EU 2019-2024

Agenda für Sicherheit und Vertrauen im digitalen Binnenmarkt

https://www.vdtuev.de/europawahl-2019/

Der europäische Binnenmarkt ist eine Erfolgsgeschichte

Mit harmonisierter Gesetzgebung, gemeinsamen Normen und Standards sowie dem freien Warenverkehr wurden Wohlstand und viele Arbeitsplätze in Europa geschaffen.

Der digitale Binnenmarkt hat großes Potenzial, an diese Erfolgsgeschichte anzuschließen – mit freiem Datenverkehr und einem europäischen Weg der Digitalisierung. Jetzt gilt es, den digitalen Binnenmarkt weiterzuentwickeln und eine Perspektive für das nächste Jahrzehnt zu entwerfen.

Sicherheit und Vertrauen spielen für den digitalen Binnenmarkt eine entscheidende Rolle. 63 Prozent der Deutschen etwa haben Angst davor, dass autonome Fahrzeuge gehackt werden (TÜV Mobility Studie 2018). 68 Prozent der Nutzer haben kein Vertrauen in die eingebauten Sicherheitsfunktionen von Smart Home Geräten (VdTÜV-Studie 2019).

Aber auch Unternehmen stehen vor der Frage, ob sie etwa Künstliche Intelligenz einsetzen können, ohne ein Sicherheitsrisiko einzugehen. Wie sicher sind Geschäftsgeheimnisse? Wie gut sind Kundendaten geschützt? Auch für den Staat ist digitale Sicherheit von höchster Relevanz. Das zeigen die Hackerangriffe auf den Deutschen Bundestag oder die Beeinflussung des US-Wahlkampfs.

Mit anderen Worten: Cybersecurity und Datenschutz sind die Schlüsselthemen für eine nachhaltige Digitalisierung von Wirtschaft, Staat und Gesellschaft.

Industrie 4.0 und das Internet der Dinge

Industriestandort Europa zum Vorreiter für sichere digitale Produkte und Anlagen machen!

Produktsicherheit um Informationssicherheit erweitern

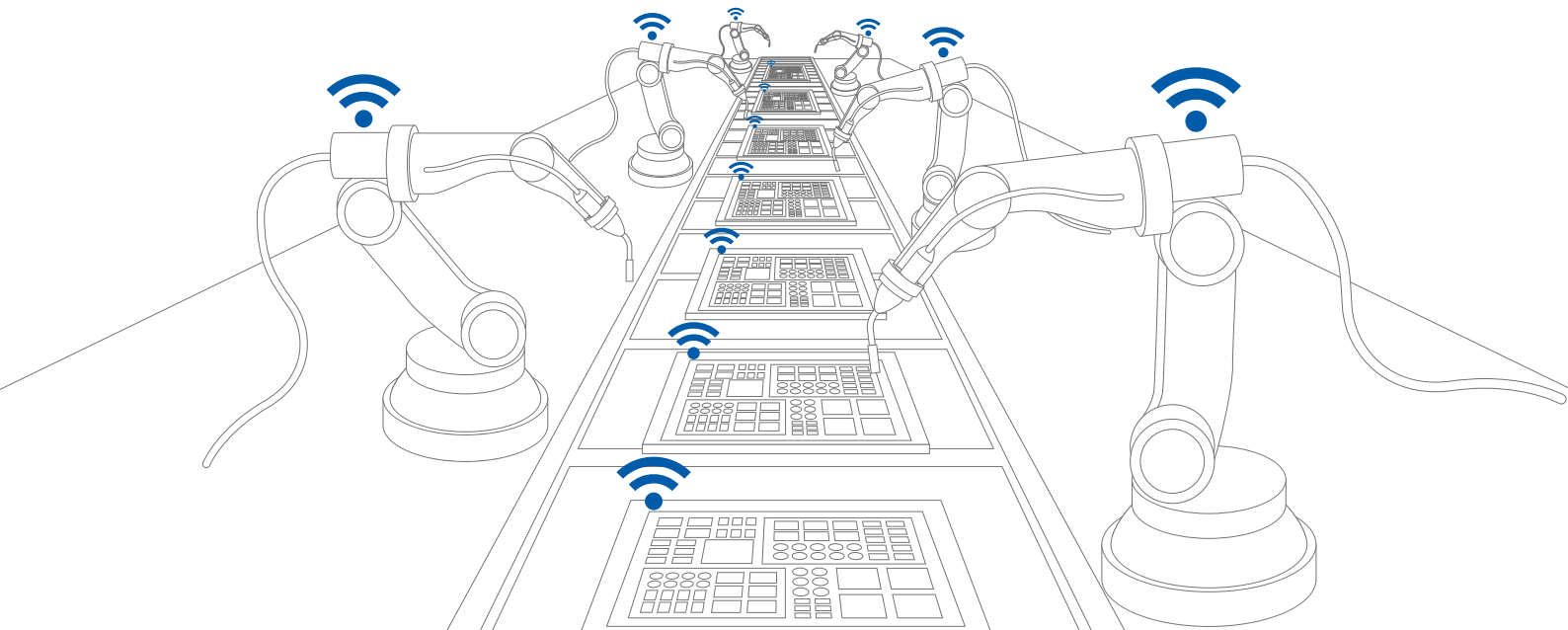
Mit Software und der Vernetzung mit dem Internet hängt die Sicherheit von Autos, Spielzeugen, Kühlschränken oder Maschinen nicht mehr nur von deren materieller Beschaffenheit, sondern zusätzlich von digitaler Sicherheit ab. Eine vernetzte Spielzeugpuppe etwa kann aus schadstoffarmen Stoffen bestehen, aber mit einer offenen Bluetooth-Schnittstelle ein Einfallstor für Hacker sein und so zum Sicherheitsrisiko werden. Um die Sicherheit von Produkten im Internet of Things (IoT) zu gewährleisten, muss der europäische Produktsicherheitsbegriff neben dem bestehenden Fokus auf Safety – also dem Schutz vor potenziellen Auswirkungen des Produktes selbst – auch um den Aspekt der IT-Security – dem Schutz vor Einwirkungen durch Hacker und unbefugte Dritte – erweitert werden.

Digitale Gefahren risikobasiert prüfen

IoT-Produkte und -Anlagen, wie zum Beispiel Aufzüge, müssen zukünftig auch digitale Sicherheitsanforderungen erfüllen, bevor sie auf den europäischen Markt kommen. Hierzu müssen die produktspezifischen EU-Rechtsakte auch mit Blick auf die anzuwendenden Konformitätsbewertungsmodule an das neue Gefährdungspotenzial von vernetzten Produkten und Anlagen angepasst und entsprechend nachgeschärft werden. Sofern das Risikopotenzial eines Produktes durch die Vernetzung signifikant steigt, wenn Gefahren für Leib und Leben oder die Privatsphäre des Nutzers drohen, sollte eine unabhängige Benannte Stelle obligatorisch in das Verfahren für die Konformitätsbewertung mit eingebunden werden. Der Cybersecurity Act weist in die richtige Richtung, jedoch darf es hier auf europäischer Ebene in Sachen Cybersicherheit von IoT-Produkten mittelfristig nicht nur bei freiwilligen Maßnahmen bleiben.

Zugang zu Software für unabhängige Tests regeln

Die Software bei Produkten hat einen immer größeren Einfluss auf deren Sicherheit. Das gilt für Aufzüge ebenso wie für Zapfsäulen. Ist die Software fehlerhaft oder nicht aktuell, bestehen Sicherheitsrisiken. Für eine digitale Sicherheitsprüfung ist deshalb ein uneingeschränkter Zugriff auf produktsicherheitsrelevante Steuerungstechnik und deren Software durch die unabhängigen Prüforganisationen notwendig. Sie benötigen hierfür eine klare rechtliche Grundlage in den europäischen Produktrichtlinien.



Mobilität

Sicheres vernetztes und automatisiertes Fahren - europäische Standards im Umgang mit Fahrzeugdaten setzen!

EU-Kommissar/in für Mobilität benennen

Technische Überwachung im Zeitalter der digitalen vernetzten Mobilität heißt konkret: Daten von Einzelnen und Unternehmen zu schützen, das Recht auf Übertragbarkeit von Daten technisch zu realisieren, Schaden von Personen, Unternehmen und Infrastrukturen abzuwenden und ein zuverlässiges Fundament durch unabhängige Prüfungen und Zertifizierungen zu schaffen. Nur so kann Vertrauen in eine vernetzte digitale Welt entstehen und fairer Wettbewerb zwischen neuen und alten Marktteilnehmern ermöglicht werden. Hier bietet sich für den Mobilitätsstandort Europa eine große Chance, international zum Vorreiter zu werden. Die Kommission sollte ein übergreifendes Forum zur Zukunft der Mobilität schaffen und einen eigenständigen EU-Kommissar für Mobilität benennen, der Kompetenzen in den Bereichen Verkehrssicherheit, digitaler Binnenmarkt und Umwelt bündelt und das Thema in der EU vorantreibt.

Zugang und Bereitstellung von Mobilitätsdaten in der Typgenehmigung bestimmen

Funktionalitäten und Eigenschaften von modernen Fahrzeugen werden zunehmend durch Software-Updates während ihres Betriebs angepasst. Bereits heute ist es beispielsweise möglich, über Softwareupdates das Abgasverhalten oder die Funktionen digitaler Assistenzsysteme zu verändern. Um die Verkehrssicherheit und Umweltverträglichkeit digitaler Fahrzeuge barriere- und diskriminierungsfrei überprüfen zu können, müssen bereits in der Fahrzeugtypgenehmigung die Prüfvorschriften für die spätere Hauptuntersuchung entsprechend verankert werden.

Mobilitätsdaten über TrustCenter verwalten

Der Zugang zu Fahrzeugdaten sowie deren Speicherung und Verwaltung sollte über herstellerunabhängige, cloudbasierte neutrale Datentreuhänder erfolgen. Diese hochgradig geschützten sogenannten TrustCenter ermöglichen den Prüforganisationen einen direkten Zugang zu den sicherheits- und umweltrelevanten Daten und Diagnosefunktionen in den Fahrzeugen. Die Fahrzeugnutzer behalten dabei die volle Hoheit über die Übermittlung, Verarbeitung und Verwendung ihrer Daten. Mit einem solchen TrustCenter-Ansatz könnte Europa international zum Treiber einer sicheren und nachhaltigen vernetzten Mobilität werden.

Künstliche Intelligenz

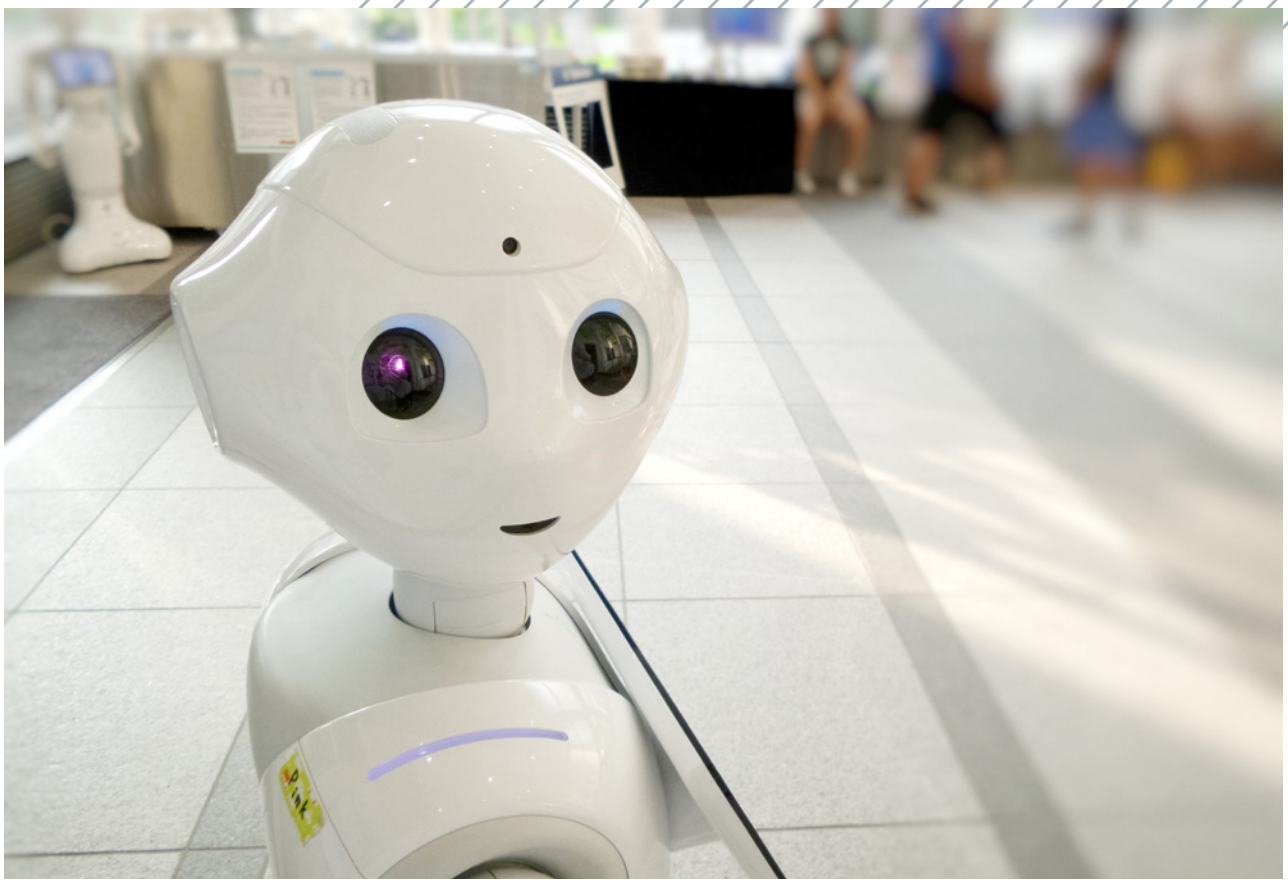
Vertrauen in KI-basierte Systeme und Produkte schaffen!

Sicherheits- und Datenschutzanforderungen für Künstliche Intelligenz festlegen

Sicherheit und Datenschutz müssen auch bei KI-Systemen eine sehr hohe Priorität haben. Die Funktionslogik, auf deren Basis Künstliche Intelligenz Entscheidungen fällt, ist oftmals intransparent und nicht nachvollziehbar. Um die Sicherheit von und das Vertrauen in KI-basierte Anwendungen zu stärken, müssen hierfür klare Sicherheits- und Datenschutzanforderungen angewandt und ggf. bestehende Regelungen angepasst werden. Dazu sollte das kohärente und international wettbewerbsfähige Regelwerk des New Legislative Framework (NLF) herangezogen werden. Wesentliche NLF-Elemente sind die Definition grundlegender Produktanforderungen, die Konkretisierung durch Normen und, in Abhängigkeit vom Gefährdungspotential, die Überprüfung der Konformität durch unabhängige Stellen.

Risikobasierte Sicherheitsbewertung für den gesamten KI-Produktlebenszyklus bestimmen

Weiterhin sollten KI-Systeme einer gesonderten Risikoanalyse unterzogen werden. Für Hochrisiko-Produkte sollten systematische Selbstdiagnosemechanismen und ausfallsichere Komponenten zum Standard gehören. Für ein fortwährend hohes Sicherheitsniveau können unabhängige Prüforganisationen eingebunden werden. Die EU-Mitgliedstaaten müssen hierfür ihre nationalen Regelungen anpassen.



Cybersicherheit

Eine europäische digitale Sicherheitsarchitektur entwickeln!

Digitale Innovationen und Sicherheit miteinander verbinden

Die digitalen Hotspots im Silicon Valley und in China haben Sicherheits- und Datenschutzansätze in ihrem Sinne definiert. In Europa wurden mit der Datenschutz-Grundverordnung eine internationale Benchmark gesetzt und bei der IT-Sicherheit mit dem Cybersecurity Act erste Schritte in die richtige Richtung gemacht. Jetzt kommt es darauf an, diesen Rechtsrahmen in seiner Umsetzung so auszugestalten, dass er den Herausforderungen der Digitalisierung umfassend Rechnung trägt, indem er Innovationen zulässt und gleichzeitig Sicherheit gewährleistet. Die EU muss zum Leuchtturm für digitale Sicherheit werden.

Digitale Sicherheitsarchitektur aufbauen

Wir brauchen klare Marktzugangsvoraussetzungen für digitale Produkte und Anlagen, eindeutige institutionelle Verantwortlichkeiten für IT-Sicherheit, dies in enger Abstimmung mit den Mitgliedstaaten, und eine stärkere Bündelung von Kompetenzen und Ressourcen, zum Beispiel durch das Pooling bei einer einzelnen Generaldirektion der Europäischen Kommission. Schließlich sind Erweiterungen der Prüfverfahren selbst nötig. Je nach Risikopotenzial ist eine regelmäßige oder dynamische und anlassbezogene Überwachung festzulegen, damit IT-basierte Produkte bei der Cybersecurity dem Stand der Technik entsprechen.

Cybersecurity Act schnell umsetzen – unabhängige Prüforganisationen bei der Ausgestaltung eng einbeziehen

Der Cybersecurity Act ist ein wichtiger Schritt hin zu mehr digitaler Sicherheit in Europa. Mit den Risikoklassen „high“, „substantial“ und „basic“ ist eine Einordnung von digitalen Gefahren möglich. Bei der Zuordnung der Risikoklassen für bestimmte Produkte und der konkretisierenden Ausgestaltung von Prüfanforderungen und -methoden sollten die Erfahrungen von unabhängigen Prüforganisationen angemessen berücksichtigt werden. Wichtig ist, dass bei anstehenden Produktregulierungen konsequent auf den Cybersecurity Act verwiesen wird, um die Wirksamkeit dieses neuen Regulierungsinstruments zügig zu verbreitern und die notwendige Rechtssicherheit für Verbraucher, Hersteller und Prüforganisationen beim Umgang mit vernetzten Produkten zu schaffen.

Über uns

Der Verband der TÜV e.V. (VdTÜV) ist der Zusammenschluss der TÜV-Unternehmen in Deutschland. Mit seinen Mitgliedern verfolgt der VdTÜV das Ziel, das hohe Niveau der technischen Sicherheit in unserer Gesellschaft zu wahren und sichere Rahmenbedingungen für den digitalen Wandel zu entwickeln.

Verband der TÜV e.V. | Friedrichstr. 136, 10117 Berlin | T +49 30 760095-400 | berlin@vdtuev.de | www.vdtuev.de
Büro Brüssel | Rue Jacques de Lalaing, 4 | B-1040 Brussels | Johannes Kröhnert | T +32 2 534 8277 | johannes.kroehnert@vdtuev.de