TÜV®

Datum
17. Nov. 2017

VdTÜV-Position: Informationssicherheit von „smart products“ in Europa

Das Internet der Dinge (Internet of Things – IoT) ist eine Generation neuer Produkte und Dienstleistungen, die miteinander kommunizieren können. Gemeint sind hiermit alle Produkte, Anlagen, Systeme und Anwendungen, die softwarebasiert operieren und Netzzugang haben, also „smarte“ Eigenschaften haben und somit „smart products“ sind. Bei diesen Produkten handelt es sich auch um Produkte des öffentlichen Interesses, wie z. B. Medizinprodukte, Aufzüge oder Spielzeuge. Es ist ein dynamisch wachsender Markt, dessen Bedeutung ständig zunimmt. Das BMWi geht davon aus, dass „bis zum Jahr 2020 ca. 20-50 Milliarden Geräte [...] über das Internet verbunden sein“ werden.[1]

Der europäische Gesetzgeber ist insbesondere verpflichtet, ein hohes Schutzniveau für die Verbraucher sicherzustellen.[2] Der Regulierungsrahmen muss somit gewährleisten, dass die relevanten Wirtschaftsteilnehmer hinreichendes Vertrauen in die Sicherheit von „smart products“ setzen können, damit diese Innovationen die notwendige Akzeptanz erfahren und Wachstumspotentiale ausgeschöpft werden.

Es stellt sich jedoch die Frage, ob der geltende regulative Rahmen für die Produktsicherheit mit Blick auf „smart products“ anforderungsgerecht ausgestaltet ist oder ob sich insofern Bedarf für gesetzgeberische Nachjustierungen ergibt.

Informationssicherheit ist Teil der wesentlichen Sicherheitsanforderungen

Eine Vielzahl von Produktsektoren regelt der europäische Gesetzgeber auf Basis des Regulierungsinstruments „New Legislative Framework (New Approach)“.[3] Danach dürfen Hersteller nur solche Produkte in Verkehr bringen, welche die „grundlegenden Sicherheits- und Gesundheitsschutzanforderungen“ erfüllen. Diese werden in Richtlinien bzw. Verordnungen für zum Beispiel Aufzüge, Druckgeräte, Haushalts- und Gartengeräte, Spielzeuge und persönliche Schutzausrüstungen näher beschrieben.

Die Spielzeugrichtlinie differenziert zum Beispiel hinsichtlich der wesentlichen Sicherheitsanforderungen[4] zwischen allgemeinen und besonderen Sicherheitsanforderungen:

- Allgemeine Sicherheitsanforderungen gemäß Artikel 10 (2)

1 Pressemitteilung des Bundesministeriums für Wirtschaft und Energie vom 07.02.2017 „Staatssekretär Machnig: Sicheres Internet gelingt nur mit sicheren Geräten“ (https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2017/20170207-staatssekretaer-machnig-sicheres-internet-gelingt-nur-mit-sicheren-geraeten.html)
2 Vgl. Art. 169 AEUV (http://www.aeuv.de/aeuv/dritter-teil/titel-xv/art-169.html)
3 Für weiterführende Informationen zum New Legislative Framework (New Approach) siehe: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en
4 Vgl. Art. 10 (1) Richtlinie 2009/48/EG (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:170:0001:0037:de:PDF)

„Spielzeuge, einschließlich der darin enthaltenen chemischen Stoffe, dürfen bei bestimmungsgemäßem oder vorhersehbarem Gebrauch und unter Berücksichtigung des Verhaltens von Kindern die Sicherheit oder Gesundheit der Benutzer oder Dritter nicht gefährden."

- Besondere Sicherheitsanforderungen nach Anhang II

  „Der Hersteller hat eine Sicherheitsbewertung des Spielzeugs betreffend chemischen, physikalischen, mechanischen, elektrischen, Entflammbarkeits-, Hygiene- und Radioaktivitätsgefährdungen gemäß Anhang II durchzuführen."

Der Hersteller ist also bereits nach geltendem Recht zwecks Erfüllung der allgemeinen Sicherheitsanforderungen verpflichtet, geeignete Schutzmaßnahmen zu treffen, um jederzeit einen sicheren Gebrauch bzw. Zustand des Produktes oder der Anlage bei bestimmungsgemäßem oder vorhersehbarem Gebrauch zu gewährleisten. Dies bedeutet, dass der Aspekt der Informationssicherheit von sicherheitsrelevanten Bauteilen oder Funktionen von Produkten und Anlagen (u.a. Software, Hardware, Sensorik, Konnektivität) bei der Ausgestaltung von Schutzmaßnahmen seitens des Herstellers im Rahmen der obligatorischen Sicherheitsbetrachtung bzw. Risikoanalyse (Safety- und Risk-Assessment) umfassend zu berücksichtigen ist. Dies ist erforderlich, um eine Gefährdung der Benutzer oder Dritter auszuschließen. Somit ist Informationssicherheit aufgrund der rechtlichen Vorgaben als integraler Bestandteil der funktionalen Sicherheit von Produkten und Anlagen anzusehen.

Informationssicherheit muss auch Teil der konkretisierenden Sicherheitsanforderungen sein

Der Aspekt Informationssicherheit kann im oben genannten Beispiel für die Produkteigenschaften von Spielzeug und deren Gefährdungspotential maßgeblich sein. Dieser wesentliche Aspekt fehlt jedoch bei der Beschreibung der besonderen, konkretisierenden Sicherheitsanforderungen im Anhang II der Spielzeugrichtlinie. Gleichzeitig ist zu überlegen, inwiefern der Schutz der Privatsphäre bzw. Daten-Selbstbestimmung als wichtige Anforderung in der Richtlinie ebenfalls Beachtung finden sollte.

Gleiches gilt für die konkretisierenden Sicherheitsanforderungen anderer sektoraler Richtlinien und Verordnungen im Zuge der New Approach Gesetzgebung[5] sowie für die allgemeine Produktsicherheitsrichtlinie[6], die auf nicht spezifisch geregelte Verbraucherprodukte Anwendung findet.

Diese Regelungslücken mögen auf den ersten Blick verwundern, sind aber durchaus nachvollziehbar. Die rasante technologische Entwicklung im Bereich IT und die damit einhergehende weitreichende Veränderung originärer Produkteigenschaften war zum Zeitpunkt der Erarbeitung der meisten Richtlinien und Verordnungen noch nicht in dieser Dimension absehbar.

Vorgenannte regulative Mängel in den aktuellen Anhängen der Richtlinien und Verordnungen erzeugen Unklarheiten hinsichtlich der bereits heute konkret und notwendig einheitlich zu berücksichtigenden Informationssicherheitsaspekte eines „smart products". Eine konsequente

[5] Siehe u.a. Richtlinie 2014/35/EU (Niederspannung), Richtlinie 2014/33/EU (Aufzüge), Richtlinie 2014/68/EU (Druckgeräte) und Verordnung 2016/425/EU (Persönliche Schutzausrichtung).

[6] Vgl. Richtlinie 2001/95/EG (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:011:0004:0017:de:PDF)

und einheitliche Risikoanalyse von „smart products“ sowie eine einheitliche Konformitätsbewertung ohne harmonisierte Vorgaben ist mit Blick auf die Informationssicherheit von „smart products“ kaum möglich. Zudem resultieren hieraus Rechtsunsicherheiten sowie unkalkulierbare Haftungsrisiken für „smart products“.

Gefährdungspotential von „smart products“ risikobasiert überprüfen

Die New Approach Gesetzgebung sieht vor, dass die Konformität eines Produktes mit den Anforderungen unter Anwendung eines risikobasierten Ansatzes mit unterschiedlichen Verfahren festgestellt und erklärt wird (CE-Kennzeichnung). Je nach Gefährdungspotential des Produktes variieren die anzuwendenden Konformitätsbewertungsmodule zwischen einer reinen Herstellerselbsterklärung bis hin zur obligatorischen Einbindung einer unabhängigen Prüfstelle (Benannte Stelle).

Bei einem „smart product“ mit grundsätzlich geringem Gefährdungspotential kann mit Blick auf den – nunmehr aufgrund der technologischen Entwicklung zunehmend hinzutretenden – Informationssicherheitsaspekt ein neues, deutlich erhöhtes Gefährdungspotential entstehen. Eine angemessene und verlässliche Qualität der Risikoanalyse des Herstellers betreffend sämtlich relevanter Informationssicherheitsaspekte des „smart products“ muss dabei sichergestellt sein. Vor diesem Hintergrund ist seitens des europäischen Gesetzgebers zu überprüfen, ob eine Benannte Stelle aufgrund des gegebenenfalls erhöhten Gefährdungspotentials bestimmter „smart products“ einzubeziehen ist.

Prüfung der Informationssicherheit erfordert Zugang zu Schnittstellen und Software

Um den Aspekt der Informationssicherheit im Rahmen der Produkt- und Anlagensicherheitsüberprüfung angemessen einzubeziehen, benötigt die unabhängige Prüfstelle zukünftig einerseits umfassenden Zugang zur produktsicherheitsrelevanten Steuerungstechnik und deren Software sowie den digitalen Schnittstellen der „smart products“ und ihren Daten. Andererseits muss der Hersteller die Benannte Stelle zukünftig auch über Änderungen der IT-Komponenten (z.B. Software-Update oder -Erweiterungen) informieren, damit diese Veränderungen des „smart products“ und den damit verbundenen Einfluss auf die Produktsicherheit bewerten kann.

Für diese Zugangsrechte und Meldepflichten muss der europäische Gesetzgeber die entsprechenden Voraussetzungen, insbesondere klare Rechte und Pflichten sowie Prüfkompetenzen schaffen.

Dies gilt umso mehr, als dass auch im Rahmen wiederkehrender Prüfungen von „smart products“ mit einem hohen Gefährdungspotential die IT-Aspekte abzuprüfen sind, um den Sicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg umfassend Rechnung zu tragen.

Fazit: Informationssicherheit nach New Approach Prinzipien europäisch regeln

Der regulatorische Rahmen muss mit den technologischen Entwicklungen und Innovationen in Europa fortlaufend Schritt halten. Im Sinne eines insgesamt kohärenten EU-Rechtsrahmens ist das seit 30 Jahren innovationsfreundliche und flexible Regelungsinstrument des New Approach

auch mit Blick auf die Informationssicherheit konsequent anzuwenden. Präzise rechtliche Vorgaben durch Richtlinien und Verordnungen sind für die umfängliche Beurteilung aller maßgeblichen Informationssicherheitsaspekte bereits vor Vermarktung der „smart products“ das geeignete Mittel. Die besonderen Sicherheitsanforderungen mit Blick auf Informationssicherheitsaspekte sollten dort entsprechend präzisiert werden.

Richtlinien und Verordnungen, die aktuell oder in Zukunft überarbeitet werden (z.B. allgemeine Produktsicherheit und Aufzüge), sollten vorgenannte Anforderungen umfassend und technologieoffen berücksichtigen, um mit den smarten Produktentwicklungen Schritt zu halten.

Auch auf untergesetzlicher, insbesondere normativer Regelungsebene (CEN, CENELEC und ETSI-Normen) sind die technischen Bewertungsgrundlagen für die Informationssicherheit von „smart products“ bzw. für die entsprechende Konformitätsbewertung zu definieren und auszugestalten. Die EU-Kommission muss hierfür durch die Erteilung entsprechender Normungsmandate die Grundlagen setzen. Nur durch ein enges Zusammenspiel von Gesetzgebung und Normung kann die notwendige Konvergenz für einen einheitlichen Informationssicherheitsrahmen für „smart products“ in Europa schnellstmöglich sichergestellt werden.

Die EU-Kommission ist im Rahmen der Überprüfung des europäischen Regulierungsrahmens für „smart products“ aufgefordert:

(a) Den Aspekt der Informationssicherheit in den konkretisierenden Sicherheitsanforderungen für „smart products“ in den jeweiligen Anhängen der Richtlinien und Verordnungen nach New Approach ergänzend aufzunehmen und damit Regelungslücken zügig zu schließen.

(b) Die von „smart products“ ausgehenden Gefährdungspotentiale unter Berücksichtigung der Informationssicherheit einer grundlegenden Neubewertung zu unterziehen.

(c) Die anzuwendenden Konformitätsbewertungsverfahren gemäß des neu ermittelten Risikopotentials des „smart products“ (auf Basis der einschlägigen Konformitätsbewertungsmodule) zu überprüfen und anzupassen.

(d) Sofern das Risikopotential des „smart products“ durch die IT-Komponenten erheblich steigt, vorzusehen, dass eine unabhängige Stelle (Benannte Stelle) obligatorisch einzubeziehen ist.

(e) Sofern das „smart product“ von einer Benannten Stelle überprüft werden soll, dieser einen hinreichenden Zugang zu Quellcodes/ Software des Produkts einzuräumen.