Estándares mínimos de seguridad en el IoT: Internet Society

Para Megan Kruse, directora de Negocios de Online Trust Alliance, una iniciativa de Internet Society, si un consumidor va a comprar cualquier tipo de dispositivo conectado a internet, debe preocuparse por su privacidad e **investigar la cantidad de datos que recopila este nuevo equipo**.

"Es por eso que **nos hemos unido a Mozilla para pedir a grandes empresas minoristas como Target, Walmart, Best Buy y Amazon que apoyen y apliquen públicamente nuestras pautas de seguridad y privacidad** mínimas y dejen de vender dispositivos conectados inseguros.

"Dado el valor y la confianza que los consumidores depositan en una empresa, éstas tienen un rol singularmente importante para resolver este problema y ayudar a construir un futuro más seguro y conectado. Los consumidores pueden y deben confiar en que, cuando le compren un dispositivo, no comprometerán su privacidad y seguridad. Firmar en estas pautas mínimas es el primer paso para cambiar el rumbo y generar confianza en este espacio".

En total, la carta está **firmada por 11 organizaciones**: Mozilla, Internet Society, Consumers International, ColorOfChange, Open Media & Information Companies Initiative, Common Sense Media, Story of Stuff, Center for Democracy and Technology, Consumer Federation of America, 18 Million Rising, y Hollaback.

En ella, las organizaciones solicitan como mínimo **cinco estándares mínimos de seguridad para dispositivos del Internet de las Cosas (IoT)**.

Comunicaciones cifradas

El producto debe utilizar el cifrado para todas sus funciones y capacidades de comunicaciones de red. Esto garantiza que todas las comunicaciones no sean escuchadas o modificadas en tránsito.

Actualizaciones de seguridad

El producto debe admitir actualizaciones automáticas durante un periodo razonable después de la venta, y debe estar habilitado de forma predeterminada. Esto garantiza que cuando se conoce una vulnerabilidad, el proveedor puede hacer que las actualizaciones de seguridad estén disponibles para los consumidores, las cuales se verifican (mediante algún tipo de criptografía) y luego se instalan sin problemas. Las actualizaciones no deben hacer que el producto no esté disponible durante un período prolongado.

Contraseñas seguras

Si el producto usa contraseñas para la autenticación remota, debe exigir que se utilicen **contraseñas seguras**, incluido el requisito de seguridad de la contraseña. Las contraseñas predeterminadas no únicas también deben restablecerse como parte de la configuración inicial del dispositivo. Esto ayuda a proteger el dispositivo de la vulnerabilidad a ataques de contraseña adivinables, lo que podría resultar en un compromiso del dispositivo.

Administración de vulnerabilidades

El proveedor debe tener un **sistema implementado para administrar las vulnerabilidades en el producto**. Esto también debe incluir un punto de contacto para reportar fallas o un programa equivalente de recompensas de errores. Esto garantiza que los proveedores gestionen activamente las vulnerabilidades a lo largo del ciclo de vida del producto.

Prácticas de privacidad

El producto debe tener una **política de privacidad de fácil acces**o, escrita en un lenguaje que sea fácil de entender y apropiado para la persona que usa el dispositivo o servicio. **Los usuarios como mínimo deben ser notificados sobre cambios sustanciales a la política**. Si los datos se recopilan, transmiten o comparten con fines de marketing, deberían ser claros para los usuarios y, de conformidad con las normativas vigentes de cada país, debería haber una manera de optar por no participar en dichas prácticas.

Los usuarios también deben tener una manera de eliminar sus datos y su cuenta. Esto también debería incluir una política que establezca períodos de retención estándar siempre que sea posible.

“Estos cinco son un subconjunto de nuestro Marco de Confianza de Internet de las Cosas, que es un conjunto más amplio de principios que los fabricantes, revendedores y responsables de políticas pueden usar para ayudar a proteger los dispositivos de IoT y sus datos”, agregó Kruse.