Dispositivos IoT dentro de la empresa: escenarios de ataque y protección

José Mesa
Coordinador de Investigación de Ciberseguridad en Ingenia

Los aspectos de seguridad a considerar cuando se permite la conexión de dispositivos IoT (Internet de las Cosas, por sus siglas en inglés) a la red de una empresa son múltiples: correcto dimensionamiento y fortalecimiento de la red donde se conectan los dispositivos, análisis y configuración personalizada de los mismos e implementación de políticas de control de *endpoints* o cortafuegos para monitorizar el tráfico y la actividad de cada uno de ellos. Además, deben tenerse en mente los planes de gestión de incidentes y sistemas de monitorización y control frente a cualquier posible brecha de seguridad.

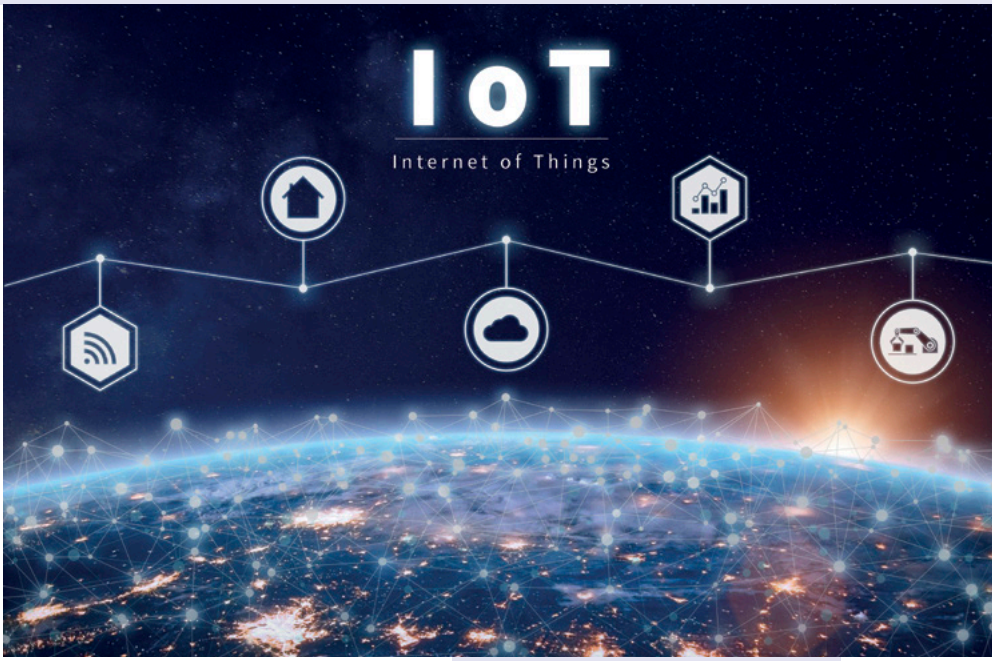
No podemos considerar estos elementos como algo trivial, que se deban dejar al libre arbitrio, ya que muchos de estos dispositivos no tienen en cuenta la seguridad como esquema de diseño durante su fabricación o incluso su ciclo de vida, aunque las empresas estén invirtiendo cada vez más en ello.

Los departamentos de seguridad deben ser los que definan las políticas adecuadas para prevenir los posibles escenarios de ataque que puedan sufrir. Es algo que los CISO de cualquier empresa están empezando a tener muy en cuenta, dadas las repercusiones que pueden acarrear en aquellas firmas que no protejan adecuadamente sus recursos; más aún cuando estos pueden servir como puerta de entrada para recabar información sobre los clientes mediante diferentes tipos de ataques. Aquellos dispositivos IoT o IIoT (*Industrial Internet of Things*) que manejen u obtengan datos privados –por ejemplo, los RFID, dispositivos de identificación o presencia– se verían afectados por la nueva aplicación de la normativa europea sobre protección de datos y el tratamiento de éstos que se lleven a cabo mediante los mismos.

Escenarios habituales

Basándose en lo anterior, es importante conocer los escenarios habituales a la hora de proteger una red IoT ante eventuales ataques:

- **Modificación de las contraseñas por defecto de los dispositivos, que pueden facilitar ataques por fuerza bruta o accesos indebidos por las credenciales de fábrica.** No es raro el día en el que se reciben alertas e informes avisando de ello, y es la primera práctica a realizar. Un nuevo *router* o cámara IP que se instale en la red vendrá con unas credenciales por defecto que son fáciles de averiguar, o incluso son públicas en Internet.
- **Configuración o limitación de los servicios en el dispositivo para evitar accesos externos y una exposición innecesaria.** Al igual que deben alterarse las credenciales de acceso, pueden desactivarse aquellos servicios que no utilicemos. En caso de ser necesario, debe fortalecerse la red a la que se conecten para controlar su uso, segmentándola adecuadamente. Plataformas como Shodan o Censys son ejemplos claros de la recolección de servicios expuestos a Internet, que cualquiera puede utilizar para comprobar la seguridad de estos dispositivos accesibles. Aquellos que no se hayan protegido adecuadamente serán fácilmente accesibles y, por ende, también lo será la entrada a la red. Un ejemplo palpable fue la intrusión sufrida en 2017 por un casino a través del controlador de la pecera, que facilitó el acceso a la red interna para, posteriormente, mediante vulnerabilidades de otros sistemas adyacentes, alcanzar la base de datos de usuarios y filtrar cerca de 10GB de información.
- **Actualización de los dispositivos para evitar ataques por servicios vulnerables.** En muchas ocasiones estos dispositivos se instalan y configuran una vez y no se les vuelve a tener en cuenta mientras funcionen correctamente. Es necesario estar al tanto de las actualizaciones de *firmware* del fabricante para evitar ataques futuros. Una red fortalecida puede servir inicialmente, pero un dispositivo vulnerable expuesto es un aliciente para atraer escaneos e intentos de acceso rápidamente.
- El ataque Blueborne a dispositivos Bluetooth únicamente puede corregirse mediante actualizaciones de *firmware* o del sistema operativo en todos los dispositivos afectados.
- **Control de accesos indebidos mediante vulnerabilidades en las interfaces web o cloud de los dispositivos.** Esto va unido a la cons-



tante actualización del dispositivo, ya que, si su interfaz de acceso y configuración es vulnerable a ataques de inyección de código, podría comprometerse el dispositivo y tener control del mismo, o utilizarlo para realizar ataques masivos a otros dispositivos, como pueden ser los realizados a través de *botnets*. Mirai sigue siendo el máximo exponente hoy en día y el evento que puso en evidencia la capacidad de los ataques a dispositivos IoT en general. Esta *botnet* que utiliza dispositivos IoT como *routers*, discos duros en red (NAS) o cámaras IP, es capaz de comprobar y comprometer dispositivos *online* para añadirlos a su propia red y realizar ataques de denegación de servicio globales o distribuir *malware* una vez se apoderan del dispositivo.

- **Correcto aislamiento de los dispositivos para intentar evitar la alteración de las mediciones realizadas o el tráfico del dispositivo.** Existen dispositivos IoT encargados de realizar mediciones que pueden ser influidas por ataques de denegación de servicio que bloquearían su funcionamiento adecuado, o por intrusiones que alterarían los datos de medición.
- **Abuso de los protocolos de conexión o de las API utilizadas por el dispositivo.** El hecho de que sea posible abusar de ciertos protocolos o comprometer las comunicaciones puede suponer el acceso a información privada o el control total del dispositivo. Los investigadores de Check Point publicaron recientemente una investigación de cómo un fallo en el sistema de identificación de los drones de DJI les permitió acceder a la base de datos del usuario, mostrando los vuelos, fotografías o vídeos realizados.

Estos escenarios sirven para poner en contexto la necesidad de utilizar herramientas y metodologías que permitan controlar, mediante plataformas de inventariado y gestión de vulnerabilidades, todos los activos IoT de los que dispongamos. Existen multitud de herramientas de protección de *endpoints* que facilitan esta tarea, pero es necesario aplicar un control exhaustivo de las redes a las que se conectan, así como un plan de choque en el momento en el que se detecte una vulnerabilidad que ha sido explotada, ya que utilizar solo VPN o segmentar la red no basta.

No podemos considerar los dispositivos IoT como algo trivial, ya que muchos no tienen en cuenta la seguridad como esquema de diseño.

Prevención

Un esquema genérico de protección ayudaría en la tarea de prevenir y controlar estos ataques:

- **Estudio de los dispositivos a implementar.** Es primordial que el dispositivo seleccionado provenga de proveedores conocidos y con cierto soporte, lo cual evitará posteriores quebraderos de cabeza al no obtenerse las actualizaciones adecuadas o ser vulnerables de serie a cualquier tipo de ataque.
- **Políticas de instalación y uso.** Solo los departamentos adecuados deben implementar, instalar y configurar este tipo de dispositivos, evitándo así que cualquier usuario pueda introducir un nuevo dispositivo en la red sin el conocimiento de los administradores, con los peligros que puede acarrear.
- **Identificación de dispositivos.** Si ya estuvieran implementados, se deberían descubrir e identificar todos y cada uno de los dispositivos presentes en la red.
- **Inventariado.** Si no se mantiene un exhaustivo compendio de los dispositivos, no se podrá gestionar adecuadamente su control, actualizaciones o gestión de vulnerabilidades
- **Segmentación.** Para poder controlar adecuadamente estos activos, deben estar configurados en su propia red aislada. Esto facilitará la tarea de llevar un mejor control de los mismos y protegerse ante eventuales ataques o filtraciones de datos, al poder desconectar o bloquear el tráfico adecuadamente.
- **Monitorización.** Debe llevarse un control del tráfico para detectar anomalías en base al comportamiento y el intercambio de indicadores de compromiso, así como la detección de nuevos dispositivos en la red no autorizados.
- **Protección.** El control de estos dispositivos es vital, ya que muchos de ellos, al no estar orientados a la seguridad o no ofrecer actualizaciones o simplemente porque han dejado de tener soporte, suponen una clara exposición en el futuro. También es importante hacer hincapié en la seguridad física del dispositivo, ya que éste puede ser modificado o bloqueado por terceros. ■