Dispositivos IoT en acción

 En agosto de este año, se publicó la ISO/IEC 30141 dedicada al Internet de las cosas (IoT). Debido al rápido crecimiento de estas tecnologías disruptivas, se vio la necesidad de un estándar que garantizase la eficiencia, seguridad y resistencia de estos dispositivos, y así conseguir maximizar los beneficios y reducir los riesgos. Ya existen varios estándares que hacen referencia a la resistencia, seguridad y protección, y este estándar proporciona la arquitectura de referencia para aplicarlos a dispositivos IoT. Esta arquitectura de referencia de IoT está estandarizada a nivel internacional. Además, utiliza un vocabulario común, diseños reutilizables y las mejores prácticas de la industria [1].

Con la cantidad de dispositivos IoT en el mercado y los escasos meses que lleva publicada la ISO/IEC 30141, no podemos esperar que desde ya todos los dispositivos IoT la adopten, pero es un primer paso para encauzar todos los dispositivos IoT en una misma dirección.

Sin ir más lejos, en mayo de este año, sucedió lo que muchos se temían. En Portland, un dispositivo Amazon Echo registro y envió una larga conversación privada. Desde Amazon se investigó y descubrieron que el dispositivo había malinterpretado la conversación regular como comandos para activar el dispositivo y enviar la conversación a uno de los contactos almacenados. Aunque se demostró que la causa había sido accidental y no malintencionada, se vio cómo reaccionarían los consumidores y los medios ante sucesos de seguridad como este. Incidentes de este tipo suponen una mancha en el expediente de cualquier dispositivo IoT, disminuyendo su popularidad y aumentando el miedo y las dudas de los consumidores.

La tendencia creciente de los dispositivos IoT implica que el rango de amenazas será cada vez mayor. La pregunta es: ¿sabremos manejarlo?

Estos dispositivos suponen además un nuevo canal de consumo. Ahora mismo, teniendo un asistente personal en casa, podemos comprar por internet a través de él. Un estudio sobre la compra por voz, comprobó que el comercio electrónico a través de asistentes domésticos digitales como Amazon Echo y

Google Home en el mercado de Estados Unidos supuso $2 mil millones en 2017. Considerando que los consumidores de Estados Unidos gastaron más de $450 mil millones en compras por internet ese año, las compras a través de dispositivos IoT han tenido un comienzo modesto.

Un informe de Javelin muestra que la mayor parte de las personas que poseen un Amazon Echo u otro dispositivo IoT todavía no se sienten cómodas usándolos para realizar pagos. De los aproximadamente 165,5 millones de consumidores estadounidenses que poseen al menos un dispositivo IoT, Javelin descubrió que más de dos tercios de estos afirman que serían un tanto escépticos a la hora de realizar un pago a través de dicho dispositivo [4].

Muchos proveedores de IoT ya están pensando en cómo conseguir que las compras a través de dispositivos IoT sean experiencias satisfactorias y no problemáticas, pero no todos tienen en cuenta la cantidad de riesgos que suponen. Si esos riesgos no son atendidos por compañías interesadas en apoyar las compras a través de dispositivos IoT, la escala potencial del comercio conectado podría resultar en un aumento del fraude de la tarjeta no presente. Además de la pérdida financiera que puede suponer para las empresas, una atención insuficiente a la seguridad también podría llevar a otros incidentes como el que comentábamos de Amazon Echo.

Una de las razones por las que ha aumentado el comercio electrónico es que tanto los PC’s como los*smartphones*proporcionan plataformas de comunicación bidireccional, lo que ha permitido una captura de datos del cliente que ha dado lugar a experiencias de compra mucho más personalizadas. Los dispositivos IoT también recogen datos, tanto que impulsará, casi en su totalidad, la cantidad de datos producidos cada año, aumentando de 218 ZB (un ZB es un billón de GB) en 2016 a 874 ZB para 2021, según Cisco [3]. Las empresas deberían estar preparándose para procesar y almacenar la cantidad de datos que se recuperarán usando estos dispositivos.

Hoy hay 18 mil millones de dispositivos conectados, para 2025 se predice que llegarán a 70 mil millones, lo que significa entre 10 y 20 dispositivos conectados por hogar, ya sean *smartphones*, ordenadores, asistentes, botones, frigoríficos, etc. Esto significa que aumenta la facilidad con la que un malware como Mirai, del que ya hemos hablado, puede encontrar dispositivos desprotegidos y convertirlos en una botnet muy potente. No creo que a Amazon le gustase que su página web se cayera durante el *Black Friday*o el *Cyber Monday*.

Además de los ataques DDoS, los delincuentes cibernéticos pueden utilizar dispositivos IoT para actividades como la falsificación de ubicación geográfica, la instalación de*ransomware*, la realización de pedidos fraudulentos o la participación en el fraude de adquisición de cuentas. Aceptar pedidos desde dispositivos de IoT será una parte importante para generar más ingresos en el futuro, por lo que bloquear todas las transacciones de dispositivos de IoT no es una estrategia antifraude válida para el futuro [2].

¿Están preparándose realmente las empresas para la llegada de todos estos sucesos? ¿Las posibilidades de fallo de los dispositivos y sus consecuencias

publicas? ¿La llegada de cantidades ingentes de datos? ¿La seguridad tanto en sus dispositivos IoT como en sus servicios?

Referencias:

[1] Reference framework for the Internet of Things – Clare Naden, 26-10-2018 https://www.iso.org/news/ref2340.html?utm_medium=email&utm_campaign=ISO%20Newsletter%20November%202018&utm_content=ISO%20Newsletter%20November%202018+CID_149acce897bf37aac32d61095d4d3f43&utm_source=Email%20marketing%20software&utm_term=Read%20more

[2] The Winding Road Toward IoT Commerce: Considering the Opportunities and Risks of Selling Through Connected Devices – CNP y Radial, 2018 https://www.radial.com/sites/default/files/CNP-Radial-White-Paper-IoT-Commerce.pdf

[3] Cisco Global Cloud Index – Cisco, 02-2018

[4] Securing Emerging Channels: Virtual Assistants, The Internet of Things, and Beyond – Javelin Strategy & Research, 07-2018 https://www.javelinstrategy.com/coverage-area/securing-emerging-channels-virtual-assistants-internet-things-and-beyond