Policy Sheet Europawahl 2019

INFORMATIONSSICHERHEIT

Vertrauen in vernetzte Produkte und Anlagen durch Zertifizierungen unabhängiger Dritter fördern!

Die Digitalisierung steht in einer Reihe mit zahlreichen wirtschaftlichen Trends für einen enormen technologischen Wandel, der neue Märkte hervorbringt und brancheninterne Spielregeln radikal umwälzt. Produkte und Anlagen, wie Spielzeuge, Haushaltsgeräte, Medizinprodukte oder Aufzüge, werden zunehmend mit Sensoren ausgestattet und sind digital vernetzbar. Das sogenannte Internet der Dinge (Internet of Things/IoT) dringt so in alle Wirtschafts- und Lebensbereiche vor. Mit dem technologischen Fortschritt steigt allerdings auch die technologische Verwundbarkeit, wie Cyberangriffe immer wieder zeigen. Die Informationssicherheit von Produkten und Anlagen (im Folgenden IoT-Produkte) rückt damit immer mehr in den Fokus.

Der europäische Gesetzgeber ist verpflichtet, ein hohes Schutzniveau der IoT-Produkte für die Verbraucher sicherzustellen. Der aktuelle regulative Rahmen für die Produktsicherheit ist in Bezug auf Informationssicherheit jedoch lückenhaft. Um die Sicherheit von IoT-Produkten zu gewährleisten, bedarf es mehrerer Schritte: Einer grundsätzlichen Erweiterung des Produktsicherheitsbegriffs, einer Analyse des Gefährdungspotenzials von IoT-Produkten sowie der Erweiterung bestehender Konformitätsbewertungssysteme.

DIE AKTUELLE LAGE

Steigende Anzahl an vernetzten Geräten, wachsende Bedrohung durch Cyberangriffe

- Für das Jahr 2017 wird die Zahl der weltweit vernetzten Objekte auf ca. 27 Milliarden geschätzt. Bis ins Jahr 2030 soll diese auf 125 Milliarden steigen[1].
- Laut einem Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) existieren mehr als 800 Millionen Schadprogramme weltweit, zu denen jeden Tag 390.000 weitere Varianten hinzukommen[2].

Erweiterte Funktionalität von IoT-Produkten führt zu höherem Gefährdungspotenzial

- Die Vernetzung von Produkten und Anlagen über das Internet zu komplexen Systemen führt zu erweiterten Funktionalitäten, die nicht mehr ausschließlich im einzelnen Produkt selbst, sondern im Netzwerk, in einer Cloud bzw. im Produktverbund liegen können.
- Aufgrund der drastisch steigenden Anzahl an digitalen Verbindungen nimmt die Möglichkeit potenzieller Zugriffe unbefugter Dritter zu, mit entsprechenden Bedrohungs- und Angriffsszenarien.
- Bei einem Produkt mit für sich genommen geringem Gefährdungspotential kann durch die Vernetzung ein neues, deutlich erhöhtes Gefährdungspotential entstehen. Auch Anlagen bzw. ihre Bestandteile sind zunehmend mit dem Internet verbunden. Dadurch steigt die Vulnerabilität komplexer Industrieanlagen durch Hackerangriffe.

1 IHT Markit (2017), The Internet of Things: A movement, not a market, https://cdn.ihs.com/www/pdf/IoT_ebook.pdf
2 BSI (2018), Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=5

Informationssicherheit weitgehend nicht in EU-Richtlinien und Verordnungen berücksichtigt

- Der Produktsicherheitsbegriff im europäischen Regulierungsrahmen (Produktsicherheitsrichtlinie, 2001/95/EG) umfasst nur den Aspekt der potenziellen Auswirkungen des Produkts (Produktsicherheit, Safety) bei bestimmungs-gemäßem Gebrauch und vorhersehbarer Fehlanwendung. Der notwendige Schutz vor potentiellen Einwirkungen auf das Produkt durch Dritte (Informationssicherheit, Security) ist bislang nicht vom Produktsicherheitsbegriff umfasst.
- Auch in den sektorspezifischen Richtlinien und Verordnungen ist der Aspekt der Informationssicherheit weitestgehend nicht berücksichtigt.
- Damit ist eine umfassende Risikoanalyse und der angemessene Umgang mit Gefährdungen durch Produkt-bauteile und -funktionen, wie Software, Hardware, Sensorik und Konnektivität, europaweit nicht konsequent und einheitlich geregelt.

UNSERE POSITIONEN

Produktsicherheit (Safety) um Informationssicherheit (Security) erweitern

- Der klassische Produktsicherheitsbegriff (Safety) muss auf europäischer Ebene um den Aspekt der Informations-sicherheit (Security) erweitert werden. Ein IoT-Produkt muss „safe“ und „secure“ sein.
- Die Informationssicherheit muss bei der Erarbeitung und Überarbeitung sektoraler (produktspezifischer) Richtlinien und Verordnungen mit aufgenommen werden.

Gefährdungspotenzial von IoT-Produkten risikobasiert überprüfen

- Ebenso muss die Anwendung der Konformitätsbewertungsmodule bei der Erarbeitung und Überarbeitung sektoraler (produktspezifischer) Richtlinien und Verordnungen an das neu bewertete und ggf. gestiegene Gefährdungspotenzial von vernetzten Produkten angepasst werden.
- Sofern das Risikopotenzial eines Produkts oder einer Anlage durch die Vernetzung steigt, sollte eine unabhängige notifizierte Stelle (Benannte Stelle) obligatorisch bzw. umfangreicher in das Konformitätsbewertungsverfahren (z.B. Zertifizierung) eingebunden werden.

Zugang zu Schnittstellen und Software von IoT-Produkten ermöglichen

- Unabhängige Konformitätsbewertungsstellen und notifizierte Stellen benötigen zu Prüfzwecken uneingeschränkten Zugriff auf produktsicherheitsrelevante Steuerungstechnik und deren Software.
- Der Hersteller muss die notifizierte Stelle über Änderungen der IT-Komponenten (z.B. Software-Updates oder Software-Erweiterungen) informieren, damit diese deren Einfluss auf die Produkt- und Informationssicherheit (Safety und Security) bewerten kann.
- Für diese Zugangsrechte und Meldepflichten muss der europäische Gesetzgeber die entsprechenden rechtlichen Voraussetzungen schaffen.

Kontaktdaten

Ansprechpartner: Daniel Pflumm
E-Mail: daniel.pflumm@vdtuev.de
Tel.: +49 30 760 095 470
www.vdtuev.de/europawahl-2019/