Verband der TÜV e.V.

TÜV®

Dezember 2017

VdTÜV-Position zum Verordnungsentwurf eines europäischen „Cybersecurity Acts“ vom 13. September 2017

Zehn Kernforderungen des VdTÜV

1. VdTÜV begrüßt, dass die Anforderungen an die Konformitätsbewertungsstellen dem „New Legislative Framework“ entsprechen. Zur Gewährleistung der Qualität der Prüfung und Zertifizierung dürfen ausschließlich akkreditierte Drittstellen zuständig sein. Dieses Zusammenspiel aus unabhängiger Konformitätsbewertung, Akkreditierung, Notifizierung und staatlicher Marktüberwachung dient einem effektiven und nachhaltigen Verbraucherschutz.
2. Die Vertrauenswürdigkeit eines Zertifikats ist an die Bewertung durch eine unabhängige Drittstelle gebunden. Produkte, Dienste, Prozesse und Systeme, die ein hohes Risiko aufweisen, müssen einer verpflichtenden Überprüfung durch unabhängige Dritte unterliegen.
3. Die Zertifikatsaussage muss stets höchstes Vertrauen verdienen. Sie sollte eindeutig, belastbar und transparent sein. Der Zertifizierung ist stets eine dem Risiko entsprechende Prüftiefe zugrunde zu legen. Je höher das Risiko, desto umfassender muss die Prüfung ausfallen.
4. Da wichtige Funktionen nicht mehr Bestandteil des IoT-Produktes sind („Back-End“-Systeme), müssen die Prüfungen über eine reine Produktbetrachtung hinausgehen.
5. Es bedarf einer Konkretisierung der Rollenverteilung. Wer prüft und zertifiziert, wer notifiziert und wer akkreditiert muss eindeutig festgelegt werden. Zur Vermeidung von Interessenkonflikten dürfen grundsätzlich die verschiedenen Akteure jeweils nur eine Rolle wahrnehmen. Ausnahmen müssen eindeutig definiert und eingegrenzt werden.
6. Ein Siegel muss konkret und einheitlich beschrieben werden und ein risikoadäquates Sicherheitsversprechen geben. Zertifizierung und die Siegelvergabe setzt voraus, dass ein akkreditierter Dritter die Bewertung durchgeführt hat. Zur Stärkung des Vertrauens sollte der Name des eingebundenen unabhängigen Dritten im Siegel enthalten sein. Die hinterlegten Prüfkriterien sollten in transparenter Weise öffentlich zugänglich sein.
7. Die zu erfüllenden Standards müssen ein hohes Maß an Vertrauen in die Sicherheit bieten. Die neue Rolle der ENISA darf nicht dazu führen, dass bestehende Standards ausgehöhlt werden. Etablierte hohe Standards (bspw. ISO/IEC 15408) müssen als Benchmark für ein europäisches Sicherheitsniveau gelten.
8. Die Interessengruppen müssen aufgrund ihrer Expertise und ihres Sachverstands intensiv bei der Erarbeitung der Zertifizierungsrahmen eingebunden werden.

9. Unabhängige Konformitätsbewertungsstellen benötigen zu Prüfungszwecken uneingeschränkten Zugriff auf die sicherheitsrelevante Steuerungstechnologie des Produktes oder Dienstes (und ihre Schnittstellen) unter Berücksichtigung hoher Datenschutzstandards.
10. Unabhängig vom Verordnungsentwurf müssen die produkt- und sektorspezifischen Anforderungen in den einzelnen „New Approach“-Regelungen in Bezug auf die Cybersicherheit überprüft und angepasst werden. Dabei bedarf es einer Neubewertung der Risiken. Zudem sollte der Aspekt der Robustheit von Produkten und der Interoperabilität in die Definition des allgemeinen Produktsicherheitsbegriffes integriert werden.

1. Neue Risiken durch die Digitalisierung

Nach der Mechanisierung, Elektrifizierung und Digitalisierung der Industrie leitete der breite Einsatz leistungsfähiger Datennetze in der Wirtschaft die vierte industrielle Revolution ein. Damit dringt das Internet der Dinge („Internet of Things", IoT) in alle Lebens- und Wirtschaftsbereiche vor. Es entstehen neue Märkte und brancheninterne Spielregeln werden radikal umgewälzt. Echtzeitkommunikation und der permanente Austausch großer Datenmengen ermöglichen neue Produktions- und Wertschöpfungsprozesse.

Eine Reihe von permanenten neuen Sicherheitsvorfällen zeigt: Die Sicherheit der internetbasierten Produkte muss über den gesamten Produktlebenszyklus und das gesamte Ökosystem sichergestellt werden. Hochinnovative Produkte wie medizinische Geräte oder vernetzte Fahrzeuge, aber auch einfache Produkte wie ein Wasserkocher verfügen zunehmend über integrierte Software und eigene IP-Adressen. Aufgrund von Updates und erweiterten Funktionalitäten, die nicht mehr ausschließlich im Produkt, sondern im „Back-End" bzw. im Produktverbund liegen, verändert sich die Definition des Produktes und des Produktsicherheitsbegriffs.[1] Die Informationssicherheit bedingt somit auch zunehmend die funktionale Sicherheit eines Produktes.

Für den Anwender steigt das Risiko, Opfer von Cyberangriffen zu werden. Sensible – häufig personenbezogene – Daten können manipuliert, ausgespäht oder zerstört werden. Dies trifft insbesondere auf kritische Infrastrukturen zu, also neuralgische Systeme wie die Strom- und Wasserversorgung. Integrität, Vertraulichkeit und Verfügbarkeit sowie das Zusammenspiel von „Safety", „Security" und „Privacy" digitaler Systeme sind wesentliche Voraussetzungen für die Akzeptanz digitaler Gesellschaftstrends, somit auch das Rückgrat von Innovation und wirtschaftlichem Wachstum. Denn erst durch Sicherheit wird aus Innovationen Fortschritt.

Im Rahmen der neuen Cybersicherheitsstrategie 2017 hat die Europäische Kommission (EU-KOM) im September 2017 den Entwurf einer Verordnung zur "EU Cybersecurity Agency" und zum „Cybersecurity Act" veröffentlicht. Der Verband der TÜV e.V. (VdTÜV) begrüßt das mit der Gesetzesinitiative verfolgte Ziel der EU-KOM, durch einen einheitlichen Rahmen für die Zertifizierung von IoT-Produkten das Vertrauen in die Sicherheit von Produkten zu stärken und ein erhöhtes Cybersicherheitsniveau zu erzielen. Ein beständiger Zertifizierungsrahmen kann wesentlich dazu beitragen, dass Produkte und Dienste bereits vor Markteintritt sicher sind und während des gesamten Produktlebenszyklus resilient bleiben. Dennoch trägt der vorliegende Verordnungsentwurf der nachhaltigen Bedeutung sicherer internetfähiger Geräte mit Blick auf die zukünftigen Gesellschaftsentwicklungen nur unzureichend Rechnung und bedarf daher wesentlicher Nachjustierungen.

[1] Vgl.: VdTÜV-Position: Regulativer Nachbesserungsbedarf für sichere IoT-Produkte in Europa, Berlin 2017 (https://www.vdtuev.de/dok_view?oid=679604).

2. Grundsätze der Produktregulierung nach dem „New Legislative Framework“

Eine Vielzahl von Produktsektoren regelt der europäische Gesetzgeber auf Basis des „New Legislative Framework“ (NLF oder früher „New Approach“). Dieses Regulierungsmodell ist eine tragende Säule des europäischen Binnenmarktes. Der „New Approach“ wurde zur europäischen Harmonisierung der Produktanforderungen entwickelt, um technische Handelshemmnisse in Europa und international abzubauen.

Der NLF begrenzt die Gesetzgebung im Produktbereich auf die Festlegung der wesentlichen Anforderungen. Diese werden in Richtlinien bzw. Verordnungen für bspw. Aufzüge, Druckgeräte, Medizinprodukte oder Spielzeuge näher beschrieben. Technische Einzelheiten werden durch die EU-KOM mandatiert und von den europäischen Normungsorganisationen (CEN, CENELEC oder ETSI) eigenständig erarbeitet.

Um Produkte auf dem europäischen Binnenmarkt in Verkehr zu bringen, müssen diese auf ihre Konformität mit den geltenden einschlägigen Anforderungen überprüft werden. Dabei hängt die Ausgestaltung der anzuwendenden Konformitätsbewertungsverfahren vom Risiko des Produktes ab. Bei Produkten mit hohem Risiko, wie Herzschrittmachern oder Druckgeräten, hat der Hersteller eine unabhängige Drittstelle (Benannte Stelle) einzubeziehen. Die Unabhängigkeit der Stelle vermeidet dabei Interessenkonflikte und bewirkt eine hohe Belastbarkeit des Prüfergebnisses. Die Kompetenz und Unabhängigkeit der Konformitätsbewertungsstelle muss bei der nationalen Akkreditierungsstelle kontinuierlich nachgewiesen werden. Dies sichert das notwendige Vertrauen für die Erfüllung der Konformitätsbewertung durch private Stellen.

Bei den meisten Produkten kann die Konformitätsbewertung durch den Hersteller ohne Einbindung einer Drittstelle erfolgen. Die Identifizierung nicht-konformer Produkte im Markt obliegt den staatlichen Marktüberwachungsbehörden der EU-Mitgliedstaaten.

- VdTÜV begrüßt, dass die in dem Entwurf der Verordnung zum „Cybersecurity Act“ beschriebenen Anforderungen an die Konformitätsbewertungsstellen den üblichen Festlegungen des NLF (Verordnung 765/2008/EG) entsprechen. Im Annex I werden klare und strenge Anforderungen an die Unabhängigkeit der Konformitätsbewertungsstellen festgelegt und die freie Wahl der Stellen durch den Hersteller vorgesehen. Gleiches gilt für die verwendeten Definitionen, die mit den geltenden Rechtsvorschriften der EU und international anerkannten Normen im Einklang stehen. Dies gewährleistet einen klaren und kohärenten Rechtsrahmen zum Nutzen aller beteiligten Akteure.
- Zur Herstellung der notwendigen Konvergenz und Vergleichbarkeit dürfen für die Konformitätsbewertung von IoT-Produkten ausschließlich akkreditierte Prüf- und Zertifizierungsstellen zuständig sein. Dabei gilt es zu beachten, dass diese Stellen ein europaweit einheitliches Qualitätsniveau bei der Wahrnehmung ihrer Aufgaben erfüllen. Die Anforderungen bzw. das Qualitätsniveau müssen durch Überwachungsmaßnahmen regelmäßig überprüft werden. Dieses staatsentlastende Zusammenspiel aus unabhängiger Konformitätsbewertung, Akkreditierung und staatlicher Marktüberwachung dient einem effektiven und

nachhaltigen Verbraucherschutz. Dieser präventive Ansatz wird dabei durch die Hersteller, Importeure oder den Handel finanziert.

- Zusätzlich ist sicherzustellen, dass die Bewertungs- und Prüfverfahren den Anforderungen der dynamischen und komplexen Cybersicherheitsumgebung Rechnung tragen (siehe bspw. ISO/IEC 15408). Das heißt, sie müssen ausreichend flexibel und schnell genug angepasst werden können, um auf neue bzw. individuelle Angriffsvektoren effizient reagieren zu können. Diese Verfahren müssen auch die notwendige Herstellerverantwortung bei Updates berücksichtigen.
- Unabhängig vom Verordnungsentwurf müssen mittelfristig die produktspezifischen Sicherheits- und Gesundheitsanforderungen in den einzelnen „New Approach"-Richtlinien / Verordnungen in Bezug auf die Cybersicherheit überprüft und angepasst werden. Die momentan bestehenden Regulierungslücken bei IoT-Produkten führen dazu, dass Cybersicherheits-Aspekte nicht oder nicht in angemessenem Maße Teil der obligatorischen Konformitätsbewertung sind.[2] Der Aspekt der Robustheit (Informationssicherheit, Datenschutz und funktionale Sicherheit) und der Interoperabilität muss aufgrund der erweiterten, dynamischen Funktionalität von IoT-Produkten in die Definition des allgemeinen Produktsicherheitsbegriffes (Richtlinie 2001/95/EG) integriert werden.[3]

3. „Cybersecurity Act": Konkretisierungen und Änderungen am Verordnungsentwurf

VdTÜV begrüßt das Ziel, durch einen übergeordneten Zertifizierungsrahmen für IoT-Produkte das notwendige Vertrauen in die Sicherheit von Produkten zu stärken. Solange keine umfassende Ergänzung aller sektor- und produktspezifischen Richtlinien und Verordnungen unter dem NLF um den Aspekt der Informationssicherheit erfolgt, kann eine übergeordnete Verordnung zu der durchgängigen Implementierung spezifischer Sicherheitsanforderungen hinleiten. VdTÜV empfiehlt folgende Konkretisierungen und Änderungen:

a. Zertifikate nur aufgrund unabhängiger Drittprüfung

Die Sicherheit eines IoT-Produktes ist zunehmend durch die Vernetzung und den Datenaustausch innerhalb eines digitalen Ökosystems definiert. Dies stellt ein Risiko für die Funktionen, aber auch für fremde Infrastrukturen, vernetzte Produkte und Dienste dar. In der Folge verschieben sich Risiken und Kritikalitätslevel. Eine klare Unterscheidung der Risikoklassen und eine entsprechende Zuordnung von IoT-Produkten muss die Grundlage für die verschiedenen freiwilligen und verpflichtenden Prüfverfahren und die Festlegung der notwendigen Einbindung unabhängi-

[2] Vgl.: VdTÜV-Position: Informationssicherheit von „smart products" in Europa, Berlin 2017 (https://www.vdtuev.de/dok_view?oid=679603)
[3] Vgl.: VdTÜV-Position: Regulativer Nachbesserungsbedarf für sichere IoT-Produkte in Europa, Berlin 2017 (https://www.vdtuev.de/dok_view?oid=679604).

ger Dritter sein. Dabei hat eine Vielzahl von Sicherheitsvorfällen in den vergangenen Jahren gezeigt, dass das „Duty-of-Care"-Prinzip bzw. das alleinige Vertrauen auf die Herstellerverantwortung flächendeckend kein ausreichendes Sicherheitsniveau garantieren kann.

- VdTÜV empfiehlt, dass Produkte, Dienste, Prozesse und Systeme, die ein hohes Risiko aufweisen, einer verpflichtenden Überprüfung durch unabhängige Dritte unterliegen sollten. Ein hohes Risiko besteht dann, wenn durch einen Angriff auf die Integrität, Vertraulichkeit oder Verfügbarkeit des Produktes oder Systems eine Gefahr für die Gesundheit der Anwender oder Dritter, die Umwelt oder für andere wesentliche Rechtsgüter (z.B. unerlaubter Eingriff in die Intimsphäre oder das Eigentum) entstehen kann. Die im Verordnungsentwurf beispielhaft aufgelisteten Produkte und Dienste (darunter „Connected Cars", Industriesteuerungsanlagen [ICS], Bezahlsysteme oder „Smart Grids") müssen daher zwingend einer Prüfung und Zertifizierung durch unabhängige Dritte unterliegen. Die Freiwilligkeit der Zertifizierung gilt es in diesen Produktbereichen durch eine verpflichtende unabhängige Drittprüfung zu ersetzen.
- Die notwendige Vertrauenswürdigkeit und Belastbarkeit eines Zertifikats ist zwingend an die Konformitätsbewertung durch eine unabhängige Drittstelle gebunden. Das heißt, wenn ein Hersteller eine freiwillige Produkt-, System- oder Dienstzertifizierung anstrebt, muss diese unabhängig vom Grad des Risikos durch einen unabhängigen Dritten erfolgen.
- Die Aussage eines Zertifikats über konkret definierte Cybersicherheits-Eigenschaften eines IoT-Produktes muss eindeutig, belastbar und transparent sein. Der Zertifizierung muss stets eine dem Risiko entsprechende Prüftiefe zugrunde liegen. Das heißt, je höher das Risiko des IoT-Produktes, desto tiefer bzw. umfassender muss die Prüfung des Produktes ausfallen. Im Verordnungsentwurf (Art. 46) beziehen sich die „Vertrauenswürdigkeitsstufen" (niedrig, mittel, hoch) jedoch auf das „durch das Zertifikat vermittelte Vertrauen". Sie sind somit ohne Bezugnahme auf das produktspezifische Risiko irreführend. Es wird außer Acht gelassen, dass die Zertifikatsaussage stets höchstes Vertrauen verdient und an das produktspezifische Risiko gekoppelt sein muss. Differenzierungen hinsichtlich des Aussagegehalts eines Zertifikats müssen sich aus den hinterlegten Prüfkriterien und -verfahren ableiten.

b. Klare Rollen- und Aufgabenverteilung

Das „Framework" muss einen freien Wettbewerb der unabhängigen Konformitätsbewertungsstellen gewährleisten. Hersteller müssen selbstständig am Markt eine akkreditierte Stelle zur Prüfung und Zertifizierung ihrer Produkte oder Dienste auswählen dürfen. Eine klare Aufgabenabgrenzung stärkt das notwendige Vertrauen in das Gesamtsystem und sorgt für faire, klare und transparente Wettbewerbsbedingungen sowie ein „Level Playing Field" in Europa.

- In dem vorliegenden Verordnungsentwurf bedarf es einer Konkretisierung der Rollenverteilung zwischen den nationalen Behörden und den Konformitätsbewertungsstellen. Es muss eindeutig definiert werden, wer prüft und zertifiziert, wer notifiziert und wer akkreditiert. Zum Schutz der Unabhängigkeit und zur Vermeidung von Interessenkonflikten, sowie damit verbundener Beeinträchtigungen des Qualitäts- und Sicherheitsniveaus, sollten Prüforganisationen sowie Genehmigungs- und Aufsichtsbehörden jeweils nur eine Rolle wahrnehmen. Das heißt, dass Genehmigungs- und Aufsichtsbehörden sowie akkreditierende und notifizierende Stellen nicht als Zertifizierungsstellen fungieren sollten.
- Dem Vier-Augenprinzip und der Trennung der Verantwortlichkeiten muss bei der Prüfung und Zertifizierung Rechnung getragen werden. Hier sind entsprechende Klarstellungen im Verordnungsvorschlag vorzunehmen.
- Die Rolle der „nationalen Aufsichtsbehörde für die Zertifizierung“ (Art. 50) bedarf der Konkretisierung. Eine strikte Rollentrennung hinsichtlich der Notifizierung, Akkreditierung und Zertifizierung sollte dabei sichergestellt werden. Der nationalen Aufsichtsbehörde sollte die Aufgabe übertragen werden, die akkreditierten Konformitätsbewertungsstellen bei der EU-KOM zu notifizieren (Art. 52, Abs. 1). Aufgrund ihrer Funktion als notifizierende Behörde sollte sie somit weder Konformitätsbewertungen noch Beratungsleistungen auf wettbewerblicher Basis anbieten. Dies dient dem konsequenten Ausschluss von Interessenskonflikten.

c. Ausnahmen klar definieren

Der Verordnungsentwurf sieht vor, dass in „hinreichend begründeten Fällen“ (vergleiche Art. 48, Abs. 4) ein Zertifikat nur von einer öffentlichen Stelle (Behörde) ausgestellt werden kann.

- Unter sachgerechter Betrachtung können „hinreichend begründete Fälle“ ausschließlich dort bestehen, wo die nationalen Sicherheitsinteressen direkt betroffen sind. Darunter sind insbesondere Sicherheitsinteressen zu verstehen, die den Kern des staatlichen Gemeinwesens betreffen oder der Gefahrenabwehr für die öffentliche Sicherheit – somit den Staatsinteressen im engeren Sinne – maßgeblich dienen. Daher bedarf es einer deutlich präzisierten Festlegung des Anwendungsbereiches für eine behördliche Zertifizierung. Aus ordnungspolitischer Sicht handelt es sich bei einer umfassenden behördlichen Zertifizierung, die über den Kernbereich der öffentlichen Sicherheit hinausgeht, um eine unsachgemäße Abkehr von den Grundsätzen der europäischen Produktregulierung auf Basis des NLF (Verordnung 765/2008/EG).
- Des Weiteren steht die im Art. 48, Abs. 4 genannte Definition der „öffentlichen Stelle" im Widerspruch zu Art. 48, Abs. 3. Hier wird der Begriff der „öffentlichen Stelle“, die auf eine Behörde hindeutet, auch auf die privat organisierten und akkreditierten Konformitätsbewertungsstellen ausgedehnt.

d. Einheitliches und transparentes Siegel

Im Verordnungsentwurf (Art. 47) ist vorgesehen, dass die Bedingungen für die Verwendung von Siegeln oder Kennzeichen individuell (je Zertifizierungssystem für eine Produktgruppe) festgelegt werden können. Dies hätte zur Folge, dass aufgrund unterschiedlicher Zertifizierungssysteme (bzw. Produkte) unterschiedliche Bedingungen für die Verwendung von Siegeln zum Einsatz kommen würden. Zudem würden unterschiedliche Anforderungen für die optische Gestaltung eines Siegels entstehen. Ein solches fragmentierte System würde der Intention, mit der Cybersicherheitszertifizierung Transparenz und Orientierung für den Verbraucher zu schaffen, zuwiderlaufen.

- Ein einheitliches Cybersicherheits-Siegel sollte in der Verordnung konkret beschrieben werden. Hierbei können die in der Verordnung 765/2008/EG für die CE-Kennzeichnung getroffenen Regelungen hinsichtlich ihres Detaillierungsgrads als Referenzpunkt herangezogen werden. Das Siegel muss in Abhängigkeit des jeweiligen Produktrisikos stets ein adäquates Sicherheitsversprechen geben und somit eine einheitliche Aussagekraft haben. Die konkreten Verfahren und Bedingungen (Prüfkriterien) für die Vergabe von Siegeln können individuell in den jeweiligen Systemen in Abhängigkeit vom Risiko und der Verwendung geregelt werden.
- Zur Stärkung des Vertrauens, zur Rückverfolgbarkeit sowie zum erleichterten Vorgehen bei Missbrauch (Markenrecht) sollte der Name des eingebundenen unabhängigen Dritten im Siegel enthalten sein. Darüber hinaus muss der Anwender auf dem Siegel einen klaren Verweis auf die Anforderungen und Prüfkriterien (Zertifizierungssystem) finden. Die hinterlegten Prüfkriterien und -verfahren sollten in zusammengefasster und allgemeinverständlicher Form öffentlich zugänglich sein.

e. Siegelvergabe nur nach unabhängiger Drittprüfung

Der Verordnungsentwurf sieht die Freiwilligkeit des Siegels oder Zertifikats vor. Zugleich wird bereits in den Erwägungsgründen (Ziffer 47) dargestellt, dass die Vergabe eines Siegels durch eine unabhängige Drittprüfung erfolgt. Wenn sich also ein Hersteller oder Dienstanbieter für eine Zertifizierung entscheidet, so ist damit die Einbindung eines akkreditierten unabhängigen Dritten in die Konformitätsbewertung verbunden.

Die Zertifizierung eines IoT-Produktes oder Dienstes setzt voraus, dass ein akkreditierter unabhängiger Dritter, bei dem es sich nicht um den Hersteller des Produktes oder Dienstes handelt, in die Konformitätsbewertung eingebunden wird. Die Vergabe (nicht das Aufbringen) eines Siegels durch den Hersteller ist damit ausgeschlossen. Ansonsten würde dies die Vertrauenswürdigkeit des gesamten Zertifizierungsrahmens unterminieren.

f. Anforderungen in sektorspezifische Regelungen überführen

Die Anforderungen eines Zertifizierungssystems für spezifischen Produkte und Systeme müssen zumindest mittelfristig in die produkt- und sektorspezifischen Sicherheitsanforderungen der jeweiligen Verordnungen und Richtlinien des NLF überführt werden – sofern dies technisch möglich ist.

- Im Zuge der Überführung der spezifischen Cybersicherheitsanforderungen in die produkt- und sektorspezifischen Verordnungen und Richtlinien (nach NLF) muss eine Neubewertung der vom Produkt ausgehenden Risiken erfolgen. Dementsprechend gilt es sorgfältig zu überprüfen, ob eine erstmalige oder umfangreichere obligatorische Einbindung einer unabhängigen Drittstelle erfolgen muss. Im Falle einer vollständigen Überführung der Anforderungen würde ein Siegel keine zusätzliche Aussage mehr über die Vertrauenswürdigkeit des Produktes treffen – und wäre somit obsolet.
- Sollten wichtige Funktionalitäten nicht mehr Bestandteil des IoT-Produktes sein, sondern im „Back-End-System“ liegen, sind Prüfungen notwendig, die über eine reine Produktprüfung hinausgehen. Auch gilt es hier die Möglichkeiten moderner Sicherheitsarchitekturen (mit bspw. sicherer Schlüsselablage und -verteilung) hinlänglich zu berücksichtigen. Insoweit muss eine sachgerechte Weiterentwicklung der bestehenden Verfahren der Konformitätsbewertung erfolgen.

g. Vertrauen durch hohe Sicherheitsniveaus

Die neue Rolle der ENISA darf nicht dazu führen, dass bestehende Standards und Zertifizierungsprozesse ausgehöhlt werden („Race to the Bottom“) und das niedrigste Sicherheitslevel zum europäischen Standard wird. Der Erfolg von Industrie 4.0 bzw. der Digitalisierung insgesamt ist davon abhängig, dass die zu erfüllenden Standards ein hohes Maß an Vertrauen in die Sicherheit bieten. Bereits etablierte und anerkannte hohe nationale Standards (wie bspw. ISO 15408) müssen dabei als Benchmark für ein europäisches Sicherheitsniveau gelten.

Die Prüfung der Informationssicherheit eines Produktes oder Systems lässt sich nicht allein über das reine Abprüfen nach einer eher statischen Norm herstellen. Eine aussagekräftige Prüfung muss daher dynamische Angriffsvektoren, die sich stets verändern und erweitern, in der Konformitätsbewertung berücksichtigen.

h. Einbindung aller relevanten Interessengruppen

Dem Verordnungsentwurf zufolge wird die ENISA bei einem zukünftigen Zertifizierungsrahmen eine strategische Rolle einnehmen.

VdTÜV begrüßt die Möglichkeit, dass nach Art. 44, Abs. 2 grundsätzlich alle Stakeholder bei der Erarbeitung der Zertifizierungssysteme „konsultiert“ werden sollen. Jedoch ist es erforderlich,

dass die Interessengruppen über eine reine Konsultation hinaus intensiv bei der Erarbeitung der Zertifizierungsrahmen eingebunden werden. Dabei muss die Expertise und der Sachverstand aller Stakeholder (Wirtschaft, unabhängige Dritte sowie staatliche Behörden) gleichermaßen in diesem Prozess Berücksichtigung finden.

i. Datenzugang zu Prüfzwecken

Unter Berücksichtigung der Cybersicherheit und der Datensouveränität des Verbrauchers („Privacy by Design“ und „Privacy by Default“), können datengetriebene Geschäftsmodelle zu einem enormen wirtschaftlichen Wachstum beitragen. Die Datenschutz-Grundverordnung (DSGVO) bereitet dafür bereits den notwendigen europäischen Rahmen. Aufgrund zahlreicher weiterer Hemmnisse mangelt es momentan jedoch an einem einheitlichen europäischen Markt für Daten. Dies führt dazu, dass wirtschaftliche, soziale und gesellschaftliche Chancen nicht realisiert werden. Aufgabe der Politik ist es, einen rechtlichen Rahmen zu schaffen, in dem sich Datenströme über Grenzen und Sektoren hinwegbewegen und zugleich bestmöglich und sicher verfügbar gemacht und bzw. weiterverwendet werden können.

Unabhängige Konformitätsbewertungsstellen benötigen zu Prüfungszwecken uneingeschränkten Zugriff auf die sicherheitsrelevante Steuerungstechnologie des Produktes oder des Dienstes (und ihrer Schnittstellen). Zudem müssen Hersteller und Dienstleister die unabhängige Konformitätsbewertungsstelle über Änderungen von IT-Komponenten informieren (z.B. Software-Updates), damit die Einhaltung der Systemanforderungen weiterhin überprüft und sichergestellt werden kann. Dieses Ziel kann mit einem geringen technischen und ökonomischen Aufwand erreicht werden.