INTERNET DE LAS COSAS (IOT, POR SU SIGLAS EN INGLÉS)

Internet de las cosas (IoT, por su siglas en inglés) es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet. Alternativamente, Internet de las cosas es el punto en el tiempo en el que se conectarían a internet más "cosas u objetos" que personas. También suele referirse como el internet de todas las cosas o internet en las cosas. Si los objetos de la vida cotidiana tuvieran incorporadas etiquetas de radio, podrían ser identificados y gestionados por otros equipos, de la misma manera que si lo fuesen por seres humanos.

El concepto de internet de las cosas lo propuso **Kevin Ashton** en el Auto-ID Center del MIT en 1999, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores.

El internet de las cosas debería codificar de **50 a 100 000 millones de objetos** y seguir el movimiento de estos; se calcula que todo ser humano está rodeado de por lo menos **1000 a 5000 objetos**. Según la empresa Gartner, en 2020 habrá en el mundo aproximadamente **26 mil millones de dispositivos** con un sistema de adaptación al internet de las cosas. Abi Research, por otro lado, asegura que para el mismo año existirán **30 mil millones de dispositivos inalámbricos conectados al Internet**. Con la próxima generación de aplicaciones de Internet (protocolo IPv6) se podrían identificar todos los objetos, algo que no se podía hacer con IPv4. Este sistema sería capaz de identificar instantáneamente por medio de un código a cualquier tipo de objeto.

La empresa estadounidense Cisco, que está desarrollando en gran medida la iniciativa del internet de las cosas, ha creado un **"contador de conexiones"** dinámico que le permite estimar el número de "cosas" conectadas ***desde julio de 2013 hasta el 2020***. El concepto de que los dispositivos se conectan a la red a través de señales de radio de baja potencia es el campo de estudio más activo del internet de las cosas. Este hecho se explica porque las señales de este tipo no necesitan ni Wi-Fi ni Bluetooth. Sin embargo, se están investigando distintas alternativas que necesitan menos energía y que resultan más baratas, bajo el nombre de **"Chirp Networks"**.

Actualmente, el término internet de las cosas se usa con una denotación de conexión avanzada de dispositivos, sistemas y servicios que va más allá del tradicional M2M (máquina a máquina) y cubre una amplia variedad de protocolos, dominios y aplicaciones.

La seguridad del Internet de las Cosas pasa por un cifrado punto a punto

El Internet de las Cosas es sin duda uno de los conceptos más interesantes de los últimos meses. Este concepto busca poder conectar a la red absolutamente cualquier objeto, desde una simple lavadora hasta farolas, coches e incluso prendas de ropa. Gracias al Internet de las cosas, también

conocido como IoT (Internet of Things) las posibilidades de un objeto convencional son prácticamente infinitas, siendo los límites nuestra propia imaginación.

Se calcula que a finales de esta década habrá ya más de **18.000 millones de dispositivos conectados a la red**, sin embargo ¿qué va a ocurrir con la seguridad y la privacidad de todas esas conexiones?

Cada dispositivo que se conecta a Internet será tratado como un smartphone o un PC, cada uno individual, con una configuración y una seguridad únicos. No existe, ni existirá, una configuración de seguridad global válida para todos los dispositivos de una red, por lo que uno de los mayores esfuerzos de los desarrolladores es el de garantizar una máxima seguridad para todos los usuarios que impida que terceras personas puedan conectarse a nuestros dispositivos, controlarlos y monitorizar su actividad.

Una vulnerabilidad no es igual de grave si, por ejemplo, se encuentra en una lavadora o en un frigorífico conectado a Internet donde un pirata informático o un usuario con malas intenciones nos pueden gastar una broma de mal gusto que si la vulnerabilidad se encuentra en un elemento de control de tráfico e incluso en los controles de centrales eléctricas o nucleares, donde el pirata informático o usuario malintencionado puede convertirse rápidamente en un terrorista.

Según los últimos estudios realizados, en el mercado negro cada registro de información confidencial y privada de un usuario cuesta alrededor de 150 dólares, lo que llama la atención directamente a los piratas informáticos que buscan cada vez nuevas técnicas con las que recopilar la mayor cantidad de información privada de los usuarios para posteriormente venderla en el mercado negro. Los dispositivos conectados a Internet son una jugosa fuente de información, por lo que sus conexiones deben protegerse de la forma más eficaz posible.

La nube cada vez tiene una mayor importancia en todo tipo de conexiones, tanto IoT como a nivel personal y empresarial. La mayoría de los servidores donde almacenamos información y datos están controladas por terceras empresas privadas y brindan a los gobiernos de accesos remotos, por lo que esta información puede ser realmente valiosa para estas organizaciones.

La mejor forma de proteger todas las conexiones y toda la información que se maneja tanto en las conexiones convencionales a Internet como en lo que se conoce como Internet de las Cosas es el cifrado punto a punto. Si queremos que se garantice la seguridad y la privacidad de los datos estos deben cifrarse antes de salir del dispositivo y viajar cifrados hasta el servidor o dispositivo final, donde ya pueden descifrarse o almacenarse cifrados a la espera de descargarlos de nuevo.

Mientras los cifrados punto a punto no sean obligatorios y se lleven a cabo la seguridad y la privacidad nunca serán completas y siempre tendremos vulnerabilidades desde donde podrán atacar a nuestra información privada.