existen **mecanismos de configuración** mediante los cuales se determinan cuál va a ser concretamente la funcionalidad a desarrollar por parte del dispositivo en cada escenario. Es muy importante comprobar que los grados de libertad disponibles en el proceso de configuración son suficientes. Esta verificación incluye:

7.7 Configuraciones de seguridad

- Revisar la interfaz administrativa del dispositivo buscando opciones que refuercen la seguridad del sistema, tales como **forzar a que las contraseñas sean robustas.**
- Buscar en la interfaz administrativa el modo de **separar los perfiles de administrador de los de usuarios normales.**
- Revisar la interfaz administrativa en busca de **opciones de cifrado.**
- Revisar la consola de administración viendo si hay opciones para **habilitar el registro seguro de varios eventos de seguridad.**
- Revisar si hay forma de **activar alertas y notificaciones** al usuario final de todos los eventos relacionados con la seguridad del sistema.

7.7 Configuraciones de seguridad

Hacer suficientemente segura la configuración de un dispositivo requiere:

- Asegurar el poder **aislar los usuarios normales de los administradores.**
- Asegurar la capacidad de **cifrar los datos en reposo y en tránsito.**
- Asegurar que se pueda forzar el uso de **políticas de contraseñas robustas.**
- Asegurar la capacidad de activar el **registro de eventos de seguridad.**
- Asegurar la capacidad de **notificar a los usuarios finales la ocurrencia de eventos relacionados con la seguridad.**

7.8 Integridad de software/ firmware

Que las reglas del mercado de la microelectrónica exijan inmensos volúmenes de venta de un mismo elemento para ser económicamente viable, implica la aparición de escenarios IoT que están plagados de dispositivos hardware de propósito general, cuya funcionalidad operativa concreta viene dictada por el software o firmware que ejecutan.

Es muy importante que esos dispositivos universales, desde el principio (arranque) y en adelante (ejecución), **puedan comprobar la integridad de los elementos software que ejecutan** y no puedan ser alterados de modo que terminen haciendo cosas para las que no estaban diseñados.

El control de cualquier arquitectura IoT pasa irremediablemente, en primer lugar, por la capacidad de actualización del software y, en segundo plano, por la posibilidad de cambiar físicamente el funcionamiento del mismo hardware (*firmware*).

7.8 Integridad de software/firmware

Comprobar la presencia de actualizaciones software/firmware inseguras incluye:

- Revisar el fichero de actualización en busca de información sensible que puede quedar expuesta, incluso si lo hace de forma ofuscada.
- Revisar la producción de los ficheros de actualización de modo que implementen un cifrado correcto utilizando algoritmos y procedimientos aprobados.
- Revisar la producción del fichero de actualización y comprobar que siempre va correctamente firmado.
- Revisar la seguridad y robustez del método de comunicación utilizado para transmitir las actualizaciones y dar publicidad de su existencia. Hay que evitar que los sistemas no se actualicen por desconocer que tenían que hacerlo.
- Revisar el servidor de actualizaciones en la red para asegurar que los métodos de cifrado de la comunicación están actualizados y correctamente configurados, y que el servidor de actualizaciones en sí mismo no es vulnerable.
- Revisar el dispositivo para su correcta validación o firmado de los ficheros de actualización.

7.8 Integridad de software/firmware

Asegurar el software/firmware que se ejecuta en un dispositivo requiere:

- Asegurar que el dispositivo tiene la habilidad real de actualizarse. En IoT es muy importante que todo tenga un mecanismo seguro de actualización.
- Asegurar que el fichero de actualización está cifrado utilizando métodos y algoritmos aceptados como seguros.
- Asegurar que el fichero de actualización se transmite a través de una conexión cifrada y que el proceso de instalación o configuración termina con una **fase de autodiagnóstico** positiva. En caso de no ser positiva, el proceso de actualización debería ser completamente revertido.
- Asegurar que el fichero de actualización no expone datos sensibles.
- Asegurar que el fichero de actualización está firmado y que es verificado antes de que se publique la actualización, se distribuya y se aplique.
- Asegurar que el servidor de actualizaciones es íntegro y seguro.
- Implementar el arranque seguro del dispositivo si es posible (secure boot) y su cadena de confianza.

7.9 Seguridad física

Algunos ataques requieren tener acceso físico al dispositivo, por lo que no pueden realizarse de forma remota. Esto será especialmente sencillo en la IoT, ya que los dispositivos estarán junto a aquello que miden u operan, por lo que generalmente no tendrán nada físico que los proteja.

Dado que el atacante va a poder acceder al dispositivo, o aproximarse al él tanto como quiera, es necesario comprobar si las medidas tomadas por cada fabricante son suficientes para proveer la **seguridad física** del dispositivo:

- Revisar la facilidad con la que se podría desmontar el dispositivo y **acceder o extraer sus medios de almacenamiento.**
- Revisar el uso de **puertos externos**, como por ejemplo un USB, para determinar si los datos contenidos dentro del dispositivo pueden ser accedidos sin necesidad de desmontarlo.
- Revisar si todos los puertos físicos externos **son necesarios** para el funcionamiento del dispositivo.
- Revisar la interfaz de administración para determinar si los puertos externos, tales como los USB, **pueden ser desactivados.**
- Revisar la interfaz administrativa para determinar si las capacidades del administrador pueden **limitarse al ámbito local**.

7.9 Seguridad física

Una adecuada **protección física** requiere:

- Asegurar que los medios de almacenamiento no pueden extraerse fácilmente.
- Asegurar que los datos almacenados están **cifrados en reposo.**
- Asegurar que los puertos USB y otros puertos externos no pueden ser utilizados para un acceso dañino al dispositivo.
- Asegurar que el dispositivo **no puede ser desmontado fácilmente.**
- Asegurar que solo se permiten aquellos puertos externos, tales como los USB, que son realmente necesarios para el correcto funcionamiento del dispositivo.
- Asegurar que el producto tiene la **habilidad de limitar las capacidades administrativas.**

8. Conclusiones

La ciberseguridad se enfrenta a un nuevo desafío proveniente de los objetos cotidianos que nos rodean, el Internet de las cosas (IoT). Desde máquinas de café y frigoríficos a asistentes virtuales y cámaras de vídeo, los consumidores están utilizando una nueva ola de dispositivos conectados, aunque rara vez tienen en cuenta las vulnerabilidades que estos pueden conllevar.

Los ataques a la IoT exponen a las empresas a la pérdida de datos y servicios, y pueden hacer que los dispositivos conectados sean peligrosos para los clientes, empleados y para el público en general. Las potenciales vulnerabilidades seguirán creciendo a medida que aumenten los dispositivos dependientes de Internet.

Con la escasa reglamentación existente que responsabilice a los fabricantes de los objetos conectados, estos dispositivos ofrecen una **vía directa de acceso a datos personales, industriales o corporativos, a menudo muy sensibles.**

Mientras tanto, los equipos de seguridad están luchando para hacer frente a un **paisaje de amenazas que cada vez es más complejo**, donde cualquier dispositivo podría estar sujeto a ataques sofisticados.

La mayoría de **los dispositivos IoT no se diseñan ni construyen teniendo en cuenta la seguridad propia y la de otros**, sino que son diseñados en pro de la funcionalidad, su facilidad de uso y su rápido lanzamiento al mercado. Estos equipos son generalmente baratos, útiles y, si es necesario, sencillos de configurar, lo cual suele conllevar un coste para la seguridad.

Lo incipiente de este nuevo paradigma y el hecho de que la mayor parte

Las potenciales vulnerabilidades seguirán creciendo a medida que aumenten los dispositivos dependientes de Internet.

de los ataques a la IoT hayan sido meras pruebas de concepto sin consecuencias serias, no significa que en el futuro los atacantes en el ciberespacio no se vayan a centrar en este mercado.

Un estudio de Hewlett-Packard encontró que el 70% de los dispositivos IoT más utilizados contienen abundantes vulnerabilidades explotables[20] por atacantes. Más aún, el 80% de esos artefactos presentan serios problemas de privacidad, puesto que **recogen datos particulares**, casi siempre innecesarios, **del usuario y sus circunstancias.**

Por el momento, únicamente **la exigencia de seguridad por parte del usuario final y de toda la sociedad** podrá imponer a los fabricantes y al mercado la necesidad de considerar todos estos aspectos **antes de lanzar un producto al mercado**. Esa misma demanda forzará a que las autoridades y los distintos sectores profesionales opten por **medidas de regulación que protejan tanto al ciudadano como a la sociedad en general** de las consecuencias que puede tener poblar el planeta con billones de dispositivos inseguros.

A diferencia de los ciberataques tradicionales, los incidentes relacionados con la IoT no se limitan a extraer información, si no que pueden ser utilizados para **causar daño físico** y ser explotados por ciberatacantes patrocinados por Estados para causar perjuicios graves.

Quizás, asegurar la "cosa" no sea la respuesta, ya que siempre habrá demasiados elementos a manejar. Por el contrario, la observación y monitorización permitirán aumentar la visibilidad, que junto con el análisis y la respuesta oportuna, proporcionarán un enfoque pragmático para reducir los riesgos inherentes al crecimiento de los dispositivos IoT. De esta manera, lo aspectos a considerar serían:

Los dispositivos ofrecen una vía directa de acceso a datos personales, industriales o corporativos, a menudo muy sensibles.

15. Ver http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

8. Consclusiones

Concentrarse en lo que se puede ver. Los dispositivos IoT suelen tener un punto de control, ya sea un enrutador, un cortafuegos o un proxy en el perímetro de la red o en la nube. Es necesario conseguir visibilidad y, cuando sea posible, controlarla.

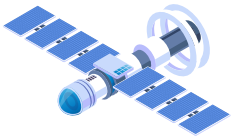
El análisis como mejor amigo. Los dispositivos IoT comparten una característica a menudo pasada por alto, y es que su comportamiento es predecible. La aplicación de "machine learning" para el modelado de comportamiento es extremadamente eficaz para perfilar el riesgo, detectar anomalías y responder.

Disponer de personal dedicado a la seguridad. Nunca se dejará de monitorizar, investigar y remediar, y se debe contar con personal que sepa analizar la situación para articular una adecuada respuesta.

El éxito se reduce a establecer una base de monitorización y control para reducir la exposición al riesgo y aplicar técnicas inteligentes a la creciente población de dispositivos IoT.

9. Decálogo de recomendaciones

A continuación, se indican diez (10) recomendaciones de seguridad para *Arquitectura IoT*



Decálogo de seguridad para Arquitectura IoT

1. **Evitar utilizar dispositivos IoT** siempre que no sean estrictamente necesarios.

2. **No utilizar**, en la medida de lo posible, **aquellos dispositivos IoT que transmiten información a servidores externos** (la Nube), incluso si son los del fabricante.

3. **Cambiar las contraseñas** por defecto de los dispositivos y utilizar contraseñas realmente robustas, que no estén en ningún diccionario, que sean suficientemente largas y por tanto difíciles de adivinar.

4. Mantener actualizados los dispositivos con las **últimas versiones disponibles de software y firmware.**

5. **Desactivar toda conectividad remota** (con Internet) de los dispositivos cuando **no sea estrictamente necesaria.**

6. **Mantener abiertos solo aquellos puertos de comunicación** que sean realmente necesarios y modificar los puertos de escucha si es posible.

7. Si los dispositivos IoT no permiten la configuración de su seguridad, **operar con ellos siempre en una red de área local (LAN)** detrás de un dispositivo (enrutador) correctamente configurado que sí provea esa seguridad.

8. En la medida de lo posible, **asegurar la autenticidad, confidencialidad e integridad en todas las comunicaciones locales (LAN),** especialmente si estas se realizan por enlaces radio (Wi-Fi, Bluetooth, etc.).

9. **Comprobar periódicamente** y sin previo aviso, **la configuración de seguridad** de todos los elementos de la arquitectura IoT y de sus dispositivos de comunicación con el exterior.

10. **Comprobar la visibilidad de los dispositivos propios en buscadores de dispositivos IoT como Shodan.**

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es