Verband der TÜV e.V.

TÜV®

Datum
17. Nov. 2017

VdTÜV-Position: Regulativer Nachbesserungsbedarf für sichere IoT-Produkte in Europa

Das Internet der Dinge bezeichnet die Verknüpfung eindeutig identifizierbarer physischer Objekte (things) über das Internet. Funktionen, Anwendungsbereiche sowie Charakteristika von Produkten verändern sich erheblich und die Komplexität nimmt zu.

Es ist somit die Frage zu stellen, ob der geltende regulative Rahmen für die Produktsicherheit mit Blick auf IoT-Produkte noch anforderungsgerecht ausgestaltet ist oder ob sich Bedarf für gesetzgeberische Nachjustierung, insbesondere auf EU-Ebene, ergibt.

Gemäß Art. 169 AEUV ist der Gesetzgeber verpflichtet, ein hohes Schutzniveau für die Verbraucher sicherzustellen. Der europäische Regulierungsrahmen muss gewährleisten, dass die relevanten Verkehrskreise hinreichendes Vertrauen in die Sicherheit von IoT-Produkten setzen können, damit diese Innovationen die notwendige Akzeptanz erfahren.

Die Vernetzung von Geräten und Maschinen über das Internet zu komplexen Systemen führt zu erweiterten Funktionalitäten, die nicht mehr ausschließlich im einzelnen Produkt selbst, sondern im „Backend-System“ bzw. Produktverbund liegen können. Aufgrund der erweiterten Funktionalitäten und der drastisch höheren Anzahl an digitalen Verbindungen besteht die Möglichkeit potenzieller Zugriffe unbefugter Dritter mit entsprechenden Bedrohungs- und Angriffsszenarien. Diese neuen Funktionalitäten und Produkteigenschaften sollten produktübergreifend geprüft werden.

Damit rückt das Problem der „Robustheit“[1] von IoT-Produkten vor Cyberangriffen unter Produktsicherheitsaspekten in den Mittelpunkt. Zu klären ist, ob und in welchem Umfang die „Robustheit“ zu den einzuhaltenden Sicherheitsanforderungen an ein Produkt zu rechnen ist. Denn sofern ein IoT-Produkt durch entsprechende technische Sicherheitsvorkehrungen gegen Cyberattacken zwingend zu schützen ist, wäre dies auch im Rahmen der erforderlichen Konformitätsbewertung zu beachten bzw. zu überprüfen.

In der allgemeinen Produktsicherheitsrichtlinie (2001/95/EG) wird der Begriff „sicheres Produkt“ wie folgt definiert: ein „sicheres Produkt“ ist „jedes Produkt, das bei normaler oder vernünftigerweise vorhersehbarer Verwendung, [...] keine oder nur geringe, mit seiner Verwendung zu vereinbarende und unter Wahrung eines hohen Schutzniveaus für die Gesundheit und Sicherheit von Personen vertretbare Gefahren birgt“.

Die hier zugespitzte Frage, ob eine missbräuchliche Einwirkung auf das Produkt durch Dritte überhaupt als „Verwendung“ im Sinne des Gesetzes anzusehen ist, und insofern Gegenstand der sicherheitstechnischen Betrachtung zu sein hat, ist damit nicht eindeutig geregelt.

Der Begriff der „vernünftigerweise vorhersehbaren Verwendung“ des Produkts knüpft erkennbar bei den bislang typischen physischen Einwirkmöglichkeiten auf das Produkt an, bezieht sich

[1] Gleichbedeutend werden hierfür auch die Begriffe „Resilienz“ und „Sabotagefestigkeit“ verwendet.

jedoch nicht auf „virtuelle“ Einwirkmöglichkeiten und hieraus ggf. resultierende Gefahren. Somit eröffnet sich eine Regelungslücke.

Auch die sektorspezifischen Richtlinien und Verordnungen nach dem New Approach enthalten keine eindeutigen, konsistenten und hinreichenden Sicherheitsanforderungen an IoT-Produkte mit Blick auf den notwendigen Schutz vor Cyberattacken.

Zudem ist ungeklärt, ob nicht auch bestimmte Produkte, die grundsätzlich aufgrund nur geringer von ihnen ausgehender Gefahren bislang nicht einer unabhängigen Konformitätsbewertung bedürfen, infolge ihrer Vernetzung völlig neu mit Blick auf ihr Gefährdungspotential und notwendige funktionstüchtige Schutzmaßnahmen/-vorrichtungen beurteilt werden müssen. Somit könnte im Zuge einer erforderlichen Neubewertung der Sicherheitsrisiken nunmehr für diese Produkte infolge ihrer Internet-Konnektivität und damit verbundener Missbrauchsgefahren eine unabhängige Drittprüfung notwendig sein.

Die Konformitätsbewertung von IoT-Produkten sollte stets die Aspekte „Safety & Security“ umfassen, denn Produktsicherheit und Informationssicherheit eines IoT-Produkts sind untrennbar miteinander verknüpft. Die erforderliche „Robustheit“ von Produkten sollte zukünftig als Voraussetzung für ein „sicheres IoT-Produkt“ im Sinne von „safe & secure“ betrachtet und gesetzlich definiert werden. Hierfür sind auf EU-Ebene die entsprechenden Voraussetzungen bzw. Klarstellungen zu schaffen, und zwar durch eine entsprechende Erweiterung des Produktsicherheitsbegriffs und der grundlegenden Anforderungen in den sektorspezifischen Richtlinien und Verordnungen. Hierfür dürfte ein horizontaler EU-Rechtsakt streng nach den New Approach Prinzipien mit sektorübergreifender Verbindlichkeit das geeignete Regelungsinstrument sein.

Erste VdTÜV-Handlungsempfehlungen an die EU-Kommission:

1. Zeitnahe und umfassende Überprüfung des europäischen Regulierungsrahmens mit dem Ziel, den Aspekt der Robustheit (Datenschutz und Informationssicherheit) und der erweiterten Funktionalität (Interoperabilität etc.) von IoT-Produkten in die Definition des Produktsicherheitsbegriffes sowie in die grundlegenden Anforderungen an Produkte zu integrieren

2. Eine sorgfältige, risikobasierte Überprüfung, inwieweit zukünftig für IoT-Produkte eine entsprechende Erweiterung des Umfangs und der Art und Weise der Konformitätsbewertung sowie Begutachtung, insbesondere durch unabhängige und qualifizierte Dritte erfolgen muss oder gar neue Prüfverfahren notwendig sind