El futuro de IoT y su seguridad.

Introducción:

La tecnología sigue creciendo muy rápidamente, en el ámbito de IoT, hay una serie de amenazas a la seguridad que necesitan ser abordadas antes de que sea demasiado tarde.

Desarrollo:

El problema mas común en los dispositivos IoT es la privacidad, estos podrían ser víctima de algún ataque que se aproveche de vulnerabilidades existentes sin parchear o de a una mala política de gestión.

Estos dispositivos son "bastante tontos" y carecen de la capacidad de cómputo para admitir el Estándar de cifrado avanzado.

Estamos atrapados en un modelo de computación cliente-servidor y eso incluye los protocolos de seguridad que lo acompañan. Se necesita un

cambio fundamental en la forma en que abordamos estos problemas y alejamos la conversación del modelo actual.

Los dispositivos IoT son "extremadamente sensibles a los costos" por lo que lo hace otro problema y cuentan con la potencia de cómputo suficiente para funcionar.

Pero dados los más de 10 años de vida útil de los dispositivos de IoT, las campañas podrían necesitar agregar más poder de cómputo para emitir nuevos algoritmos de seguridad capaces de defenderse de futuros ataques que usan computación cuántica para descifrar el cifrado.

Los satélites, desempeñan un papel clave en las redes de IoT, la débil naturaleza de las señales satelitales las hace vulnerables a la falsificación, lo que permite a los piratas informáticos secuestrar dispositivos conectados.

Conclusión:

Nunca puedes estar totalmente seguro, siempre puede existir una gran cantidad de brechas en la tecnología pero es mejor reducir el riesgo a no hacerle caso y tener muchos afectados.

Referencia:

- https://www.mobileworldlive.com/featured-content/home-banner/industry-must-address-urgent-iot-security-threat/

- https://www.welivesecurity.com/la-es/2018/07/25/seguridad-iot-a-tiempo-ganar-batalla/