¿Cuáles son los riesgos de automatizar los surtidores de gasolina?

En la actualidad, se presta mucha atención a la forma en que las empresas aprovechan las soluciones de automatización para mejorar sus procesos e impulsar la eficiencia. Una de las formas en que esto está ocurriendo es utilizando dispositivos conectados a Internet, conocidos colectivamente como la Internet de las cosas (IOT).

Según los datos recogidos de IOT Analytics, hay más de 7.000 millones de dispositivos IOT en funcionamiento en la actualidad, y este número se triplicará en los próximos 6 años. La introducción y adopción de 5G, que permite una velocidad de datos muy alta, que es requerida por la mayoría de los dispositivos IOT, está contribuyendo a este aumento, permitiendo una gama más amplia de aplicaciones IOT.

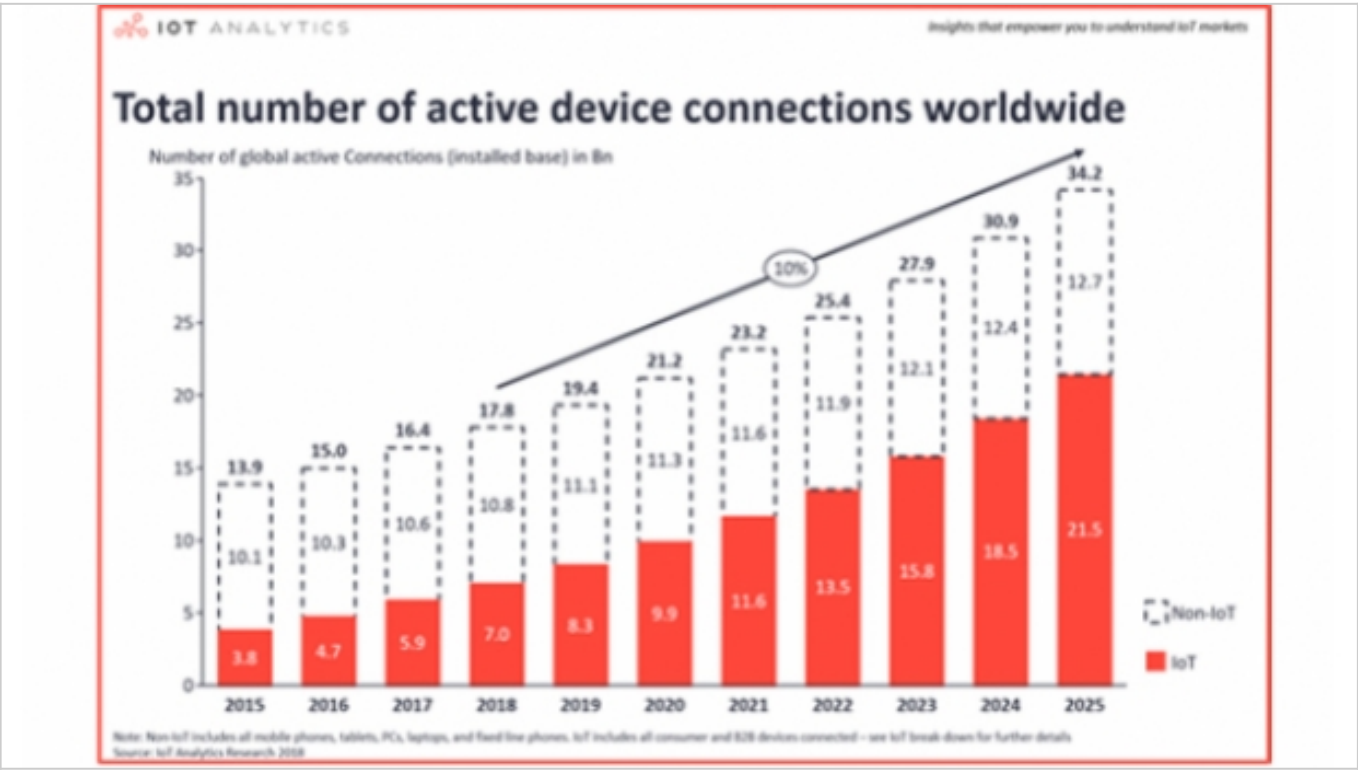
Para el consumidor, no es sólo los medidores inteligentes donde estamos viendo esta optimización - está en todas partes. No es raro ver asistentes personales en el hogar, que se utilizan habitualmente para reproducir música o comprar productos a petición del usuario, lo que permite una experiencia de compra simplificada, mientras que las empresas que prestan estos servicios se benefician de un

mayor conocimiento y, en última instancia, de un mayor número de compras al usuario, simplemente porque es una forma más cómoda de realizar las compras.

El aumento de los dispositivos IOT llevará a un aumento exponencial de la cantidad de datos que se recogen y procesan. Proporcionar grandes oportunidades para la optimización del negocio a través de una visión actualizada de los datos, permitiendo que las tecnologías de aprendizaje de máquinas tomen decisiones automatizadas basadas en las tendencias actuales. Esto se convertirá en parte integral del éxito de las empresas que emplean dispositivos IOT, ya que permitirá mayores oportunidades de automatización y procesos más ágiles. Los sistemas físicos con monitoreo IOT y ML obtendrán beneficios adicionales, tales como capacidades de predicción de oferta y demanda, fallas y mucho más.

Los dispositivos IOT también están mejorando las experiencias de compra para muchas compras hechas en persona. Nos estamos acercando a la edad de la tienda sin personal; ya hay varios de estos en todo el mundo y dependen de un avanzado sistema de cámaras para identificar al comprador y sus compras, para asegurar que se les cobra la cantidad correcta en el momento de la salida, lo que a su vez permite una experiencia más agilizada debido a la eliminación de la cola de espera y el proceso de salida. Un espacio en el que esto está ocurriendo más rápido que otros es en la estación de servicio de combustible. La mayoría de las estaciones de servicio ofrecen ahora la función de "pago en el surtidor", lo que permite al conductor evitar las colas una vez que haya terminado de repostar.

Los negocios de combustible están llevando esto más lejos al aumentar el número de sitios no tripulados, ya que muchos de los servicios ofrecidos en las estaciones de servicio ahora pueden automatizarse, lo que conduce a mayores beneficios para estos negocios. Sin embargo, la comodidad suele tener un coste y, lamentablemente, en esta era de ciberataques a gran escala, los dispositivos IOT se están convirtiendo en objetivos para los estafadores, ya sea para robar información o para utilizar los propios dispositivos como parte de ataques a mayor escala, por ejemplo, en ataques de denegación de servicio distribuidos (DDoS, Distributed Denial of Service).



Recientemente ha habido informes de ataques a bombas de combustible conectadas a Internet, así como guías técnicas en profundidad publicadas en la web oscura con detalles sobre cómo realizar una adquisición de un dispositivo. En el caso de las bombas de combustible, se están manipulando dispositivos para que los atacantes reciban combustible a un precio reducido. En algunos casos, el dispositivo se utiliza como un skimmer de tarjetas, enviando la información de la tarjeta de pago directamente al atacante para venderla en la web oscura. Debido a que estos dispositivos están conectados a Internet con muy poca seguridad, un gran número de bombas pueden ser atacadas a la vez, sin que el atacante tenga que estar presente.

Afortunadamente, la mayoría de estos hacks pueden ser evitados con relativa facilidad - un cambio de la contraseña de acceso por defecto (con una contraseña fuerte) es suficiente para prevenir los ataques a gran escala. ¿Pero qué pasa con la protección de la propia terminal? Estos ataques son más difíciles de prevenir, especialmente en sitios no tripulados. Dado que estos sitios no tienen personal presente para disuadir a los estafadores, se convierten en un blanco obvio para este tipo de ataques. Mi equipo y yo hemos emprendido recientemente un ejercicio para prevenir incluso este tipo de ataque. Donde los miembros de nuestro equipo de fraude visitaron varios sitios no tripulados. Determinamos que las medidas de seguridad básicas, como la instalación de cámaras de seguridad de circuito cerrado de televisión, apuntando a cada terminal de pago de la bomba de combustible, serían suficientes para disuadir a muchos estafadores.

Siguiendo nuestro consejo, estos sitios no tripulados han experimentado un marcado descenso de la actividad fraudulenta y el proveedor de combustible está buscando ahora extender nuestras recomendaciones a través de su red. Esto no sólo reducirá la cantidad de actividad fraudulenta, sino que también disminuirá el coste total de la gestión de los sitios no tripulados y es más probable que

el cliente despliegue más sitios no tripulados para aumentar aún más la optimización.

Los dispositivos IOT son una herramienta poderosa para automatizar y mejorar el conocimiento del negocio, pero requieren algunas medidas de seguridad básicas para garantizar que sigan siendo seguros para que las empresas los utilicen. Es muy emocionante imaginar a dónde nos llevará esta tecnología en los próximos años, pero sin mejoras en la seguridad, podrían convertirse en uno de los mejores blancos para los estafadores del futuro. Si su empresa utiliza dispositivos IOT, asegúrese de que cumplen con las estrictas políticas de seguridad y esté siempre alerta a las modificaciones de hardware y a los ataques remotos para proteger su empresa.

Oliver Tearle es Director de Investigación de The ai Corporation (ai), una empresa de confianza en todo el mundo para el desarrollo de tecnología innovadora que permite a nuestros clientes tomar el control y crecer de forma rentable. Fundada en 1998, tiene un largo historial de ofrecer soluciones a algunas de las instituciones financieras y de pago más grandes del mundo y a los comerciantes internacionales. A través de nuestro enfoque implacable en estas herramientas, nos esforzamos constantemente para ayudar a nuestros clientes a crear retornos altamente rentables.

