Debido al alza en ataques cibernéticos a dispositivos IoT (Internet de las Cosas), todos estos dispositivos ahora deberán cumplir requisitos de seguridad específicos, según las nuevas propuestas del gobierno.

El objetivo de esta legislación es ayudar a proteger a los ciudadanos y las empresas del Reino Unido de las amenazas de los hackers, que tienen como objetivo en aumento a los dispositivos de Internet de las Cosas.

Al hackear dispositivos IoT, los piratas informáticos pueden construir un ejército de dispositivos que pueden ser utilizados para realizar ataques DDoS para eliminar los servicios en línea, mientras que los dispositivos IoT mal protegidos también servirían como una forma fácil para que los piratas informáticos accedan a redes y otros sistemas por medio de una red.

Las medidas propuestas por el Departamento de Cultura, Medios y Deportes (DCMS), se han desarrollado en conjunto con el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido y se dan después de un período de consulta con expertos en seguridad de la información, fabricantes de productos y minoristas.

> *«Nuestra nueva ley hará que las empresas que fabrican y vendan dispositivos conectados a Internet rindan cuentas y detengan a los piratas informáticos que amenazan la privacidad y seguridad de las personas»,* dijo Matt Warman, ministro de digital y banda ancha de DCMS.

Además, siguen los requisitos voluntarios recomendados de mejores prácticas, pero la legislación exigiría que los dispositivos IoT vendidos en Reino Unido deben seguir tres reglas particulares para poder vender productos, que son:

- Todas las contraseñas de dispositivos conectados a Internet del consumidor, deben ser únicas y no reiniciables a ninguna configuración de fábrica universal.
- Los fabricantes de dispositivos IoT para consumidores deben proporcionar un punto de

contacto público para que cualquiera pueda informar una vulnerabilidad y se actuará de forma oportuna.
- Los fabricantes de dispositivos de IoT para consumidores, deben indicar explícitamente el período mínimo de tiempo durante el cual el dispositivo recibirá actualizaciones de seguridad en el punto de venta, ya sea en la tienda o en línea.

Actualmente no está claro cómo se harán cumplir dichas normas en virtud de cualquier ley futura. Si bien el gobierno ha dicho que su ambición es introducir legislación en esta área, y dijo que esto se haría *«lo antes posible»*, no hay detalles sobre cuándo pueda ocurrir.

Muchos dispositivos conectados se envían con contraseñas predeterminadas simples que en muchos casos no se pueden cambiar, mientras que algunos fabricantes de productos de IoT por lo general carecen de un medio de contacto para informar vulnerabilidades, especialmente si el dispositivo se produce en otro lado del mundo.

Por otro lado, se sabe que los productos de IoT dejan de recibir repentinamente soporte de los fabricantes, y al proporcionar un período de tiempo exacto para que los dispositivos sean compatibles, los usuarios podrán pensar en la seguridad del producto a largo plazo.

Si los productos no siguen estas reglas, la nueva ley propone que estos dispositivos podrían ser potencialmente prohibidos en el Reino Unido.

> *«Si bien el Gobierno del Reino Unido alentó anteriormente a la industria a adoptar un enfoque voluntario, ahora está claro que se necesita una acción decisiva para garantizar que el diseño incorpore una seguridad cibernética sólida»*, dijo Warman.
>
> *«Nuestra nueva ley hará que las empresas que fabrican y vendan dispositivos conectados a Internet, rindan cuentas y eviten que los piratas informáticos amenacen la privacidad y la seguridad de las personas. Significará que los estándares de seguridad sólidos se incorporan desde la etapa de diseño y no se atornillan como una ocurrencia tardía»*, agregó.

Por otro lado, Nicola Hudson, directora de políticas y comunicaciones de la NCSC expresó su opinión:

> *«La tecnología inteligente es cada vez más importante en la forma en que vivimos nuestras vidas, por lo que el desarrollo de esta legislación para garantizar que estemos mejor protegidos es enormemente bienvenido. Les dará a los compradores una mayor tranquilidad de que la tecnología que están trayendo a sus hogares es segura y que problemas como las contraseñas prestablecidas y la interrupción repentina de las actualizaciones de seguridad son cosa del pasado».*

El Reino Unido no está solo en el intento de asegurar el Internet de las cosas: ENISA, la agencia de ciberseguridad de la Unión Europea, también trabaja para lograr una legislación en esta área, mientras que el gobierno de Estados Unidos, también está tratando de regular IoT en un esfuerzo por proteger a los usuarios contra ataques cibernéticos.