Mona Mirtsch

9 Konformitätsbewertung im Bereich Cybersicherheit

9.1 Einleitung

Die digitale Transformation und insbesondere das Internet der Dinge (*Internet of Things* IoT) ermöglichen eine wachsende Zahl von neuen Dienstleistungen, sogenannten Smart Services, sowohl im industriellen- und auch im Verbraucherbereich. Einhergehend mit den Chancen treten jedoch auch Risiken insbesondere im Zusammenhang mit der IT- und Cybersicherheit in den Vordergrund, die nicht nur Organisationen, sondern auch Einzelpersonen und die breite Öffentlichkeit betreffen. Ein bekanntes Beispiel für aktuelle Bedrohungen im Bereich der Cybersicherheit stellt hierbei der sogenannte WannaCry-Ransomware-Vorfall[1] dar, der im Jahr 2017 unter anderem auf große Unternehmen wie die Deutsche Bahn AG abzielte und dort Anzeigetafeln in Bahnhöfen lahmlegte (BSI 2017).

Cybersicherheit ist ein komplexes Konstrukt, da es nicht nur die Produkte (einschließlich Hard- und Software) und Systeme, sondern auch die gesamte Infrastruktur (wie cloudbasierte Dienste) und verknüpfte Organisationen betrifft. Als Voraussetzungen für sichere Produkte, Dienstleistungen und Prozesse wird die Cybersicherheit nach Auffassung einiger Interessengruppen aus regulativer Sicht bisher jedoch unzureichend berücksichtigt (ANEC und BEUC 2018; IFIA/CEOC 2017; VdTÜV 2017).

Die Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netzwerk- und Informationssytemen in der EU (NIS-Richtlinie) stellt einen ersten Schritt dar, insbesondere im Bereich der kritischen Infrastrukturen (European Commission 2016). Der aktuelle europäische Vorschlag eines Rechtsaktes zur Cybersicherheit (Bundesrat 2017) – im Folgenden Cybersecurity Act – zielt darauf ab, mit Hilfe eines europäischen Zertifizierungsrahmens die Sicherheit und das Vertrauen in Produkte und Dienste der Informations- und Kommunikationstechnologie (IKT) zu erhöhen und die derzeitige europäische Fragmentierung in Bezug auf bestehende, meist nationale, Zertifizierungssysteme zu verringern.

Das Ziel dieses Kapitels besteht darin, die Rolle von Konformitätsbewertung für die Erhöhung der Cybersicherheit von Produkten, Dienstleistungen und Prozessen zu betrachten. Dazu wird der Begriff Cybersicherheit beleuchtet sowie ausgewählte Cy-

1 Hierbei handelte es sich um eine sogenannte Schadsoftware (*malware*), die den Zugriff auf Anwendungen oder Daten verschafft und mit einer Lösegeldforderung zur Freigabe der Daten oder Anwendungen (*ransom* englisch für Lösegeld), meist in Form von Kryptowährungen (wie z. B. bitcoin), verbunden ist.

https://doi.org/10.1515/9783110629057-009

bersicherheitsnormen kurz vorgestellt. Im Folgenden wird der regulative europäische Rahmen für die Konformitätsbewertung aus ordnungspolitischer Sicht sowie der aktuelle Verordnungsentwurf zum Cybersecurity Act (Bundesrat 2017) dargestellt. Im Analyseteil werden Positionen ausgewählter Interessengruppen, die in einem definierten Zeitraum in Bezug auf den Cybersecurity Act systematisch gesammelt wurden, analysiert und daraus Handlungsempfehlungen abgeleitet sowie ein Ausblick auf die Entwicklung der Konformitätsbewertung in der digitalen Transformation gegeben.

9.2 Status quo

Definition von Cybersicherheit

Die Begriffe Informationssicherheit, Informationstechnologie- (IT) Sicherheit und Cybersicherheit werden allzu oft synonym verwendet, wobei der Begriff Cybersicherheit am weitreichendsten ist (Solms und van Niekerk 2013). Allen Begriffen ist gemein, dass sie sich u. a. auf die drei Ziele Vertraulichkeit, Integrität und Verfügbarkeit beziehen. Diese sind nach der ISO/IEC Norm 27000 folgendermaßen definiert:

- Vertraulichkeit (*confidentiality*): Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt wird
- Integrität (*integrity*): Eigenschaft der Richtigkeit und Vollständigkeit
- Verfügbarkeit (*availability*): Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat (DIN 2017)

Informationssicherheit beschreibt die „Aufrechterhaltung der Vertraulichkeit […], Integrität […] und Verfügbarkeit […] von Informationen" (DIN 2017). Darauf aufbauend differenziert von Solms (2013) IT-Sicherheit von Informationssicherheit dahingehend, dass bei der IT-Sicherheit die Informationen mit Hilfe von IT-Technologien gespeichert oder übertragen werden. Laut dem Bundesministerium des Innern (2016) bezieht sich die IT-Sicherheit auf die Informationssicherheit innerhalb eines informationstechnischen Systems, wobei sich dieses auf eine abgeschlossene Einheit bezieht.

Cybersicherheit stellt insofern eine Erweiterung des Begriffes IT-Sicherheit dar, als dass der Cyberraum den virtuellen Raum aller (z. B. über das Internet) verbundenen und anschließbaren IT-Systeme weltweit beschreibt. Daher ist Cybersicherheit, z. B. in der deutschen Cybersicherheitsstrategie, als IT-Sicherheit aller angeschlossenen Informationssysteme definiert (Bundesministerium des Innern 2016).

Gemäß einer Studie der CEN/CENELEC-Fokusgruppe hat Cybersicherheit ferner einen weitaus größeren Anwendungsbereich und beschränkt sich nicht nur auf die Informationssicherheit (Abbildung 9.1).

Die Cybersicherheit gilt demnach auch für den Schutz von Sachwerten wie Produktionslinien, Kraftwerke oder Industrielle Automatisierungs- und Steuerungssysteme. Dabei kann die Bedrohungsquelle entweder krimineller Herkunft sein (z. B. bei

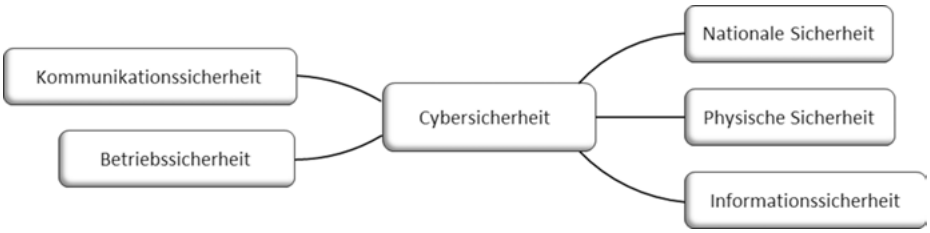

Abb. 9.1: Bestandteile von Cybersicherheit (Quelle: Eigene Darstellung basierend auf CEN/CENELEC (2017)).

Hackerangriffen) oder auch unbeabsichtigter Natur sein (z. B. aufgrund menschlicher Fehler). Zusammenfassend beschreibt die CEN/CENELEC-Fokusgruppe (2017) Cybersicherheit als Sicherheit im Cyberraum. Diese umfasst dabei die Merkmale Vertraulichkeit, Integrität und Verfügbarkeit im Sinne der ISO/IEC-Norm 27000 erweitert um den Schutz der Privatsphäre und die Resilienz vor Cyberangriffen. Die Schutzziele in Bezug auf die Privatsphäre umfassen laut einer Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018) folgende Aspekte:

- Datenminimierung: Begrenzung der notwendigen Datenerfassung auf das notwendige Maß
- Nichtverkettung: keine Zusammenführung von personenbezogenen Daten
- Transparenz: Darlegung der erhobenen Daten und Zweck der Erhebung
- Intervenierbarkeit: Recht auf Auskunft sowie Speicherung und Löschung der Daten bei Wunsch der Personen (DSK 2018)

Unter Resilienz vor Cyberangriffen wird die Widerstandsfähigkeit verstanden, auftretende Cyberangriffe zu bewältigen und u. a. daraus neue Erkenntnisse und Fähigkeiten zur Bewältigung potentieller zukünftiger Cyberangriffe zu gewinnen (CEN/CENELEC 2017).

Der Begriff Cybersicherheit kann jedoch nicht nur einen Zustand, sondern auch Tätigkeiten umfassen. Im Entwurf des Cybersecurity Acts werden als Cybersicherheit „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, deren Nutzer und betroffenen Personen vor Cyberbedrohungen zu schützen“ (Bundesrat 2017) verstanden. Diese Definition wird auch im Rahmen dieses Kapitels zugrunde gelegt.

Cybersicherheitsrelevante Normen und Standards

Eine große Anzahl von Normen und Standards befassen sich mit Cybersicherheit. Die Europäische Cyber-Sicherheitsorganisation (ECSO), die die europäische Cybersicherheits-Industrie als Vereinigung vertritt, hat eine umfangreiche Übersicht über relevante Spezifikationen, Normen und Systeme in Bezug auf Cybersicherheit erstellt, die

regelmäßig überarbeitet wird (European Cyber Security Organisation 2017). Demnach können Cybersicherheitsstandards und -normen unterteilt werden in Kategorien für:

- Produkte bzw. Komponenten
- Systeme
- Organisationen
- IKT-Service-Provider
- Cloud-Service- (d. h. Infrastruktur-) Anbietern
- Personen

Im Folgenden werden drei cybersicherheitsrelevante Normen bzw. Normenfamilien im Bereich Managementsysteme, Systeme/Komponenten sowie Kriterien zur Bewertung vorgestellt, denen im Kontext des Cybersecurity Acts besondere Bedeutung als Grundlage für die Konformitätsbewertung zugesprochen wurden (CEN/CENELEC 2018a). Diese unterscheiden sich neben dem Anwendungsgebiet, im Prüfansatz, in der Marktbedeutung und hinsichtlich der internationalen gegenseitigen Anerkennung.

Die weit verbreite Normenreihe ISO/IEC 27000 beschreibt den Aufbau und die Implementierung eines Informationssicherheitsmanagementsystems (ISMS). Da es sich um allgemeine Anforderungen handelt, ist die Normenreihe sowohl für kleine und mittlere Unternehmen (KMU) als auch für große Unternehmen sowie für weitere Organisationsarten (wie z. B. Behörden und gemeinnützige Gesellschaften) sektorübergreifend anwendbar, wobei insbesondere die Kosten der Implementierung der Norm und die Zertifizierung – gerade für KMU – eine nicht unerhebliche Hürde darstellen können. Das ISMS bezieht sich dabei sowohl auf IT-Systeme, Prozesse sowie Personen (Fuchsberger 2018). Während in der ISO/IEC 27000 relevante Begriffe definiert werden, legt die folgende ISO/IEC 27001 die ISMS-Zertifizierungsanforderungen fest. Branchenspezifische Anwendungen, wie die von Telekommunikationsorganisationen (ISO/IEC 27011), Cloud-Computing-Dienste (ISO/IEC 27017) oder Anforderungen an Energieversorgungsunternehmen (ISO/IEC TR 27019) werden in weiteren Bestandteilen der Normenreihe beschrieben. Eine Zertifizierung ist jedoch, analog zur ISO 9000er Standardfamilie und ISO 9001, nur nach ISO/IEC 27001 möglich (ISO/IEC 2013). Branchenspezifische Normen können als Bestandteil eines Konformitätsbewertungsprogramms mit einbezogen werden, wenn sie nicht im Widerspruch zu den in der ISO/IEC 27001 festgelegten Anforderungen stehen (ISO/IEC 2017). Gemäß der jährlich durchgeführten ISO-Studie wurden in Deutschland im Jahr 2016 insgesamt 1.338 Zertifikate von akkreditierten Konformitätsbewertungsstellen erteilt, wobei dies ein Anstieg um 35 % gegenüber dem Vorjahr darstellt (ISO 2017).

Die Normenreihe IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ wurde für Produkte und Dienstleistungen im Bereich der industriellen Steuerungs- und Automatisierungstechnik entwickelt und stellt nach Auffassung von Konformitätsbewertungsstellen und der Industrie die bedeutendste Grundlagennorm für die Zertifizierung von Produkten, Prozessen und Dienstleistun-

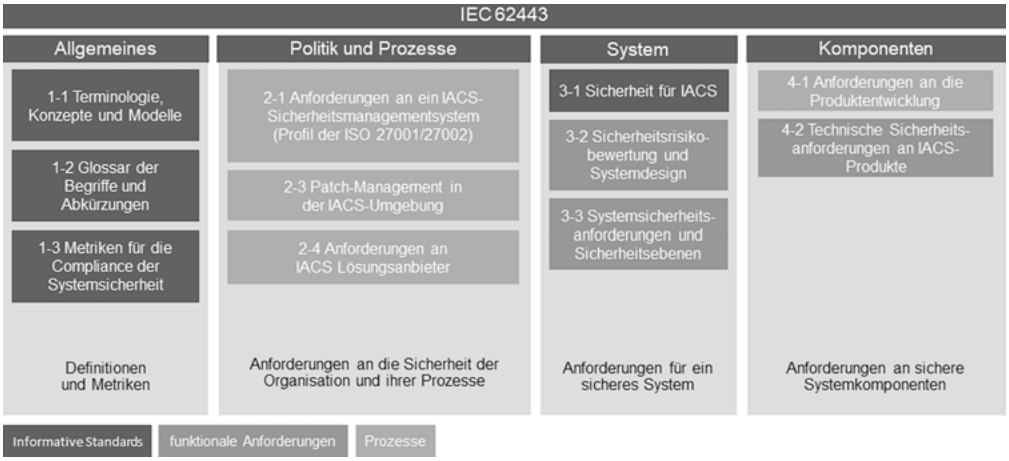

Abb. 9.2: Übersicht zur Normenreihe IEC 62443 (Quelle: Eigene Darstellung basierend auf TÜV Nord (2017b)).

gen im Bereich der vernetzten Systeme dar (TÜV Nord 2017b; ZVEI 2017). Initiiert von der internationalen Gesellschaft für Automatisierung wurde diese Standardreihe von der IEC weiterentwickelt.

Die Normenreihe IEC 62443 befasst sich zentral mit der Cybersicherheit von Industrial Automation Control Systemen (IACS), die als IT-System, bestehend aus mehreren Komponenten wie z. B. Aktoren und Sensoren, der Steuerung von Produktionsstraßen und Prozessstrecken dienen. Des Weiteren bezieht die IEC 62443 auch Anforderungen an die Produktentwicklung sowie Sicherheitsanforderungen an IACS Produkte mit ein. Aufgrund der komplexen Betrachtungsweise und des ganzheitlichen Schutzes wird die IEC 62443 als die führende Normenfamilie im Bereich Industrial Cybersecurity betrachtet und aufgrund fehlender branchenspezifischer Normen auch von weiteren Industriezweigen genutzt (ZVEI, 2017). Die Normenreihe gliedert sich in die Teile Allgemeines, Politik und Prozesse, System sowie Komponenten. Abbildung 9.2 zeigt die insgesamt 11 Teilnormen (TÜV Nord 2017b).

Eine weitere normative Grundlage in diesem Bereich steht seit 1999 mit der ISO/IEC 15408er Normenreihe zur Verfügung. Die darin formulierten Evaluationskriterien für IT-Sicherheit haben ihren Ursprung in einer internationalen, behördlichen Zusammenarbeit, die erstmals 1996 gemeinsame Grundlagen für die Bewertung von Datensicherheit postulierten. Das Ziel dieser Einigung war die bessere Vergleichbarkeit sowohl der Überprüfung von Informationstechnik als auch der Zertifizierung auf Produktebene. Die Bewertung kann sich dabei sowohl auf Produkte als auch einzelne Komponenten und Systeme beziehen. Damit grenzt sich diese Normenreihe auch von der ISO/IEC 27001 ab, die Anforderungen an eine Organisation und deren Managementsystem beschreibt. Die sogenannten Common Criteria (2018) stellen im Gegensatz zu den beiden vorher genannten Normenfamilien ferner keine technische

Anforderungen für die Bewertung von Produkteigenschaften fest, sondern Kriterien auf der Ebene der Prüfverfahren zur Bewertung von Informationstechnik und unterscheiden streng nach Funktionalität und Vertrauenswürdigkeit. Die Normenreihe gliedert sich in drei Teile: Während der erste Teil Begriffe erläutert sowie allgemeine Prinzipien (Introduction and general model), beschreibt der zweite Teil funktionale Sicherheitsanforderungen (Security functional components) und der dritte Teil Anforderungen an die Vertrauenswürdigkeit (Security assurance components). Die Prüfungsintensität kann nach sogenannten Vertrauenswürdigkeitsstufen (Evaluation Assurance Levels, EAL) angepasst werden. Der Prüfumfang sowie die Prüfmethode ergeben sich aus der angestrebten EAL-Stufe für das jeweilige zu prüfende Produkt (TÜV Nord 2017a). Die Common Criteria werden vorwiegend für behördliche Produkte (wie z. B. Smart Cards, Zugangsberechtigungssysteme oder biometrische Systeme) verwendet. Ausgewählte europäische Sicherheitsbehörden haben im Rahmen des sogenannten SOG-IS-Abkommens (Senior Officials Group – Information Systems Security) festgelegt, dass auf Basis der gemeinsamen Kriterien erstellte Zertifikate bis zur EAL-Stufe 4 anerkannt werden. Für bestimmte technische Bereiche wie z. B. Smart Cards, ist auch eine höherwertige Anerkennung möglich. Jedoch sind bisher lediglich 14 der europäischen Mitgliedstaaten dem SOG-IS Abkommen beigetreten (SOGIS 2017). Weltweit werden Zertifikate nur mit EAL 1 und 2 im Rahmen des Common Criteria Recognition Arrangements (CCRA) gegenseitig anerkannt (Bundesrat 2017).

Während die ISO/IEC 27001 und IEC 62443 Anforderungen an Unternehmen bzw. Produkte/Systeme definieren (Gegenstand der Bewertung), beschreiben die Common Criteria bzw. die ISO/IEC 15408 die Anforderungen, Prüfung und Bewertung selbst, sprich für die Konformitätsbewertung an eine Konformitätsbewertungsstelle (Normen zur Evaluierung), und legen fest, mit welchem Prüfaufwand welche Vertrauenswürdigkeitsstufe hinsichtlich der Prüfung erreicht werden kann. Damit legen die Common Criteria keine Anforderungen an das Produkt bzw. die Prozesse fest, tragen jedoch insbesondere im internationalen behördlichen Kontext zu gemeinsamen Prüfungskriterien und zur gegenseitigen Anerkennung bei.

Der regulative Rahmen und das System der Konformitätsbewertung

Produkte und Dienstleistungen, die auf dem europäischen Binnenmarkt angeboten werden, müssen Anforderungen in Bezug auf Sicherheit, Gesundheit, Umwelt- und Verbraucherschutz einhalten. Im sogenannten alten Konzept (Old Approach) wurden die notwendigen technischen und administrativen Anforderungen an Produkte und Dienstleistungen detailliert in Rechtsvorschriften beschrieben (Europäische Kommission 2016). Seit der Einführung des sogenannten neuen Konzepts (New Approach) im Jahr 1985 (Official Journal of the European Communities 1985) müssen die auf dem EU-Markt in Verkehr gebrachten Produkte harmonisierten „wesentlichen Anforderungen“ in Bezug auf Sicherheit, Gesundheit, Umwelt- und Verbraucherschutz entsprechen

(Europäische Kommission 2016). Die wesentlichen Anforderungen werden gemäß dem Vertrag über die Arbeitsweise der Europäischen Union in Form von Verordnungen, Richtlinien und Beschlüssen definiert (Art. 288 AEUV). Diese betreffen große Produktfamilien (wie z. B. Spielzeug, Bauprodukte oder Maschinen) bzw. horizontale Risiken (wie z. B. elektromagnetische Verträglichkeit) (CEN 2018). Die spezifischen Anforderungen an die Produkte werden in harmonisierten Normen festgeschrieben (Europäische Kommission 2016). Dazu kann die Europäische Kommission die Europäischen Normungs- und Standardisierungsorganisationen (CEN/CENELEC bzw. ETSI) auffordern, technische Normen und Spezifikationen zu entwickeln, falls diese noch nicht verfügbar sind. Die Verwendung der harmonierten Normen ist nicht gesetzlich erforderlich – allerdings löst deren Anwendung die Vermutungswirkung gegenüber Dritten aus, dass der Hersteller durch die Beachtung der Normen die gesetzlich vorgeschriebenen Anforderungen erfüllt (DIN 2018). Falls ein Hersteller beschließt, andere technische Spezifikationen zu nutzen, obliegt es ihm (in den meisten Fällen durch die unabhängige Bestätigung eines Dritten) nachzuweisen, dass wesentliche Anforderungen erfüllt wurden (Europäische Kommission 2016). Das CE-Zeichen (Conformité Européenne, d. h. europäisches Konformitätszeichen) kennzeichnet als Herstellererklärung, dass das Produkt den Anforderungen der geltenden europäischen Richtlinien bzw. Verordnungen entspricht. Dies richtet sich jedoch nicht (wie fälschlicherweise oftmals angenommen) an die Verbraucher (ANEC 2012), sondern an Marktüberwachungsbehörden.

Die Art der Konformitätsbewertung ergibt sich mit dem Gesamtkonzept zur Konformitätsbewertung (Global Approach) aus dem Jahr 1990 aus der Zuordnung in sogenannte Module (A bis H) der jeweiligen Richtlinien und Verordnungen und bewegt sich zwischen Herstellererklärungen und einer Konformitätsbewertung durch eine sogenannte Notifizierte Stelle (Europäische Kommission 2016). Als Erweiterung des neuen Ansatzes wurde im Jahr 2008 der „neue Rechtsrahmen“ (New Legislative Framework, NLF) eingeführt. Dieser umfasst neben der Verordnung (EG) Nr. 765/2008 zur Schaffung einer rechtlichen Grundlage der Akkreditierung und der Marktüberwachung die Verordnung (EG) Nr. 764/2008 über Verfahren im Zusammenhang mit der gegenseitigen Anerkennung in der EU und den Beschluss Nr. 768/2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten (Europäische Kommission 2016).

Der Konformitätsbewertung, definiert nach ISO als „Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind“ (ISO/IEC 2004), kommt demnach eine wesentliche Rolle zum Nachweis der Einhaltung wesentlicher Anforderungen an Produkten und Dienstleistungen sowie dem Abbau von Handelshemmnissen (durch die gegenseitige Anerkennung von Konformitätsbewertungen) im internationalen Handel zu. Das System der Konformitätsbewertung besteht gemäß Teichler et al. (2013) aus den folgenden drei Bestandteilen:

- die Anforderungen an Produkte bzw. Dienstleistungen: definiert bspw. durch harmonisierte europäische Normen und Standards
- Aktivitäten der Konformitätsbewertung: Diese beinhalten neben der Prüfung, Inspektion und Zertifizierung (ISO/IEC 2004) auch weitere Tätigkeiten wie die Kalibrierung, Verifikation, Anbieten von Eignungsprüfungen und Herstellen von Referenzmaterialien.
- die Bestätigung der Kompetenz der Konformitätsbewertungsstelle. Dies erfolgt gemäß der Verordnung (EG) Nr. 765/2008 durch eine nationale Akkreditierungsstelle.

Im Hinblick auf den Bedarf an Konformitätsbewertung werden in Deutschland die folgenden drei Bereiche unterschieden:

Im freiwilligen Bereich erfolgt die Konformitätsbewertung auf Initiative der Marktteilnehmer hin. Im Zuge von Marktkräften können Marktteilnehmer beispielsweise ein Interesse haben, als vertrauensbildende Maßnahme Konformitätsnachweise, wie Zertifikate, zu nutzen. Der Staat gibt hier keine Vorgaben vor, kann diese Initiativen jedoch unterstützen, z. B. durch Mitarbeiten in Normenausschüssen oder Nachfrage von Konformitätsbewertungsdienstleistungen (z. B. freiwillige Zertifizierung von Managementsystemen von Behörden). Konformitätsbewertungen können dazu beitragen, bestehende Informationsasymmetrien zwischen Marktteilnehmern zu verringern. Viscusi (1978) beschreibt mit Hilfe der Signaling Theorie, dass Hersteller den Verbrauchern beispielsweise Produkteigenschaften mit Hilfe von Zertifizierungen signalisieren, um sie in die Lage zu versetzen, sich für Produkte mit hoher Qualität zu entscheiden. Damit trägt ein Zertifikat oder die Verwendung eines Labels zur Vertrauensbildung bei.

Im gesetzlich geregelten Bereich gibt der Staat in seiner Rolle als Regulierer Vorgaben und kann damit sowohl bei der Festlegung der Anforderungen, bei Vorgaben zur Konformitätsbewertung als auch bei der Kompetenzbestätigung aktiv eingreifen. Dies erfolgt im Zuge des New Approachs und des NLF durch die Festlegung von wesentlichen Anforderungen in EU-Richtlinien und EU-Verordnungen, wobei die Konformitätsbewertung in der Regel durch sogenannte Notifizierte Stellen (wie der Bundesanstalt für Materialforschung und -prüfung, BAM) erfolgt. Die Akkreditierung (als eine Art der Konformitätsbewertung) hat zum Ziel, die Kompetenz der Konformitätsbewertungsstelle unparteilich zu bestätigen und damit das Vertrauen zu erhöhen. Darüber hinaus wird eine Akkreditierungen durch Anerkennungsabkommen der Akkreditierungsorganisationen gefördert. Auf europäischer Ebene wird die von der European co-operation for Accreditation (EA) im Rahmen des Multilateral Agreement (EA MLA) erreicht. International sind derzeit zwei Abkommen in Kraft: Zum einen wird die Anerkennung der Akkreditierungen von Laboratorien und Inspektionsstellen durch die International Laboratory Accreditation Cooperation (ILAC) in Form von Mutual Reco-

gnition Arrangements (MRA) gewährleistet. Zum anderen wird die globale Anerkennung von Akkreditierungen von Zertifizierungsstellen vom International Accreditation Forum (IAF) in Form von Multilateral Agreements (MLA) ermöglicht (Deutsche Akkreditierungsstelle 2018).

Im hoheitlichen Bereich obliegt es dem Staat, die Rahmenbedingungen für Konformitätsbewertung festzulegen, diese ggf. selbst zu übernehmen bzw. die Grundlagen dafür selbst festzulegen. Dies ist beispielweise im Schutzbereich der inneren Sicherheit, wie z. B. der Justiz und der Polizei, der Fall. Ein konkretes Beispiel umfasst die Konformitätsbewertung von Metalldetektoren und Scannern für Gepäck und Passagiere, die z. B. am Flughafen eingesetzt werden. Der Staat legt in diesem Bereich die Anforderungen fest (z. B. mit eigenen Spezifikationen oder durch Bezug auf Normen), führt die Konformitätsbewertung eigenständig durch oder lässt diese durch von ihm zugelassene bzw. zertifizierte Konformitätsbewertungsstellen überprüfen und übernimmt auch die Kompetenzüberprüfung dieser Konformitätsbewertungsstellen, beispielsweise durch die Zertifizierung der Auditoren (Teichler et al. 2013). Das Hauptargument für eine Konformitätsbewertung im hoheitlichen Bereich liegt darin, dass es möglich ist, sowohl die Prüfanforderungen als auch die Prüfmethoden vertraulich zu halten. Ein negativer Effekt dabei ist, dass Unternehmen ihre Produkte und Systeme aufgrund national unterschiedlicher Anforderungen mehrfachen Prüfung unterziehen müssen, falls die Zertifikate international nicht gegenseitig anerkannt werden (Wurster und Murphy 2014).

Die Konformitätsbewertung soll dazu beitragen, Marktunvollkommenheiten zu internalisieren. Die Informationsasymmetrie beispielsweise beschreibt den Zustand, wenn Käufer und Verkäufer über unterschiedliche Wissensstände verfügen (Stiglitz 2000). Der amerikanische Wissenschaftler Akerlof (1970) hat am Beispiel des Gebrauchtwagenmarktes beschrieben, wie ein Markt scheitern kann. Anderson und Moore (2006) beschreiben in ihrem Aufsatz über die Ökonomie der Informationssicherheit, dass es sich im Bereich von Sicherheit von Software auch um einen Markt handelt, in dem Verbraucher Signale brauchen, um die Qualität von IT-Sicherheitssoftware zu erkennen. Die folgende Abbildung 9.3 stellt das System der Konformitätsbewertung mit den drei Bereichen und Elementen grafisch als Zusammenfassung dar.

Als der New Approach und der NLF in Europa eingeführt wurden, beschränkten sich die zu harmonisierenden Aspekte auf die Bereiche Sicherheit, Gesundheit, Umwelt- und Verbraucherschutz (Europäische Kommission 2016). Da aus Sicht verschiedener Akteure (ANEC und BEUC 2018; IFIA/CEOC 2017; VdTÜV 2017) Cybersicherheit eine Voraussetzung für die Sicherheit von Produkten, Dienstleistungen und Prozessen ist, kann es nun einen grundsätzlichen Bedarf geben, die grundlegenden Anforderungen an Produkte und Dienstleistungen zu überarbeiten sowie regulative Maßnahmen zur Erhöhung der Cybersicherheit in Europa zu ergreifen.

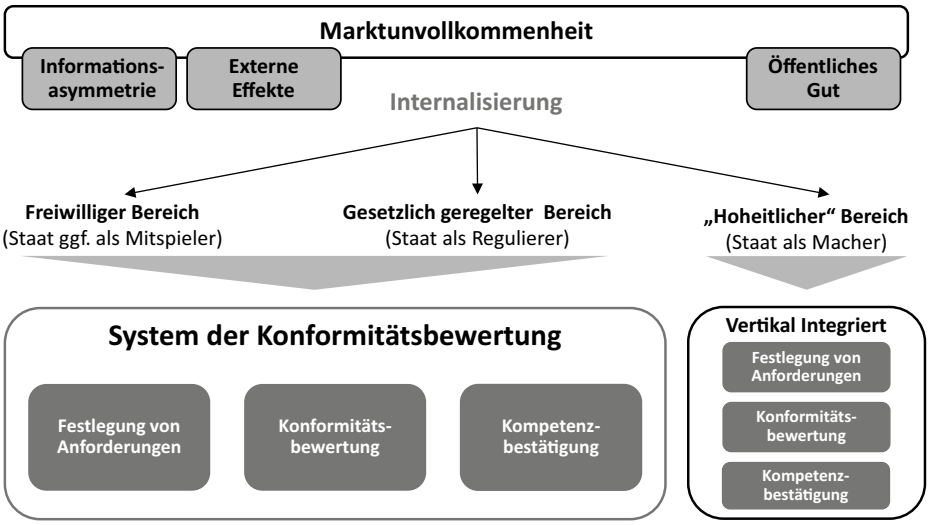

Abb. 9.3: Das System der Konformitätsbewertung und Formen der Internalisierung (Quelle: Eigene Darstellung basierend auf Teichler et al. (2013)).

Europäische Initiativen zur Erhöhung der Cybersicherheit: Cybersicherheitsplan der EU und Richtlinie über die Sicherheit von Netz- und Informationssystemen

Im Jahr 2013 veröffentlichte die EU einen „Cybersicherheitsplan der EU für ein offenes, freies und chancenreiches Internet" (Europäische Kommission 2013). Der Cybersicherheitsplan beinhaltet die Rolle von Sicherheitsnormen, Sicherheitssiegeln sowie EU-weiten Zertifizierungssystemen. Die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) ist der erste Teil einer EU-weiten Gesetzgebung zur Erhöhung der Cybersicherheit. Sie zielt auf Dienste ab, die für Gesellschaft und Wirtschaft wesentlich sind und zunehmend auf IKT angewiesen sind und schließt Betreiber wesentlicher Dienste in den Bereichen Energie, Verkehr, Wasser, Banken, Finanzmarktinfrastrukturen, Gesundheitswesen und digitale Infrastruktur sowie Anbieter digitaler Dienste, wie Suchmaschinen, Cloud-Computing und Online-Marktplätze, ein. Um diese Richtlinie zu verabschieden, mussten die EU-Mitgliedstaaten spätestens bis Mai 2018 nationale Gesetze einführen und die Betreiber wesentlicher Dienste bis spätestens November 2018 ermitteln (European Commission 2016). Die nationale Umsetzung der NIS-Richtlinie erfolgte jedoch nicht fristgerecht in allen Ländern, wobei der aktuelle Stand auf der Website der Europäischen Kommission einzusehen ist (European Commission 2018). In Deutschland wurde das Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 in der Union bereits am 23.06.2017 beschlossen, welches auf dem IT-Sicherheitsgesetz aus dem Jahr 2015 aufbaut (BSI 2016). Dieses Gesetz änderte das bislang gültige BSI-Gesetz und gibt nunmehr den von dem Gesetz betroffenen Unternehmen vor, Maßnahmen zur Bewältigung von Sicherheitsrisiken

nach dem „Stand der Technik“ zur Gewährleistung eines hohen Sicherheitsniveaus umzusetzen.

In diesem Zusammenhang fordert die zuständige Behörde, dass Betreiber wesentlicher Dienste mit dem Inkrafttreten der NIS-Richtlinie mit Hilfe einer Zertifizierung einer akkreditieren Konformitätsbewertungsstelle nachzuweisen haben, dass die Anforderungen an ein ISMS im Sinne der ISO/IEC 27001 und zusätzlicher, branchenspezifischer Normen, wie z. B. DIN SPEC 27019, für Energieversorger (Bundesnetzagentur für Elektrizität 2016) erfüllt werden. Diese Forderung bestand für Energieversorger bzw. Akteure in den Sektoren Wasser, Ernährung und Informationstechnik und Telekommunikation bereits bis zum Stichtag 31.01.2018 bzw. 03.05.2018. Für die Sektoren Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen gilt die Frist von Juni 2019 zur Erbringung des Nachweises (TÜV Nord 2018). Dieser Nachweis ist für Anbieter digitaler Dienste zwar nicht gefordert, jedoch müssen diese Anbieter seit dem 10.05.2018 auch Maßnahmen nach dem Stand der Technik in Bezug auf IT-Sicherheit ergreifen und Sicherheitsvorfälle melden (BSI 2017).

Es bleibt anzumerken, dass von der NIS-Richtlinie nur ein Bruchteil der Unternehmen in Deutschland, z. B. im Bereich der kritischen Infrastrukturen gemäß dem BSI nur 2.000 der ca. 3,5 Millionen (Stand 2016), betroffen sein werden (BSI 2016). Eine sehr viel größere potentielle Tragweite in Bezug auf die Konformitätsbewertung im Zusammenhang mit der Erhöhung von Cybersicherheit stellt der im Folgenden dargestellte Verordnungsentwurf zum Cybersecurity Act dar.

Case Study: Vorschlag eines Rechtsakts zur Cybersicherheit (Cybersecurity Act)

Im September 2017 legte die Europäische Kommission einen „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die ‚EU Cybersicherheitsagentur, (ENISA) […]“ sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“) vor (Bundesrat 2017). In der vorherigen Folgenabschätzung wurden mehrere Probleme im Zusammenhang mit der zunehmenden Anzahl von Cyber-Vorfällen in Europa identifiziert:

- „Unterschiedliche, nebeneinander bestehende Konzepte und Ansätze im Bereich der Cybersicherheit in den Mitgliedstaaten,
- verstreute Ressourcen und uneinheitliche Ansätze aller Organe, Einrichtungen und sonstigen Stellen der EU im Bereich der Cybersicherheit und
- unzureichende Sensibilisierung und Aufklärung der Bürger und Unternehmen in Verbindung mit dem zunehmenden Aufkommen zahlreicher nationaler und sektorspezifischer Zertifizierungssysteme“ (Bundesrat, 2017)

Der vorgeschlagene Cybersecurity Act verfolgt zwei Ziele: erstens die aktuelle Marktfragmentierung von Cybersecurity-Zertifikaten zu beheben und zweitens die Sicherheit und das Vertrauen von IKT-Produkten und -Dienstleistungen zu erhöhen.

Zur Folgenabschätzung hat die Europäische Kommission gemeinsam mit ENISA im Jahr 2017 eine europaweite Umfrage durchgeführt, die sich an Behörden der Mitgliedsstaaten, Unternehmen und Verbraucherverbände richtete. Im Rahmen dieser quantitativen Erhebung wurden u. a. vier Optionen zum Umgang mit nationalen Cybersicherheitssystemen abgefragt:

- Option 0: Nichts tun: Keine politische Initiative oder Maßnahme der EU
- Option 1: Soft-Law-Ansatz: Kommission würde nationale oder branchenspezifische Initiativen fördern und unterstützen
- Option 2: Ausweitung des SOG-IS-Abkommens (Abkommen ausgewählter Sicherheitsbehörden im Zusammenhang mit den Common Criteria): Legislativer Vorschlag, der die Teilnahme der Mitgliederstaaten an dem SOG-IS-Abkommen verbindlich vorschreibt
- Option 3: Europäisches Zertifizierungssystem: EU-weiter Zertifizierungsrahmen mit eigenem Geltungsbereich, Regeln für die Arbeitsweise und deren Überwachung (ENISA 2017)

Die Rückmeldung von 33 Teilnehmern der Befragung (von denen 14 Teilnehmer nationalen Behörden der Mitgliedstaaten angehörten) hatte das Ergebnis, dass Option 3 mit 33 % die höchste Zustimmung hatte. Dieses Ergebnis bildete neben weiteren Erhebungen und Workshops im Rahmen der Folgenabschätzung die Grundlage für die Ausarbeitung des Rechtsakts zur Cybersicherheit (European Commission 2017b).

Die Zertifizierung, definiert im Rahmen des Vorschlages als „förmliche Evaluierung von Produkten, Diensten, Prozessen durch eine unabhängige und akkreditierte Stelle anhand bestimmter definierten Kriterien und Normen“ (Bundesrat 2017. S. 10), soll demnach dazu beitragen, die Sicherheit zu erhöhen und das Vertrauen zu stärken, indem Nutzer und Käufer über die sicherheitsrelevanten Eigenschaften der Produkte und Dienste informiert werden.

Dazu soll die europäische Agentur ENISA beauftragt werden, einen europäischen Rahmen „für die Ausarbeitung spezifischer Zertifizierungssysteme für bestimmte IKT Produkte/-Dienste für europäische Cybersicherheitssysteme“ (Bundesrat 2017) zu schaffen. Dementsprechend würden mit dem Cybersecurity Akt keine operativen Zertifizierungssysteme geschaffen bzw. eingeführt werden, sondern zunächst ein Rahmen. Dieser Rahmen soll folgende Elemente beinhalten (Bundesrat 2017):

- Produktkategorien und -art der betroffenen IKT-Produkte und Dienste: Allgemein wurden vernetzte Geräte (IoT) als Ausgangpunkt für die Idee eines Zertifizierungssystems genannt. Der vorgeschlagene Rahmen sollte jedoch nicht auf bestimmte Produkte, Systeme oder Dienstleistungen beschränkt sein. Bestimmte Technologien, wie industrielle Automatisierungssysteme, vernetzte und selbstfahrende Fahrzeuge, elektronische Gesundheitssysteme und intelligente Netze

(Smart Grids) wurden konkret genannt, da sie ein hohes Maß an Cybersicherheit erfordern.
- Kriterien für die Zertifizierung: Die Zertifizierung besteht hierbei in der „förmlichen Evaluierung von Produkten, Diensten und Prozessen durch eine unabhängige und akkreditierte Stelle anhand bestimmter definierter Kriterien und Normen". Dabei können existierende Normen verwendet werden oder bei Bedarf neue Normen entwickelt werden.
- Vorgesehene Vertrauenswürdigkeitsstufe: Die Zertifizierung sollte unterschiedliche Vertrauenswürdigkeitsstufen enthalten, z. B. niedrig, mittel oder hoch, wobei sich die Vertrauenswürdigkeitsstufe auf ein begrenzten, mittleres Maß oder hohes Maß an Vertrauen, bezieht, dass das Zertifikat „in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produktes oder -Dienstes" vermitteln soll. Dabei kann ein europäisches System für die Sicherheitszertifizierung je nach Produkt- bzw. Dienst eine oder mehrere Vertrauenswürdigkeitsstufen beinhalten, wobei eine Einordnung von Produkt- bzw. Dienstleistungsgruppen in die drei vorgesehenen Vertrauenswürdigkeitsstufen noch zu erfolgen hat.

Darüber hinaus soll eine Europäische Gruppe für die Cybersicherheitszertifizierung eingerichtet werden, die aus „nationalen Zertifizierungsaufsichtsbehörden aller Mitgliedstaaten" besteht (Bundesrat 2017). Diese Gruppe würde die ENISA bei der Erstellung der von der Europäischen Kommissionen geforderten Zertifizierungssysteme für Cybersicherheit unterstützen.

In Bezug auf die Verbindlichkeit der Cybersicherheitszertifizierung, sollte „der Rückgriff auf eine europäische Cybersicherheitszertifizierung […] daher weiterhin auf freiwilliger Basis erfolgen, sofern in den Rechtsvorschriften der Union zur Festlegung von Anforderungen an die Sicherheit von IKT-Produkten und -Diensten nicht etwas anderes bestimmt ist" (Bundesrat 2017). Aus diesem Passus ergibt sich, dass Unternehmen zunächst (bis weitere Rechtsvorschriften erlassen werden, die sich auf die Cybersicherheit Zertifizierungssysteme beziehen) frei wählen können, ob sie ihre Produkte und Dienstleistungen zertifizieren lassen. Allerdings sollen aufgrund des „Vorrang(s) der europäischen Systeme für die Cybersicherheitszertifizierung vor den nationalen Systemen" (Bundesrat 2017) nationale Cybersicherheits-Zertifizierungssysteme nicht mehr bestehen dürfen und neben den europäischen Systemen und keine nationalen Systeme für die gleichen IKT-Produkte bzw. -Dienste einer bestimmten Vertrauenswürdigkeitsstufe parallel betrieben werden. Bestehende Zertifikate wären jedoch bis zum Ablauf gültig. Dem Vorschlag zufolge könnten nationale Regelungen nur dann weiterhin bestehen, wenn IKT-Produkte und -Dienstleistungen nicht durch ein europäisches System zur Zertifizierung von Cybersicherheit abgedeckt sind (Bundesrat 2017).

9.3 Öffentliche Diskussionen zum Cybersecurity Act-Vorschlag

Der Cybersecurity Act-Vorschlag hat eine kontroverse Diskussion ausgelöst und dazu geführt, dass sich interessierte Kreise mit dem Thema Zertifizierung von Cybersicherheit auseinandergesetzt und sich dazu öffentlich umfassend geäußert haben. Mit Hilfe der umfangreichen Positionspapiere, Präsentationen und Beiträge in öffentlichen Diskussionsrunden konnte eine umfangreiche Datenbasis aufgebaut werden, die für die folgende Analyse genutzt wurde. Der Cybersecurity Act-Vorschlag wurde im September 2017 veröffentlicht. Hier werden folgende Datenquellen im Zeitraum zwischen September 2017 und März 2018 analysiert:

- Feedback an die Kommission, Vorschlag eines Rechtsakts zur Cybersicherheit während der öffentlichen Konsultationsphase (European Commission 2017b)
- Podiumsgruppenteilnehmer und veröffentlichte Präsentationen der öffentlichen Anhörung zum „Cybersecurity Act" des Europäischen Wirtschafts- und Sozialausschusses (European Economic and Social Committee 2018)
- Podiumsgruppenteilnehmer und veröffentlichte Präsentationen einer Konferenz der europäischen Normungsorganisationen und der ENISA mit dem Titel „Cybersecurity Act – Establishing the Link between Standardisation and Certification" (CEN/CENELEC 2018b)
- Schriftliche Stellungnahmen, die außerhalb der öffentlichen Konsultationsphase veröffentlicht wurden

Die veröffentlichten Positionspapiere/Presseveröffentlichungen sowie Präsentationen wurden systematisch auf Aussagen hinsichtlich eines europäischen Rahmens für die Cybersicherheitszertifizierung analysiert. Aus den insgesamt 74 Dokumenten wurden insgesamt 343 Aussagen identifiziert und zu übergreifenden Themen zusammengefasst. In einem folgenden Schritt wurden die zuvor identifizierten übergeordneten Themen innerhalb der einzelnen Interessengruppen verglichen und Unterschiede zwischen den einzelnen Interessengruppen identifiziert.

9.4 Einschätzungen durch die Interessengruppen

Übergreifende Analyse der Aussagen von Interessengruppen zum Cybersicherheit-Zertifizierungsrahmen

Im Rahmen der folgenden Analyse wurden die Interessengruppen näher betrachtet, die sich nach de Vries et al. (2003) in der Regel auch an Projekten zur Normung in IT-relevanten Bereichen beteiligen. Abbildung 9.4 zeigt auf, dass Unternehmensverbände und Unternehmen die aktivsten Akteure im Betrachtungszeitraum in Bezug auf die Anzahl der Beiträge waren, gefolgt von Standardisierungsorganisationen und Kon-

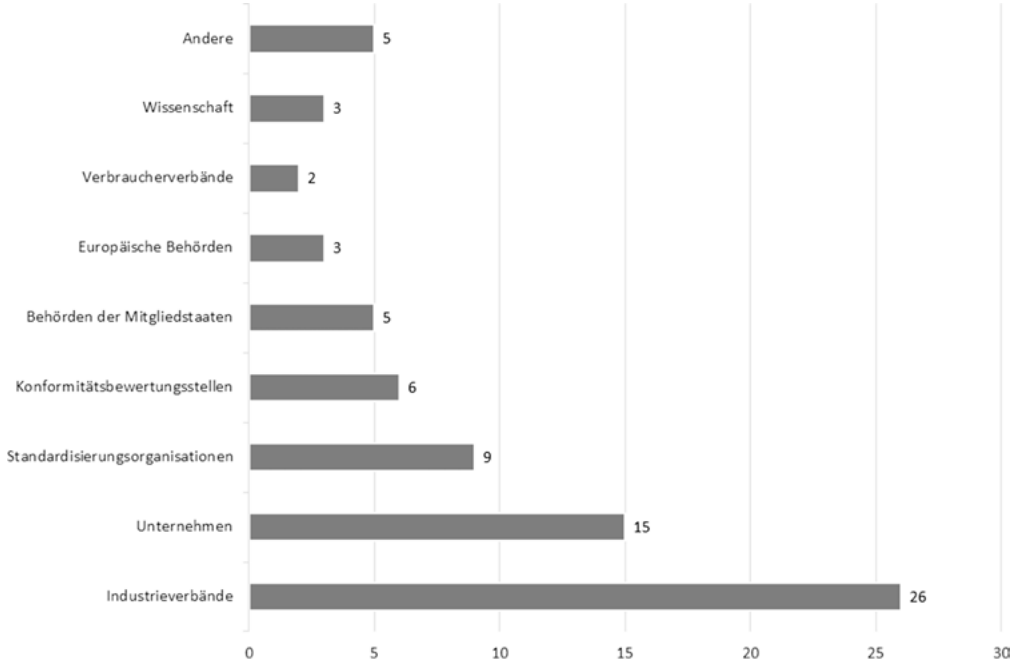

Abb. 9.4: Anzahl der Beiträge von interessierten Kreisen (Quelle: Eigene Darstellung).

formitätsbewertungsstellen. Die Mitgliedstaaten bzw. deren Behördenvertreter haben nach Kenntnis der Autorin im Betrachtungszeitraum keine offiziellen Stellungnahmen veröffentlicht, jedoch ihre Ansichten auf einer von der Kommission und der ENISA (ENISA conference 2018) organisierten Konferenz zum Ausdruck gebracht.

Die Diskussion zu dem im Verordnungsvorschlag geplanten Rahmen für die Zertifizierung zur Cybersicherheit betraf vier übergreifende Themenfeldern mit den jeweils identifizierten Ausgestaltungsmöglichkeiten (Bundesrat 2017):

- Ausgestaltung des Rahmens für die Konformitätsbewertung: Sollten der Rahmen bzw. die Konformitätsbewertung freiwillig oder verpflichtend sein (also in den freiwilligen, gesetzlich geregelten oder hoheitlichen Bereich fallen)?
- Art der Konformitätsbewertung: Durch wen darf die Konformitätsbewertung durchgeführt werden (wird eine dritte Partei stets notwendig sein oder wird eine Herstellererklärung auch zulässig sein)?
- Zugrundeliegenden Anforderungen für die Konformitätsbewertung: Gegen welche Kriterien soll die Konformitätsbewertung erfolgen (nationale versus europäische versus globale Normen)?
- Rollen und Verantwortlichkeiten: Wer wird den Rahmen und später die Grundlagen der Konformitätsbewertung (z. B. Zertifizierungssysteme) weiterentwickeln und durch wen erfolgt die Überwachung der relevanten Akteure?

Analyse der Gruppen der einzelnen interessierten Kreise

Um zu einem tieferen Verständnis zu den Ausgestaltungsmöglichkeiten eines europäischen Cybersicherheit-Zertifizierungssystems zu kommen, werden im folgenden Abschnitt die zusammenfassten Positionen je Interessengruppe vorgestellt:

Industrie (Unternehmen und Wirtschaftsverbände)

Freiwillige versus verpflichtende Konformitätsbewertungen: Unternehmen und Unternehmensverbände sprechen sich grundsätzlich für freiwillige Systeme im B2C- und B2B-Bereich aus. Dies wird damit erklärt, dass Unternehmen ein intrinsisches Interesse haben, sichere Produkte auf den Markt zu bringen. Es wurden ferner alternative Mechanismen vorgeschlagen, die sich auf die Eigenverantwortung der Industrie stützen würden, wobei das Programm der EU zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH) als konkretes Beispiel diente (LEET Security 2017). Im B2B-Bereich wurde darauf hingewiesen, dass der Zweck der Vertrauensbildung durch Zertifikate und Labels aufgrund fehlender Informationsasymmetrien zwischen Unternehmen in einigen Branchen nicht besteht (Bähr 2017; VDMA 2017).

Art der Konformitätsbewertung: Unternehmen und Unternehmensverbände befürchten, dass die Einführung verpflichtender Konformitätsbewertungen durch eine externe dritte Partei die europäische Wirtschaft zusätzlich belasten und damit schwächen könnten. Um eine umfassende Konformitätsbewertung (einschließlich aller relevanten Schnittstellen) durchführen zu können, benötigen Dritte zudem Zugriff auf alle relevanten Daten. Hierbei zögert die Industrie, da sie hierfür sensible Unternehmensdaten offenbaren müsste. Unternehmen weisen darauf hin, dass Selbsteinschätzungen (z. B. durch unternehmensinterne Konformitätsbewertungsstellen) und eine darauf basierende Herstellererklärung ein angemessenes oder sogar höheres Maß an Sicherheit bieten können als Konformitätsbewertungen durch eine externe dritte Partei (Friedrich 2018). Da die Zertifizierung immer von einer dritten Partei durchgeführt wird, verursacht sie ggf. zusätzliche Kosten und die Einbindung eines Externen könnte unter Umständen auch zeitintensiver sein. Dies könnte die Zeit bis zur Markteinführung verlängern, was in einer durch sehr kurze Innovationszyklen gekennzeichneten Branche erhebliche Nachteile mit sich bringen kann. Des Weiteren würden kleine und mittelständische Unternehmen (KMU) überdurchschnittlich belastet. Vertreter von Unternehmensverbänden weisen deshalb darauf hin, dass der vorliegende Vorschlag dem etablierten neuen Rechtsrahmen (New Legislative Framework) nicht stringent folgt. Der Gesetzgeber sollte lediglich die grundlegenden Anforderungen festlegen und eine Einteilung in die Module vornehmen. Als Alternative wird eine risikobasierte, horizontale Regulierung von Cybersicherheit statt einer regulatorischen Konformitätsbewertung vorgeschlagen (VDMA 2017).

Rolle der zugrundeliegenden Anforderungen und Normen: Unternehmen und Unternehmensverbände betonen die Rolle von Normen als Anforderungsdokumente. Da die Unternehmen, die Feedbacks eingereicht oder an Podiumsdiskussionen teilgenommen haben, auf internationalen Märkten tätig sind, bevorzugen sie internationale Normen gegenüber europäischen Normen. Dies gilt insbesondere im Zusammenhang mit Unternehmen, die in globale Wertschöpfungsketten integriert sind (European Commission 2017b).

Rollen und Verantwortlichkeiten: Unternehmensverbände und Unternehmen stellen die Rolle und Legitimität der „Europäischen Gruppe für die Cybersicherheitszertifizierung" in Frage, die für die Empfehlung der neuer oder weiterentwickelter Konformitätsbewertungssysteme an die Europäische Kommission verantwortlich sein soll. Neue Systeme sollten vielmehr gemeinsam mit der Industrie entwickelt werden. Eine Konsultation, wie sie derzeit vorgeschlagen wird, ist aus Sicht der Unternehmen nicht ausreichend. Lediglich Angelegenheiten der nationalen Sicherheit sollten nach breiter Auffassung der Industrie den nationalen Behörden, beispielsweise im Rahmen von dem SOG-IS-Abkommen, vorbehalten bleiben (European Commission 2017b).

Private Konformitätsbewertungsstellen

Freiwillige versus verpflichtende Konformitätsbewertungen: Private Konformitätsbewertungsstellen, die sich zu dem Cybersecurity Act-Vorschlag geäußert haben, befürworten grundsätzlich eine verpflichtende Zertifizierung. Da die geltende Richtlinie 2001/95/EG zur Produktsicherheit von einer „vernünftigerweise vorhersehbaren Verwendung" ausgeht (Europäisches Parlament und der Rat 2001), deckt sie, nach Auffassung eines Verbandes privater Konformitätsbewertungsstellen den potentiellen Missbrauch verbundener IoT-Geräte im Cyberraum möglicherweise nicht ab (VdTÜV 2017). Daher gäbe es nun einen Bedarf, die grundlegenden Anforderungen an Produkte und Dienstleistungen zu überarbeiten (CEN/CENELEC 2018a; IFIA/CEOC 2017; VdTÜV 2018). Da es einige Zeit dauern wird, Cybersicherheitsaspekte in alle sektoralen und produktspezifischen Richtlinien zu integrieren, können verpflichtende Zertifizierungssysteme als Übergangslösung sinnvoll sein (VdTÜV 2018). Diese sollten insbesondere bei Produkten mit höherem Risiko verpflichtend vorgeschrieben werden (IFIA/CEOC 2017).

Art der Konformitätsbewertung: Private Konformitätsbewertungsstellen betonen die Wichtigkeit einer unabhängigen Zertifizierung, um Vertrauen unter den Konsumenten aufzubauen und unabhängige Siegel vergeben zu können. Daher ist auch bei einer Regelung, die auf Freiwilligkeit setzt, eine Zertifizierung nur durch eine dritte Partei zu bevorzugen (IFIA/CEOC 2017). Da weder der Endnutzer die Cybersicherheit testen, noch der Hersteller unabhängig die Cybersicherheit bestätigen kann, ist eine Prüfung durch einen unabhängigen Dritten notwendig. Dazu ist es jedoch erforderlich, Zugang zu den betreffenden internen Daten der Unternehmen zu erhalten, um die

Konformitätsbewertungen (z. B. nach einer Softwareaktualisierung) vollständig und kontinuierlich durchführen zu können. In diesem Zusammenhang verweisen internationale Vereinigungen der Anbieter von Konformitätsbewertungsdienstleistungen jedoch darauf, dass öffentliche Behörden oftmals nicht über die notwendigen internen Ressourcen verfügen, um dieser Aufgabe gerecht zu werden, und betonen die Bedeutung von privaten Konformitätsbewertungsstellen (IFIA/CEOC 2017).

Rolle der zugrundeliegenden Anforderungen und Normen: Die Vereinigungen von internationalen Konformitätsbewertungsstellen betonen ebenfalls die Bedeutung von international akzeptierten Normen als Anforderungen der Konformitätsbewertung. Dies ist vor allem für global agierende Hersteller und Dienstleistungsanbieter essentiell. In diesem Zusammenhang wird die Adaption von international anerkannten Zertifizierungssystemen als europäische Zertifizierungssysteme (analog der Adaption internationaler ISO Normen als europäische Normen) vorgeschlagen (IFIA/CEOC 2017). Bestehende Normenreihen, wie z. B. ISO/IEC 15408, sollten dabei als Benchmark gelten (VdTÜV 2018).

Rollen und Verantwortlichkeiten: Ein wesentlicher Kritikpunkt der privaten Konformitätsbewertungsstellen beinhaltet, dass die interessierten Kreise, wie z. B. der private Sektor (einschließlich den privaten Konformitätsbewertungsstellen oder Verbraucherorganisationen), nur konsultiert, aber nicht aktiv an der Entwicklung von Systemen beteiligt werden sollten (VdTÜV 2018). Vorgeschlagen wird vielmehr, dass Vertreter der Industrie, Konformitätsbewertungsstellen sowie nationaler Behörden gemeinsam für die Entwicklung der Systeme verantwortlich sein sollen (IFIA/CEOC 2017).

Behörden der Mitgliedstaaten

Freiwillige versus verpflichtende Konformitätsbewertungen: Ein wesentlicher Diskussionspunkt für Behörden der Mitgliedsstaaten ist die Frage, ob nationale Systeme im Bereich der nationalen Sicherheit aufgrund der Souveränität der Einzelstaaten in diesem Bereich von einem europäischen System abgekoppelt werden sollten. Der Grund liegt darin, dass es den Einzelstaaten obliegt, das verfassungsmäßige Recht der Bürger in Bezug auf Sicherheit zu schützen. Daher weisen die Mitgliedstaaten auf das Recht der Behörden hin, eigene Konformitätsbewertungen im Bereich der nationalen Sicherheit zu verlangen bzw. die Konformitätsbewertung selber durchzuführen.

Art der Konformitätsbewertung: Vertreter der Behörden der Mitgliedsstaaten differenzieren bei der Art der Konformitätsbewertung je nach Risiko der Produktgruppe. Für Produkte mit hohem Risiko verweisen die Vertreter der Behörden auf unabhängige Dritte in Form akkreditierter Konformitätsbewertungsstellen. Allerdings erkennen die Behörden bei Produkten und Diensten mit niedrigem Risiko auch die Vorteile von Herstellererklärungen für die Industrie an. Um Produkte und Dienstleistungen auf hoher

Sicherheitsstufe beurteilen zu können, verweisen Vertreter der Behörden der Mitgliedstaaten auf erforderliche behördliche Einbeziehung bei der Sicherheitsbewertung.

Rolle der zugrundeliegenden Anforderungen und Normen: Vertreter der Behörden betonen auch die Wichtigkeit internationaler Normung und betonen die Transparenz der zugrundeliegenden Anforderungen der Konformitätsbewertungen vor allem im Hinblick auf eine international angestrebte Akzeptanz. In diesem Zusammenhang kann europäischen gegenüber internationalen Normen Vorzug gewährt werden (z. B. wenn diese dem Cybersicherheitsbedürfnis eher entsprechen). Dies sollte jedoch transparent kommuniziert werden. Ein Positionspapier des ECSO fasst den Meinungsaustausch während der ECSO-Sitzungen und die Kommentare der Mitgliedstaaten zusammen. Demnach haben Frankreich und Deutschland als Einzelstaaten Bedenken bezüglich des derzeitigen Vorschlags für den Aufbau eines Cybersicherheit-Zertifizierungsrahmens und würden die bestehenden Systeme (z. B. SOG-IS, basierend auf den Common Criteria) erweitern, anstatt sie zu ersetzen (ENISA conference 2018).

Rollen und Verantwortlichkeiten: Nach Auffassung von Vertretern der Behörden von Mitgliedstaaten sollten die nationalen Behörden das Recht behalten, neue Konformitätsbewertungssysteme zu initiieren und die Kontinuität von Systemen, wie dem SOG-IS-Übereinkommen, zu gewährleisten. Des Weiteren soll die Industrie mit einbezogen werden, um diese sichere Produkte zu entwickeln (ENISA conference 2018).

Verbraucherorganisationen

Freiwillige versus verpflichtende Konformitätsbewertungen: Europäische Verbraucherverbände befürworten verpflichtende Zertifizierungssysteme für diejenigen Produkte, welche ein hohes Risiko für die Gesundheit und Sicherheit der Verbraucher darstellen können. Falls es den Unternehmen frei überlassen wäre, ihre Produkte und Dienstleistungen zertifizieren zu lassen oder nicht, würde dies zu einer weiteren Fragmentierung des Marktes führen. Da der aktuelle Vorschlag eines Rechtsaktes versucht, gerade dies zu verhindern, sollten nach der Auffassung von zwei europäischen Verbraucherorganisationen Zertifizierungen verpflichtend sein (ANEC und BEUC 2018).

Art der Konformitätsbewertung: Die europäischen Verbraucherorganisationen weisen darauf hin, dass das Vertrauen der Verbraucher auf der unabhängigen und unparteiischen Konformitätsbewertung beruht. Daher bevorzugen diese Interessengruppen die Durchführung der Konformitätsbewertung durch eine dritte Partei.

Rolle der zugrundeliegenden Anforderungen und Normen: Die europäischen Verbrauchervertretungen heben die Bedeutung von Normen als Anforderungen für Zertifikate hervor, um den Verbrauchern zuverlässige Informationen zu liefern (Openforum Europe 2017a). Darüber hinaus sehen sie die Notwendigkeit von Mindestsicherheitsanforderungen für alle verbundenen Produkte und Dienste, die in horizontale Richt-

linien wie die über die allgemeine Produktsicherheit (2001/95/EG) integriert werden sollten (ANEC und BEUC 2018).

Rollen und Verantwortlichkeiten: Die europäischen Verbraucherverbände kritisieren, dass die Interessen der Verbraucher im vorliegenden Vorschlag nicht ausreichend vertreten sind, und fordern die Ernennung eines Verbraucherexperten für den ENISA-Verwaltungsrat. Darüber hinaus sollten Konsumenten regelmäßig konsultiert werden, wenn die „Europäische Gruppe für die Cybersicherheitszertifizierung" Zertifizierungssysteme erstellt (ANEC und BEUC 2018).

Europäische Standardisierungsorganisationen

Freiwillige versus verpflichtende Konformitätsbewertungen: Das Europäische Institut für Telekommunikationsnormen (ETSI) befürwortet, dass der aktuelle Vorschlag auch in Zukunft nur für freiwillige Zertifizierungen gelten soll, wobei für verpflichtende Konformitätsbewertungen im Bereich Cybersicherheit zukünftig der neue Rechtsrahmen (New Legislative Framework) gelten soll (ETSI 2018). Nationale Zertifizierungssysteme oder europäische Abkommen, wie z. B. SOG-IS, sollten nicht generell ausgeschlossen werden, insbesondere wenn die betroffenen Produkte und Dienstleistungen sich auf den Bereich der nationalen Sicherheit beziehen. Die Europäischen Komitees für Normung und für elektrotechnische Normung (CEN und CENELEC) empfehlen hingegen, den neuen Rechtsrahmen (New Legislative Framework) konsequent anzuwenden, anstatt ein paralleles Zertifizierungssystems zu etablieren, welches zur Verwirrung am Markt führen würde (CEN/CENELEC 2018a).

Art der Konformitätsbewertung: Europäische Standardisierungsorganisationen weisen darauf hin, dass der aktuelle Rechtsrahmen auch die Möglichkeit der Herstellererklärung vorsieht und dieses Prinzip beibehalten werden sollte. Dabei wird auf die Erfahrungen im gesetzlich geregelten Bereich, beispielsweise auf dem Gebiet der Produktsicherheit, verwiesen. Dies versetzt insbesondere KMUs in die Lage, sich im Wettbewerb mit großen Unternehmen zu behaupten (ETSI 2018).

Rolle der zugrundeliegenden Anforderungen und Normen: Die große Bedeutung von Normen im Zusammenhang mit Konformitätsbewertungssystemen wird von den europäischen Standardisierungsorganisationen hervorgehoben. ETSI und CEN/CENELEC empfehlen, wenn immer möglich, sich auf internationale Normen zu beziehen, um den Zugang der europäischen Industrie zu globalen Märkten nicht zu behindern. Dabei sollte der angestrebte Rahmen bestehende, weit verbreitete Normen, wie z. B. die Common Criteria (ISO/IEC 15408), Anforderungen an ISMS (ISO/IEC 27000ff) und Normen für industrielle Steuerungs- und Automatisierungstechnik (IEC 62443) sowie sektorspezifische Normen berücksichtigen (CEN/CENELEC 2018a). Des Weiteren besteht der Wunsch von CEN/CENELEC, dass die formell anerkannten europäischen und internationalen Standardisierungsorganisationen eingeladen werden, die zugrundeliegenden Anforderungen und Normen zu erstellen.

Hierbei sollten den international anerkannten Normen, die durch ISO, IEC oder ITU entwickelt wurden, Priorität eingeräumt werden.

Rollen und Verantwortlichkeiten: In Bezug auf Zuständigkeiten wird von CEN/CENLEC auf den Neuen Ansatz und dem NLF verwiesen, der eine Gewaltenteilung zwischen Legislative, Standardisierung und Konformitätsbewertung vorsieht (CEN/CENELEC 2018a). ETSI weist darauf hin, dass Interessengruppen, wie Konsumenten sowie die Industrie im Rahmen klarer Prozesse die Möglichkeit haben sollten, Feedback zu neuen und Änderungen an bestehenden Systemen vorzuschlagen (ETSI 2018).

9.5 Diskussion der Ergebnisse und Handlungsempfehlungen

Zusammenfassend lässt sich feststellen, dass die Meinungen innerhalb einer Interessensgruppe recht konsistent sind und die interessierten Kreise gemäß ihrer Stellung im System der Konformitätsbewertung argumentiert haben. Die kontroversen Diskussionen von Interessengruppen verdeutlichen jedoch, dass Initiativen zur Erhöhung der Cybersicherheit und Vertrauen von IKT Produkten und -Diensten zwar begrüßt werden, der aktuelle Vorschlag eines Rechtaktes zur Cybersicherheit viele, zurzeit noch unbeantwortete, offene Fragen aufwirft. Diese umfassen die diskutierten vier Fragen zur Ausgestaltung bzw. Entwicklung und Überwachung von Konformitätsbewertungssystemen.

In Bezug auf freiwillige versus verpflichtende Zertifizierungen, plädiert die Industrie für freiwillige Konformitätsbewertung und setzt auf die Mechanismen der wirtschaftlichen Selbstverwaltung. Während sie auf die langjährigen, guten Erfahrungen im Bereich der Herstellererklärung hinweist, sprechen sich private Konformitätsbewertungsstellen und Verbraucherverbände für eine verpflichtende Konformitätsbewertung durch eine dritte Seite aus (Art der Konformitätsbewertung), was wenig überrascht, wenn man sich die Rollenverhältnisse vor Augen ruft. In Bezug auf die zugrundeliegenden Anforderungen der Konformitätsbewertung wird die Rolle von internationalen Normen überwiegen hervorgehoben. Einigkeit besteht ferner in der bis dato unzureichenden Einbindung von allen relevanten Interessengruppen (insbesondere der Wirtschaft) bei der Entwicklung des Rahmens und zukünftigen Rollen und Verantwortlichkeiten der Europäischen Gruppe für die Cybersicherheitszertifizierung.

In der Gesamtschau der Positionen der verschiedenen Interessengruppen wird deutlich, dass eine Konsensfindung schwierig sein wird und eine differenziertere Betrachtung des Rahmens hilfreich wäre. Aus ordnungspolitischer Sicht kann das beschriebene System der Konformitätsbewertungssystem dazu beitragen, die richtige Einordnung von IKT-Produkten und -Dienste in die drei Sektoren freiwilliger Bereich, gesetzlich geregelter Bereich und hoheitlicher Bereich vorzunehmen. Daraus würde sich der Grad der Verbindlichkeit, die Art der Konformitätsbewertung sowie der Gegenstand der Konformitätsbewertung ableiten lassen.

Zertifizierungssysteme im freiwilligen Bereich können zur Erhöhung von Cybersicherheit von IKT Produkten und -Diensten beitragen, wenn diese im Sinne der Signaling-Theorie von den Anbietern selbst genutzt werden können bzw. aktiv von den Konsumenten eingefordert werden. In diesem Zusammenhang beinhaltet der Cybersecurity Act Vorschläge für die Einführung von Siegeln und Kennzeichnungen. Diese Siegel oder Kennzeichnungen wären dann erfolgreich, wenn sie in den Kaufentscheidungsprozessen der Konsumenten mitberücksichtigt würden. Dazu müssten die Kriterien für ein Zertifikat/Siegel jedoch risikobasiert, verwendungsorientiert und für den Konsumenten nachvollziehbar sein. Falls eine Abstufung (wie z. B. bei der Energieverbrauchskennzeichnung) vorgesehen wird, so sollte diese auf einer wissenschaftlich fundierten Bewertungsmethode basieren. In diesem Zusammenhang wird auf die Forschungs- und Entwicklungstätigkeiten des Joint Research Zentrums der Europäischen Kommission hingewiesen, das sich mit der Festlegung geeigneter Sicherheitskennzahlen und Vergleichswerten im Zuge einer quantitativen Bewertung von Produkten hinsichtlich der Cybersicherheit befasst. Falls Siegel und Kennzeichnungen eingesetzt würden, sollte der Konsument jedoch stets darüber informiert sein, dass es, ähnlich wie bei der Produktsicherheit, eine absolute Cybersicherheit nicht geben kann (European Economic and Social Committee 2018).

Nach dem Inkrafttreten des Cybersecurity Acts würde der Rahmen sowie spezifische Zertifizierungssysteme entwickelt werden, die nach dem jetzigen Verordnungsentwurf freiwilliger Natur sein würden. In diesem Zusammenhang würde der Überwachung der Einhaltung der zugrundeliegenden Kriterien eine besondere Rolle zukommen, insbesondere falls die Herstellererklärung ein mögliches Mittel der Konformitätsbewertung darstellt.

Die NIS-Richtlinie zum Schutz von kritischen Infrastrukturen und wesentlichen Diensten hat gezeigt, dass freiwillige Ansätze im Bereich der Cybersicherheit jedoch an Grenzen stoßen und somit die betroffenen Unternehmen verpflichtet werden mussten, Maßnahmen zur Netzwerk- und Informationssicherheit zu treffen und diese im Bereich der kritischen Infrastrukturen in Form von Zertifikaten nachzuweisen (Bendiek et al. 2017). Eine verpflichtende Zertifizierung aller Unternehmen, die im Bereich IoT Produkte und Dienste anbieten, würde jedoch Unternehmen und insbesondere KMUs aufgrund der zu erwartenden hohen Kosten in deren Wettbewerbsfähigkeit im globalen Markt benachteiligen. Die NIS-Richtlinie begegnet diesem Aspekt damit, dass Kleinstunternehmen und kleine Unternehmen im Bereich der Anbieter digitaler Dienste von Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen ausgenommen sind (BSI 2017). Eine kostengünstige Variante stellt die Herstellererklärung dar.

Der jetzige Verordnungsentwurf gibt einen Hinweis darauf, dass Rechtsvorschriften folgen können, die mit einer Verbindlichkeit einer Zertifizierung einhergehen können (Bundesrat 2017). In Bezug auf die verpflichtenden Zertifizierungen im gesetzlich geregelten Bereich würden jedoch die langjährigen positiven Erfahrungen dafür sprechen, die bewährte Methodik des Neuen Ansatzes und des NLF dahingehend anzu-

wenden, dass der Staat wesentliche Anforderungen an die Cybersicherheit (entweder als Zusatz zu bestehenden Richtlinien/Verordnungen oder als neue horizontale Verordnung) festlegt und eine Einteilung in die Module vornimmt, woraus sich die Art der Konformitätsbewertung (einschließlich der Möglichkeit der Herstellererklärung) ergibt. Die Spezifizierung der grundlegenden Anforderungen würde durch harmonisierte (vorzugsweise international anerkannte) Normen erfolgen mit der zuvor beschriebenen Vermutungswirkung für Unternehmen, die diese Normen nutzen. Bei einer konsequenten Anwendung des neuen Ansatzes und des NLF würde folgen, dass sich eine eventuell verpflichtende Zertifizierung bzw. die verpflichtende Nutzung von Siegeln und Kennzeichnungen für Unternehmen nicht aus dem Cybersecurity Act sondern aus produktgruppenspezifischen bzw. horizontalen Verordnungen ergeben würden. Eine derzeit viel diskutierte, konkrete Möglichkeit stellt die Einbeziehung von IoT-Produkten und Diensten in die Funkanlagenrichtlinie 2014/53/EU (Radio Equipment Directive) im Kapitel 3(3) dar (ANEC und BEUC 2018). In den grundlegenden Anforderungen der Funkanlagenrichtline werden cybersicherheitsrelevante Schutzanforderungen (wie z. B. Schutz vor missbräuchlicher Nutzung personenbezogener Daten sowie vor Betrug) formuliert, wobei der Europäischen Kommission im Jahr 2014 die Befugnis übertragen wurde, delegierte Rechtsakte zur Zuordnung von Kategorien und Klassen von Funkanlagen zu den in der Funkanlagenrichtlinie genannten Anforderungen zu erlassen.

Für Produkte und Dienstleistungen, die ein hohes Risiko für die öffentliche Sicherheit darstellen, scheint es ratsam und auch für andere Akteure akzeptabel, diese in den hoheitlichen Bereich aufzunehmen und der nationalen Souveränität den Mitgliedsstaaten zu überlassen. Die Mitgliedstaaten dürften dann eigene Anforderungen festlegen (z. B. mit eigenen technischen Spezifikationen) und, falls gewünscht, die Konformitätsbewertung auch eigenständig vornehmen. In diesem Zusammenhang wäre eine europaweit einheitliche Einordnung notwendig, welche Produkte und Dienste in diesen hoheitlichen Bereich fallen. Da jedoch Cybersicherheit keine Grenzen kennt und Unternehmen von einem europaweit gültigen Zertifikat aus Kosten- und Zeitgründen stets profitieren würden, ist demzufolge angemessen, auch im hoheitlichen Bereich eine weitestgehend Harmonisierung anzustreben. Dies sollte jedoch mit dem Ziel geschehen, das allgemeine europäische Cybersicherheitslevel auch im Bereich innere Sicherheit zu erhöhen anstelle eines vielfach befürchteten *race to the bottom* (ENISA conference 2018).

Zusammenfassend bestehen die größten Herausforderungen darin, zu definieren, welche Produkte, Dienste und Systeme in welchen Bereich der Konformitätsbewertung fallen, wobei ein risikobasierter Ansatz durchweg gefordert wird. Insbesondere für die Masse an IoT-Geräten im Bereich B2C werden gesetzlich vorgeschriebene Basissicherheitsanforderungen gefordert. Aus Standardisierungssicht besteht hier noch Handlungsbedarf bei der Erstellung von vorzugsweise international anerkannten Standards und Normen.

9.6 Ausblick

Nachdem mehrere Ausschüsse Änderungswünsche zum Verordnungsentwurf des Cybersecurity Acts eingereicht haben, wird das Europäische Parlament seine Position formulieren und voraussichtlich im Herbst 2018 die Trilog-Verhandlungen zwischen der Europäischen Kommission, dem Europäischen Rat und dem Europäischen Parlament beginnen (European Parliament Research Service Blog 2018). Der Vermerk vom Rat der Europäischen Union vom 29.05.2018 zur allgemeinen Ausrichtung des Verordnungsvorschlages des Cybersecurity Acts bezieht die Herstellererklärung neben der unabhängigen Prüfung durch Dritte als Möglichkeit der Konformitätsbewertung ein. Voraussetzung hierfür sei, dass die IKT-Prozesse, -Produkte- und -Dienste ein geringes Risiko darstellen und eine geringe Komplexität aufweisen und eine niedrige Vertrauenswürdigkeitsstufe aufweisen (Rat der Europäischen Union 2018).

In Bezug auf die Ausgestaltung eines europäischen Systems der Konformitätsbewertung im Bereich Cybersicherheit hat die Auswertung der Aussagen der Interessengruppen ergeben, dass das heutige Konformitätsbewertungssystem mit dem starken Fokus auf produktbasierte, statische Prüfung in der digitalen Transformation und insbesondere in Bezug auf Cybersicherheit einer Anpassung bedarf. Sehr dynamische Innovationszyklen mit sehr kurzen Markteinführungszeiten sowie die verstärkte Individualisierung durch Möglichkeiten der additiven Fertigungstechnologien verlangen nach einem Wandel der Systeme zur Konformitätsbewertung (Carl 2017). Die Nutzung großer Datenmengen (Big Data) sowie Techniken zur Modellierung und Simulation bieten beispielsweise Möglichkeiten für dynamische Zertifizierungen, wobei eine Überprüfung der Anforderungen auf Basis von Standards kontinuierlich und (teil)automatisiert erfolgen soll. Eine lebenszyklusorientierte Zertifizierung von IoT-Produkten würde ferner der Herausforderung begegnen, dass Produkte nach dem Inverkehrbringen möglichen Cyberangriffen ausgesetzt sind und ständigen Sicherheitswartungen (z. B. in Form von Softwareupdates) bedürfen, wozu es bereits erste Forschungs- und Entwicklungsaktivitäten für dynamische Zertifizierungen im Bereich Cloud-Dienstleistungen in Bezug auf Datensicherheit und Datenschutz gibt.