IOT CONFIANZA POR DISEÑO

El Marco de confianza IoT de OTA

El advenimiento de las cosas conectadas en nuestra vida cotidiana trae consigo la promesa de comodidad, eficacia y entendimiento, pero también crea una plataforma para riesgos compartidos. Gartner predice que más de 20 billones de dispositivos estarán conectados para el 2020. Desde monitores de actividad física hasta termostatos, cerraduras y electrodomésticos inteligentes, este Internet de las cosas (IoT por sus siglas en inglés) representa un mercado masivo y finalmente redefinirá cómo las personas interactúan con el mundo que las rodea.

La confianza de los consumidores es clave para que IoT florezca y crezca, pero muchos de los productos de hoy en día son lanzados apresuradamente al mercado al menor costo posible con poca consideración por las protecciones básicas de seguridad y privacidad. Esto introduce varios niveles de riesgo tanto para los usuarios como para Internet mismo; desde vigilancia inconsciente y datos comprometidos hasta riesgos físicos (por ej., cerraduras inteligentes) hasta cámaras de seguridad usadas como parte de una red de bots para atacar a Internet. Por defecto, muchos recolectan grandes cantidades de información personal y delicada que puede ser compartida y negociada en el mercado abierto. La mayoría de estos dispositivos no tienen la funcionalidad (o un método fácilmente descubrible) para borrar sin esfuerzo los datos personales de uno.

Ante la ausencia de la puesta en práctica de normas de seguridad y prácticas de privacidad responsables estamos llegando a una encrucijada donde quizá haya que implementar una regulación. Pero en realidad la legislación por sí sola no será eficiente. Aprobar regulaciones tardaría demasiado y nunca podrá seguirle el ritmo al panorama de riesgo, que evoluciona constantemente.

En respuesta más de cien actores representantes de la industria, gobierno y defensores del consumidor contribuyeron a un conjunto recomendado de acciones clave como parte de la Online Trust Alliance (OTA), que ahora es una iniciativa de Internet Society. La puesta en práctica de este Marco de confianza IoT eleva el nivel de seguridad de los dispositivos IoT y los servicios relacionados para proteger mejor a los consumidores y a la privacidad de sus datos. El marco cumple diversas funciones ya que:

- Guía las decisiones de fabricantes y proveedores con respecto al diseño y a las políticas de negocios desde el diseño inicial y a través del ciclo de vida completo del producto,
- Les brinda a los compradores y a los canales de distribución los filtros necesarios para evaluar la privacidad y la seguridad y
- Les da a los legisladores los principios de seguridad necesarios para desarrollar defensa y política económica informada.

Aunque hay otros marcos relacionados a IoT, este arco de confianza de IoT es único de dos formas significativas:

- **Abarca asuntos de seguridad, privacidad y sustentabilidad a largo plazo (ciclo de vida).** Muchos otros se enfocan sólo en la seguridad o interoperabilidad o privacidad, y muy pocos toman en cuenta los asuntos de ciclo de vida asociados con estos productos y servicios, como cómo transferir datos y cuentas relacionadas con un hogar inteligente o que hacer si ya no se encuentran disponibles actualizaciones para un dispositivo de larga vida, como un abridor de una puerta de garaje.

- **Aborda el ecosistema entero de forma holística**. Esto incluye dispositivos/sensores, aplicaciones móviles y servicios de backend. La mayoría de los marcos solo se centran en los dispositivos, pero un sistema sólo es tan fuerte como su parte más débil.

El marco incluye una lista de principios factibles en ocho categorías. Si se los sigue, estos principios pueden reducir los riesgos de seguridad y privacidad, aumentar la confianza y posibilitar la prosperidad del ecosistema IoT:

- **Autenticación –** autentique a dispositivos y a usuarios para prevenir el acceso malicioso.
- **Encriptación –** encripte datos exhaustivamente para prevenir la escucha a escondidas de datos delicados.
- **Seguridad –** la seguridad debe incorporarse a todas las áreas, dispositivos, aplicaciones y servicios de backend, ya sean ofrecidas directamente o a través de terceros. Deberían realizarse pruebas y actualizaciones regularmente para minimizar vulnerabilidades.
- **Actualizaciones –** ponga a los compradores al tanto de la capacidad de actualización del dispositivo y entregue dichas actualizaciones de manera segura y con una mínima intervención o un mínimo impacto sobre el usuario (ej., que se requiera reconfiguración).
- **Privacidad –** divulgue claramente las políticas relacionadas con la privacidad, como aquellas sobre la recolección y el compartir de datos, y limite la recolección a lo justo y necesario para mantener el funcionamiento.
- **Divulgaciones –** las divulgaciones rigurosas, fáciles de encontrar sobre las políticas de privacidad, recolección de datos, funcionalidad con o sin conexión y la duración del soporte/parches permiten al consumidor tomar decisiones informadas.
- **Control –** los consumidores tienen opciones y control sobre los datos recolectados por el dispositivo/servicio y la capacidad de transferir o eliminar los datos en caso de pérdida o venta.
- **Comunicaciones –** las comunicaciones con el consumidor luego de la compra (por ej., información sobre actualizaciones/soporte) deben ser establecidas y aseguradas proactivamente empleando las mejores prácticas para limitar los ataques de ingeniería social.

Asegurar niveles de seguridad y privacidad adecuados para productos y servicios IoT es una responsabilidad colectiva. Los principios del marco pueden ser empleados por una amplia gama de actores para cumplir su papel de proteger a los usuarios y a Internet.

- **Vendedores IoT y la cadena de suministro –** siguiendo estos principios, los vendedores pueden aumentar la confianza del mercado en las soluciones IoT. Para generar consciencia y destacar a los líderes que priorizan la seguridad y la privacidad del consumidor, Internet Society está pidiendo a los vendedores que se comprometan públicamente con los principios del marco.
- **Canales de distribución (ofertas de paquetes, revendedores) –** los principios del marco pueden emplearse como filtro para determinar que productos vender, asegurando mejor seguridad y privacidad para los compradores. Internet Society también está pidiendo un compromiso público por parte de estos actores para que solo ofrezcan productos que apoyan los principios del marco.
- **Legisladores y agencias gubernamentales –** Internet Society está pidiendo que los principios del marco sean usados para guiar políticas, leyes y regulaciones asociadas con productos y servicios IoT para el consumidor para reducir riesgos de seguridad y privacidad para los consumidores y las empresas. Los gobiernos, como grandes compradores de soluciones IoT, también pueden usar el marco como base para sus requisitos de compra.
- **Organizaciones de prueba y reseña de productos –** Internet Society está pidiendo que los principios del marco se incorporen en los procesos de prueba y reseña. Es esto generará conocimiento en los

consumidores sobre sus elecciones de seguridad y privacidad y fomentará mejores decisiones de compra.

- **Consumidores y empresas –** los consumidores y empresas pueden usar los principios del marco como guía para tomar decisiones informadas. Para que esto sea más fácil, Internet Society ha proporcionado listas de verificación para consumidores y empresas que resumen los principios clave.

En resumen, la promesa de comodidad, eficiencia y entendimiento de un Internet de las cosas conectado se ve amenazada por riesgos innecesarios introducidos por seguridad y privacidad insuficientes en la mayoría de los productos y servicios IoT de hoy en día. El Marco de confianza IoT de Internet Society identifica los requisitos clave que deben entender, evaluar y adoptar fabricantes, proveedores de servicio, distribuidores/compradores y legisladores como parte del Internet de las cosas.

0420-1