IoT segura para tu empresa

Muchos de los retos a los que se enfrenta el Internet de las Cosas (IoT) tienen que ver con las **limitaciones que tienen muchos dispositivos conectados, como duración de las baterías, ancho de banda, rango de transmisión, interoperabilidad, muchas entre otras**.
Sin embargo, el qué más preocupa tanto a usuarios comunes como a empresas, es el tema de la ciberseguridad.
Para Leonardo Carissimi, director de Soluciones de Seguridad en Unisys para América Latina, **la seguridad cibernética no debe ser un obstáculo para la IoT, sino un facilitador que se puede promover con el uso de numerosas herramientas**, mejores prácticas y experiencias extraídas del mundo de TI.
Según el directivo, para garantizar que la innovación en los negocios y en la seguridad cibernética ésta debe estar esté alineada y se puede lograr en tan sólo cinco pasos:

-Concientizar sobre la seguridad. Este es un principio muy importante del que debe estar consciente todos los empleados que conforman una empresa cuando se adquiere y se implementa nueva tecnología. Empezar de cero y diseñar e implementar arquitecturas que incorporen el tema de seguridad, lo cual debe ser un requisito para todas las decisiones.

-Ciber resiliencia. Es necesario incluir mecanismos de prevención y contención de incidentes. Para eso, se necesitan evaluar las capacidades y funcionalidades de los distintos elementos: sus sensores, sus gateways, sus vulnerabilidades, cuál es la naturaleza de los datos que transitarán, con que aplicaciones interactuarán, y donde están ubicados (centros de datos corporativos, dispositivos móviles, sistemas en la nube); y para quienes están destinados, ya sean empleados, terceros, clientes o socios.

-Mecanismos de contención: Ante un incidente que involucre la seguridad, se debe llevar a la fase de la solución, diseño y despliegue. La tecnología de micro-segmentación puede previamente prevenir el efecto de futuros imprevistos con diferentes perfiles de riesgo. **Si se diseña y despliega la arquitectura de IoT teniendo la contención como principio, las empresas estarán un paso por delante de los delincuentes cibernéticos** en el caso de un acceso exitoso a su infraestructura. Se trata de reducir la Superficie de Ataque, aprovechando la flexibilidad y la escalabilidad que solamente técnicas avanzadas proporcionan. Además, si la micro-segmentación de la red se hace por software, técnicas de reajuste dinámico de los perímetros pueden aumentar la resistencia y la seguridad de la arquitectura.

–Detección de Incidentes. Toda empresa debe asegurar que las alertas pertinentes sean notadas. Por tanto, herramientas de correlación de eventos y plataformas SIEM (Security Incident & Event Management) serán cruciales para hacer frente a este reto.

–Respuesta a Incidentes: En necesaria la detección oportuna para llevar a cabo los procesos y aplicación de herramientas que con ayuda de profesionales calificados puedan corregir las instrucciones de cibercriminales.