LITORALPRESS

Fecha: 31-03-2025
Medio: Revista Electro Industria
Supl. : Revista Electro Industria
Tipo: Noticia general
Título: Falta de seguridad en dispositivos ¡IoT pone en riesgo al sector energético en Latam

Pág. : 33
Cm2: 466,5

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

# Falta de seguridad en dispositivos IIoT pone en riesgo al sector energético en Latam

**El sector energético está ampliando el uso de dispositivos de Internet Industrial de las Cosas (IIoT) para impulsar su crecimiento, mejorar la eficiencia y atender a la ciudadanía con mayor eficacia. Aunque esta tecnología puede aportar un valor empresarial significativo, también representa un nuevo vector de ataque crítico que los equipos de seguridad deben defender.**

Se estima que el tamaño del mercado de Internet Industrial de las Cosas será de US$154,14 mil millones en 2025, y se espera que alcance los US$672,20 mil millones para 2030, con un crecimiento del 34,41% durante el período de pronóstico. Tan solo el tamaño del mercado mundial de gestión de energía de IoT se valoró en US$61.020 millones en 2022; se prevé aumentará de US$70.580 millones de dólares en 2023 a US$222.560 millones de dólares en 2030, con una tasa compuesta anual del 17,8%.

"Las inversiones en ciberseguridad de los sectores energéticos suelen destinarse a proteger los datos y los sistemas de información, pero no a los procesos industriales que funcionan a gran escala y tienen sistemas únicos con exigentes requisitos de disponibilidad", afirma Jairo Parra, experto en Ciberseguridad para Akamai LATAM.

Los dispositivos IIoT están cada vez más conectados a través de iniciativas de transformación digital. En los últimos años, el número de ataques de ransomware (tanto logrados como fallidos) a nivel global dirigidos a empresas energéticas ha aumentado notablemente, en un promedio de 37 en 2021 a 62 en 2023, según el último estudio de Akamai. Las consecuencias de estos ataques pueden tener efectos perjudiciales en la población y en las economías, como cortes del suministro eléctrico o daños a infraestructuras, lo que puede provocar que la empresa pierda credibilidad, se roben datos de individuos y empresas, se produzcan cortes de suministro, escasez, riesgos de seguridad, interrupción de la producción y pérdidas financieras o incluso se ponga en riesgo la vida de las personas.

## Recomendaciones para un ambiente IIoT eficaz

Ante dicho escenario, Jairo Parra resalta que "las empresas deben utilizar la ciberseguridad específica para entornos industriales que protejan los dispositivos IIoT". Por ello, recomienda seguir los "cinco controles críticos" para la ciberseguridad industrial del SANS Institute, con el fin de ayudar a las organizaciones a priorizar los controles más importantes y desarrollar un proceso de ciberseguridad eficaz.

Los controles incluyen:

1) Desarrollar un plan de respuesta a incidentes del Sistema de Comando de Incidentes (ICS) en preparación para un ataque.
2) Construir una arquitectura defendible.
3) Obtener visibilidad y monitoreo de la red ICS.
4) Utilizar acceso remoto seguro.
5) Realizar una gestión de vulnerabilidades basada en riesgos que priorice y mitigue las vulnerabilidades adecuadas para entornos industriales de alta disponibilidad.

"Si bien no todos los dispositivos IIoT tienen la capacidad de instalar software de seguridad, acciones como la microsegmentación ayudarán a tener una mejor estrategia de ciberseguridad, ya que se tiene una amplia visibilidad de cómo los activos se comunican entre sí a nivel de proceso de comunicación, quién tiene acceso a qué recurso, permitiendo detectar y bloquear cualquier malware desde su origen, así como evitar movimientos laterales", comenta el experto.

Por último, Jairo Parra reitera que "es indispensable que cada dispositivo que se conecte a la red se configure tomando en cuenta la seguridad. Además, la información que circula dentro de un sistema de IIoT debe mapearse en consecuencia. Reconocer que no existe una defensa perfecta contra las amenazas puede ayudar a crear protocolos de mitigación que puedan contener y reducir significativamente los efectos de un ataque exitoso". ◘