European Office

Cybersecurity: Integraler Bestandteil eines EU-Binnenmarktes

VDMA-Diskussionspapier zur Gestaltung eines europäischen Rahmens für Industrial Security

Registration number
in the register of representative bodies:
976536291-45

August 2017

Cybersecurity: Integraler Bestandteil eines EU-Binnenmarktes

1. Strategische Aufgabe für Industrie 4.0 und für Europa

Cybersecurity ist nicht nur für das „Internet of Things“, sondern auch für das „Industrial Internet of Things“, Industrie 4.0 und damit für den Maschinenbau ein essenzielles Querschnittsthema. Die mit der Digitalisierung der Industrie einhergehende Vernetzung schafft neue Möglichkeiten für mehr Produktivität, bessere Ressourceneffizienz und neue Geschäftsfelder. Es entstehen aber auch neue Risiken durch mehr Akteure, mehr Schnittstellen und immer mehr Datenaustausch. Digitale Abbilder von sensiblen Betriebsgeheimnissen und sicherheitsrelevanten Prozessdaten gelangen ins Netz und sind damit gefährdet.

Produktions- und Geschäftsprozesse können nur dann erfolgreich digitalisiert werden, wenn

- die Sicherheit (Safety) für Mensch und Umwelt,
- die Verfügbarkeit von Anlagen und Diensten,
- der Schutz von Know-how,
- die Integrität von Daten,
- die Transparenz der Datenübertragung und Datenverwendung
- Vertraulichkeit und
- die Erfüllung bestehender gesetzlicher und vertraglicher Verpflichtungen

gewährleistet sind. Cybersecurity trägt wesentlich zur Erfüllung dieser Ziele bei und ist damit eine strategische Aufgabe der Unternehmen unter Wahrung ihrer Geschäftsinteressen. Die Unternehmen des Maschinen- und Anlagenbaus haben bei der Digitalisierung der Industrie eine Doppelrolle: Als Betreiber von Anlagen digitalisieren sie ihre eigenen Produktions- und Geschäftsprozesse und als Technologieintegrator bieten sie ihren Kunden moderne vernetzte Maschinen und Anlagen an.

Auch die Politik wird durch Cybersecurity herausgefordert und muss einen geeigneten und wirksamen Rahmen bieten. Die Gestaltung des Rahmens muss ohne Frage unbedingt auf europäischer und internationaler Ebene erfolgen. Zu vermeiden ist ein Flickenteppich nationaler Einzelregelungen, wie er derzeit in Europa zu entstehen droht. Weder die Digitalisierung der Wertschöpfungsketten noch Netzattacken machen an Landesgrenzen halt. Vielmehr ist ein einheitlicher, harmonisierter Rahmen die Grundlage digitalen Wirtschaftens und dient dem Ausbau der Wettbewerbsfähigkeit europäischer Unternehmen.

2. Cybersecurity ist kontextabhängig

Cybersecurity ist kein Selbstzweck: Sie schützt Systeme und Infrastrukturen vor Angriffen und trägt so dazu bei, übergeordnete Ziele wie Safety (Schutz von Menschen und Umwelt), Datenschutz und Verfügbarkeit öffentlicher und privater Dienste zu erreichen. Dies hilft bei der Verringerung von Vernetzungsrisiken.

Im Kontext von Industrie 4.0 begleitet Cybersecurity die Digitalisierung und Vernetzung von Industrieunternehmen und dient hier in erster Linie privatwirtschaftlichen Zielen, wie z.B. der Aufrechterhaltung der Funktionalität, der Vertraulichkeit von Geschäftsinformationen, der Integrität und Verfügbarkeit von Anlagen und Funktionen. Der Schutz kann nicht absolut sein, sondern muss dem unternehmerischen Risiko entsprechend angemessen sein und ausreichende Freiräume für Innovationen und unternehmerische Entscheidungen lassen.

Cybersecurity ist nicht immer und überall gleich wichtig. Der gleiche Angriff auf die gleichen Komponenten kann je nach Umgebung unterschiedliche Folgen auslösen und wird auf unterschiedlich vorbereitete Nutzer treffen. Wichtig ist daher, bei der Gestaltung eines

Rahmens für Cybersecurity nach Risiken und Akteuren zu differenzieren. Aus Sicht des VDMA lassen sich grundsätzlich drei Bereiche unterscheiden:

B2C: Cybergefahren in Internet-of-Things-Massenmärkten

Viele Anwendungen von IoT-Geräten werden in einem B2C-Kontext stattfinden, in dem der Betreiber des Gerätes ein privater Endanwender ist. Dieser Bereich ist überwiegend durch die folgenden Eigenschaften gekennzeichnet:

- Die **Geräte** sind Gebrauchsgüter mit einer Lebensdauer von 3-10 Jahren (Smartphones, Router, Thermostate, Kühlschränke) im niedrigen bis mittleren Preissegment (im Vergleich zu Investitionsgütern), überwiegend hergestellt in großen Stückzahlen. Häufig fehlt ein Bildschirm als Nutzerzugang (z.B. bei IP-Kameras). Die Geräte benötigen für Ihre Basisfunktion nicht unbedingt eine kontinuierliche Netzwerkverbindung (z.B. Haushaltsgeräte).
- Die **Nutzer** haben überwiegen wenig Security-Expertise. Schutz von Know-how und Betriebskapital spielt eine eher geringe Rolle, Privacy und Vertraulichkeit hingegen eine große. Datenschutz ist gesetzlich durch die Datenschutzgrundverordnung (2016/679) und die geplante E-Privacy-Verordnung geregelt.
- **Verträge**: Einzelvertragliche Regelungen spielen keine Rolle. Verträge werden auf Basis von AGBs geschlossen.

B2B: Cybersecurity in digitalisierten Wertschöpfungsnetzwerken

Im „Industrial Internet of Things“ sind die Anwender erster Linie Unternehmen, die ihre Anlagen und Maschinen vernetzen:

- Bei den „Dingen“ handelt es sich um **kapitalintensive Investitionsgüter**, die eher in hoher Variantenvielfalt, kleineren Stückzahlen oder gar Einzel- oder Auftragsfertigung hergestellt werden. Die Nutzungsdauer ist eher lang und kann bis zu 30 Jahre betragen. Inverkehrbringen und Betrieb sind gesetzgeberischen Maßnahmen unterworfen. Prozesse und Prozessänderungen – und damit auch Retrofit und Updates- sind häufig stark formalisiert bzw. standardisiert ((z.B. nach EN ISO 9001, IEC 62443 und ISO/IEC 27001). Die Anwendungsfälle sind sehr uneinheitlich.
- Die **Nutzer sind Unternehmen** oder andere Organisationen. Die Security-Expertise variiert, ist aber grundsätzlich höher als bei privaten Endkunden. Der Schutz von Betriebskapital und Know-how sowie die Erfüllung gesetzlicher Auflagen spielen eine große Rolle.
- **Verträge** werden teilweise einzelvertraglich ausgehandelt. Damit können grundsätzlich auch Security-Anforderungen individuell formuliert werden. Im Übrigen werden Verträge auch im B2B-Bereich auf Basis von AGB geschlossen.

„B2Critis“: Cybersecurity zum Schutz kritischer Infrastrukturen

Dort, wo die Vernetzung von Anlagen, Maschinen und Komponenten kritische Infrastrukturen erreicht, bekommt Security eine besondere Bedeutung. Hier geht es um die Absicherung gesellschaftlicher und gesamtwirtschaftlicher Risiken. Die Betreiber dieser kritischen Infrastrukturen unterliegen den Auflagen der NIS-Richtlinie. Unternehmen, die als Lieferanten von Hard- oder Software für KRITIS-Organisationen auftreten, müssen entsprechend hohe Anforderungen erfüllen.

Diese drei grundsätzlichen Bereiche erfordern unterschiedliche Ansätze, um den Risiken und Gegebenheiten gerecht zu werden. Eine „One-size-fits-all“-Lösung ist nicht sachgerecht. In vielen Fällen würde sie auch nicht funktionieren.

Die Antworten auf die folgenden Fragen werden für die drei Bereiche B2C, B2B und B2Critis unterschiedlich ausfallen:

- Welche Aufgaben muss der Gesetzgeber übernehmen, welche können der Wirtschaft überlassen werden?
- Wieviel Schutz entsteht durch unternehmerisches Eigeninteresse (Verfügbarkeit, Schutz von Know-How, Vertraulichkeit, Datenintegrität)?
- Gibt es ausreichend geeignete Security-Produkte und -Dienste im Markt, die KMUs nutzen können, um ihre eigene Cybersecuritystrategie sicherzustellen und sie im Wettbewerb mit Großunternehmen zu unterstützen?
- Ergeben sich aus der Vernetzung im Rahmen von Industrie 4.0 oder den IoT Risiken für die Allgemeinheit, die über den bereits geregelten Schutz kritischer Infrastrukturen hinausgehen? (z.B. durch DDoS-Attacken über IP-Kameras oder Breitband-Router)?
- Gibt es Marktversagen bzw. übergeordnete gesellschaftliche Interessen, die politisches Handeln erfordern?
- Wie wird die Verantwortung zwischen den Herstellern von IoT-Komponenten, Maschinen, Anlagen und Systemen einerseits und Betreibern andererseits aufgeteilt?

3. Herausforderungen, Chancen und Stand der Dinge bei der Cybersecurity

Cybersecurity ist komplexer und weitreichender als bisherige Bereiche der Produktregulierung, die auf der Formulierung von Schutzzielen basieren. Während die Berücksichtigung von Security-Aspekten bis zur Inbetriebnahme bereits eine komplexe Aufgabe darstellt, ist die Gewährleistung der Security während der Nutzungsphase eine zusätzliche Herausforderung. Die existierenden gesetzlichen Regelungen zur Vermarktung von Produkten entfalten ihre Wirkung lediglich bis zum Inverkehrbringen, in Einzelfällen bis zur Inbetriebnahme.

Im Einzelnen sind es folgende Aspekte, die Cybersecurity zu einer besonderen Herausforderung werden lassen:

- Cybersecurity ist ein „Moving Target“ und abhängig vom Produktlebenszyklus: Vernetzte Geräte sind nach Inverkehrbringen einer sich stetig ändernden Gefahrenlage ausgesetzt. Neue Bedrohungen (z.B. durch neue Attacken, neue Angriffsmuster, bisher unentdeckte Schwachstellen, autonomisierte Angreifer) machen den Security-Stand des Produkts bei Auslieferung zum Teil irrelevant und erfordern ein ständiges Monitoring und Updating. Netzwerkfähige Geräte werden zudem in unterschiedliche Produkte (z.B. Maschinen und Anlagen) eingebaut. Sowohl diese IoT-Komponente als auch die Maschine oder Anlage werden möglicherweise im Laufe ihres Betriebes verändert. Beispielsweise kann eine neue Funktionalität per Software-Installation hinzukommen. Diese Software kann durch einen bisher unbeteiligten Dritten bereitgestellt werden.
- Die Verantwortung liegt bei mehreren Parteien: dem Hersteller der IoT-Komponente, dem Hersteller der Maschine, dem Integrator und dem Betreiber. Im Umfeld IoT und Industrie 4.0 verschwimmt die Grenze zwischen Produkt und Service. Damit kommen weitere Akteure (z.B. Servicedienstleister) ins Spiel.

- In Abhängigkeit vom Industriesektor können Maschinen und Systeme oft nicht zeitnah mit Updates versorgt werden. So sind Prozessanlagen teilweise Monate im Dauerbetrieb, da das Abschalten und Wiederhochfahren selbst bereits einen hohen Aufwand darstellt. Eine Verfügbarkeit stabiler Internetverbindungen kann zudem nicht als selbstverständlich angesehen werden.
- Anforderungen an die Security-Fähigkeiten von Produkten und Services sind von Umwelt, Standort, Kritikalität, Nutzungsdauer und nicht zuletzt vom Wert des Geschäftsprozesses abhängig.
- Die langen Lebenszyklen und hohen Investitionskosten von Industrieanlagen werden in vielen Fällen eine nachträgliche Vernetzung des Bestands erfordern.

Zusätzlich zu diesen digitalspezifischen Aspekten gibt es weitere Herausforderungen, die nicht spezifisch nur Cybersecurity betreffen, die aber berücksichtigt werden müssen:

- Produkte werden für einen bestimmten Einsatzzweck („intended use“) entwickelt. Diesem bestimmten Einsatzzweck liegen sowohl Risikobetrachtungen als auch Security-Fähigkeiten des Produkts zu Grunde. Geräte können so spezifisch für lokale Vernetzung oder den direkten Internetzugriff entwickelt werden. Anforderungen an die Cybersecurity von Produkten müssen diesem Umstand Rechnung tragen und die Notwendigkeit der bestimmungsgemäßen Verwendung aufnehmen.
- Cybersecurity kann nicht gemessen werden, wie z.B. ein Energieverbrauch. Es gibt keine zeitlich stabilen Grenzwerte für Fähigkeiten, die einen Vergleich oder Kennzahlen ermöglichen.
- Die Implementation der Cybersecurity bestimmt in hohem Maße die Schutzwirkung. Security ist immer Teil eines Geschäftsprozesses und muss technisch und organisatorisch sauber implementiert werden. Cybersecurity im industriellen Umfeld kann nicht durch einzelne Maßnahmen gewährleistet werden. Eine „silver bullet“, die EINE Maßnahme, gibt es nicht. Es bedarf eines dem jeweiligen Risiko angemessenen Schutzkonzeptes und dessen Absicherung.
- Das Security-Niveau von Gesamtsystemen ist nicht durch die Summe der Komponenten definiert. Vielmehr muss das Gesamtrisiko der Anlage beurteilt werden. Nicht nur das sichere Design von Komponenten ist wichtig, sondern auch die sichere Gestaltung der Gesamtanlage – des Schutzkonzeptes – und der Betriebsprozesse durch den Betreiber.

Auf der anderen Seite bietet ein industrielles B2B-Umfeld gute Chancen, Cybersecurity-Anforderungen zügig und auf angemessenem Niveau zu identifizieren und zu adressieren:

- Es gibt etablierte Prozesse und Erfahrungen in der Zusammenarbeit in Wertschöpfungsketten. Vertragsrechtlichen Lösungen erlauben grundsätzlich passgenaue Definitionen und Umsetzungen.
- Bestehende Industrie 4.0-Netzwerke helfen Unternehmen, ihre Expertise und ihre Fähigkeiten auszubauen. Dazu leisten Wirtschaftsverbände einen wichtigen Beitrag.
- Es gibt etablierte Standardisierungsprozesse auf europäischer und internationaler Ebene, auf die aufgebaut werden kann.

4. Schritte hin zu einem EU-Rahmen für Cybersecurity

Um die richtige Antwort auf diese Herausforderungen zu formulieren, sind zunächst die Anforderungen zu ermitteln, bevor gesetzgeberische Maßnahmen erwogen werden. Übereilt und kontraproduktiv wäre es, kurzfristig eine undifferenzierte breite Anwendung verpflichtender Anwendungen oder gar Drittzertifizierung vorzugeben. Dies würde bedeuten, das „Pferd von hinten aufzuzäumen".

Zertifizierung bedeutet, dass durch Prüfungen die Erfüllung von Anforderungen nachgewiesen wird. Solange jedoch die Anforderungen nicht klar definiert sind, bringen Zertifikate nicht die gewünschte Transparenz und Sicherheit. Da Zertifikate von Produkten nur eine Momentaufnahme zum Zeitpunkt des Inverkehrbringens sind und nicht dem „moving target" hinreichend Rechnung tragen können, kann Zertifizierung momentan keinen Beitrag zur Lösung leisten.

Wichtig ist vielmehr, die etablierten Abläufe zur Gestaltung regulatorischer Regimes als Wegweiser zu nehmen und den Weg hin zu einem EU-Rahmen in die folgenden drei Schritte zu unterteilen:

Schritt 1: Anwendungsbereich (Scope) und Zielgruppe identifizieren

Stand heute ist nicht klar erkennbar, an wen sich die europäischen Aktivitäten zur Cybersecurity richten - Betreiber kritischer Infrastrukturen, an die europäische Privatwirtschaft, an Diensteanbieter, IoT-Anbieter oder den ICT-Sektor - und welche Produkte oder Dienstleistungen in den Anwendungsbereich fallen. Die Begriffe „IoT" und IIoT müssen an dieser Stelle näher definiert und weiter differenziert werden.

Schritt 2: Security-Anforderungen definieren und mit den bestehenden Normen abgleichen

Höchste Priorität muss sein, zunächst die *Security-Anforderungen* an die zuvor festgelegte Zielgruppe zu identifizieren und zu definieren. Jedes eventuelle Konformitätsbewertungs-verfahren greift zur Erstellung von Prüfungskriterien auf definierte Anforderungen zurück, ebenso wie eine Herstellerselbsterklärung oder eine vertragliche Zusicherung. Inkohärente Anforderungen, durch Auditoren oder konformitätsbewertende Stellen selbst formulierte oder gar entgegenstehende nationale Anforderungen führen zu Interessenkonflikten, Verunsicherungen, Risiken und Intransparenz im Markt.

Die Anforderungen für die unterschiedlichen Anwendungsbereiche von digitalisierten Produkten sollten von neutralen Instanzen definiert werden. Dies kann mit Unterstützung von Normungsorganisationen oder Standardisierungsplattformen oder in einigen Fällen auch durch den Gesetzgeber geschehen. Es kann auch Bereiche geben, in denen privatrechtliche vertragliche Regelungen zwischen den Vertragspartnern ausreichen. Anforderungen sollten technologieneutral formuliert werden, um einerseits die Innovation von Produkten und Dienstleistungen nicht zu behindern und andererseits der schnellen technologischen Entwicklung auf der „Angreiferseite" Rechnung zu tragen.

Die Anforderungen müssen in bestimmten Zeitabständen auf Aktualität überprüft werden. Die Definition von Anforderungen kann nur unter Einbindung von Anwendern und Anbietern erfolgen. Dafür bieten sich z.B. die Branchenverbände als geeignetes Netzwerk-instrumentarium an. Die in einem branchenspezifischen offenen Konsortium erarbeiteten Anforderungen müssen hiernach in einer konsensbasierten Norm mit betroffenen Interessensgruppen abgestimmt werden. Dies muss auf breit zugänglichen, von der Industrie organisierten Plattformen (CEN/CENELEC, DIN/DKE, OPC Foundation usw.), geschehen. Dabei ist wichtig, die Einbindung in die internationale Normung zu gewährleisten. Die Umsetzung der identifizierten Security-Anforderungen in internationalen Normen (ISO/IEC)

stärkt die europäische Industrie im Welthandel. Rein europäische Anforderungen hingegen führen zu einer Fragmentierung des Weltmarktes zulasten der europäischen Industrie.

Die Gründung weiterer Plattformen und intransparenter Konsortien, die Definitionen und Vorgaben rund um die Digitalisierung in der Investitionsgüterindustrie vornehmen, macht aus Sicht des VDMA keinen Sinn. Im Gegensatz zu neu zu etablierenden Plattformen sind in der Normung die anzuwendenden Prozesse und Verfahren bekannt und bewährt.

Nur so können die Risiken analysiert und eventuelle Lücken aufgezeigt werden. Auf diese Weise kann eine breite Unterstützung und Umsetzungsfähigkeit der Anforderungen an die Cybersecurity erreicht werden. Der VDMA hat als Anwendernetzwerk bereits Erfahrung in der Formulierung von Anforderungen an die Cybersecurity. So wurden in 2016 im VDMA Arbeitskreis „Industrial Security“ mit Unterstützung des Fraunhofer AISEC konkrete Handlungsempfehlungen für Industrie 4.0 Security formuliert.

Schritt 3: Dort, wo nötig, Konformitätsbewertungsverfahren auswählen

Falls der europäische Gesetzgeber Marktversagen feststellt und eine Intervention in Form einer gesetzlichen Regelung für erforderlich hält, muss der geeignete Regelungsansatz aus Sicht des VDMA nach dem *„New Legislative Framework“* definiert werden. Nachdem Anforderungen und damit auch das erforderliche Schutzniveau festgelegt worden sind, können Entscheidungen über das erforderliche Konformitätsbewertungsverfahren (inkl. Kennzeichnungen) getroffen werden. Im Beschluss 768/2008/EG sind alle relevanten Module zur Konformitätsbewertung beschrieben. Diese sollten auch im Bereich Security genutzt und, falls erforderlich, weiterentwickelt werden.

Der VDMA und seine Mitglieder sind fest davon überzeugt, dass dies den einzig gangbaren Weg zur Sicherstellung von Konsistenz und Kohärenz für einen europäischen Binnenmarkt darstellt.

Für die überwiegende Anzahl von Fällen im B2B-Bereich ist die Konformitätsbewertung basierend auf Modul A (Selbsterklärung) des Beschlusses 768/2008/EG ausreichend. Für den Bereich der kritischen Infrastrukturen ist die Anwendung eines anderen Moduls, wie Drittzertifizierung oder Baumusterprüfung, zu prüfen. Dieses Vorgehen setzt die oben beschriebene Prüfung auf eventuelle Normungslücken und das anschließende Erstellen der grundlegenden Anforderungen in einem branchenspezifischen offenen Konsortium voraus.

Bei der Entscheidungsfindung muss dabei immer im Blick bleiben, dass verpflichtende Drittprüfungen und damit Labels und Zertifizierungen immer einen Eingriff in die Privatautonomie darstellen. Gerade bei einem dynamischen Querschnittsthema mit hoher Innovationsrate wie Cybersecurity sollte die Politik hier sehr umsichtig agieren. Falls eine Kennzeichnung als notwendig erachtet wird, sollten die sich aus dem NLF ergebenden Optionen in Erwägung gezogen werden (z.B. die CE-Konformitätskennzeichnung).

Erster Ansatz: Transparenz der Fähigkeiten verbessern

Aus Sicht des VDMA liegt der Schlüssel zur Lösung des „Moving target“-Problems nicht in Versuchen, ein allgemeines Bewertungsschema in Bezug auf die Erfüllung der Anforderungen zu erstellen. Vielmehr sollte der Ansatz sein, auf mehr Transparenz in Bezug auf die Security-relevanten *Fähigkeiten* der zu vernetzenden Produkte und deren *bestimmungsgemäßen Verwendung* zu setzen.

Bereits jetzt müssen Anforderungen an die Cybersecurity von Anbietern und Herstellern in ihre Produkte und Dienstleistungen integriert werden. Dabei müssen Produkte und Dienstleistungen Anforderungen erfüllen, die je nach Branche, Rechtsraum, Lebensdauer und Kritikalität der Anwendung unterschiedlich sein können. Eine *transparente, vergleichbare*

und überprüfbare Darstellung der Fähigkeiten kann helfen, den Abgleich zwischen den Anforderungen und den Eigenschaften von Produkten und Dienstleistungen zu erleichtern.

Nur wenn der Betreiber die Geräte bestimmungsgemäß verwendet, kann in der Praxis ein Abgleich von Anforderungen und Fähigkeiten erfolgen. Auch hier bietet die Transparenz von Fähigkeiten und Produkteigenschaften zur Cybersecurity einen vielversprechenden Ansatz, die Eignung von Geräten für den jeweiligen Einsatzzweck sachbezogen sicherzustellen.

5. Zusammenfassung: 9 Prinzipien für die Gestaltung eines europäischen Rahmens für Cybersecurity

1. Der rechtliche Rahmen für Cybersecurity muss auf europäischer Ebene gestaltet werden und ein Teil des Binnenmarkts sein. Ein Flickenteppich aus nationalen Regelungen würde die Unternehmen mit einer Vielzahl von Regelungen belasten und Europa im internationalen Digitalisierungswettbewerb zurückwerfen.
2. Cybersecurity als „Moving target“ erfordert, dass einerseits jeder Hersteller in der Wertschöpfungskette die Verantwortung für sein finales Produkt übernimmt – vom Hersteller der Komponente über den Maschinenbauer bis hin zum Systemintegrator. Andererseits muss der Betreiber die bestimmungsgemäße Verwendung der Systeme und die Beachtung von Security-Aspekten in seinem Verantwortungsbereich gewährleisten. Ziel eines Rahmens für Cybersecurity muss sein, die Teilung von Verantwortlichkeiten zwischen Hersteller und Betreiber wirksam, praxisgerecht und nachhaltig zu gestalten.
3. Priorität muss die Definition technologieneutraler Security-Anforderungen sein. Diese Definition ist die Basis für alle weiteren Schritte. Diese Anforderungen für die unterschiedlichen Anwendungsbereiche von digitalisierten Produkten können von neutralen Instanzen definiert werden. Dies kann mit Unterstützung von Normungsorganisationen oder Standardisierungsplattformen oder in einigen Fällen auch durch den Gesetzgeber geschehen. In vielen Fällen reichen möglicherweise auch vertragliche Regelungen zwischen den Vertragspartnern aus. Prinzipien wie „Security by design“ und „Security by default“ müssen dabei Anwendung finden.
4. Fehlende Normen und Standards für die Definition von branchenspezifischen Cybersecurity-Anforderungen müssen durch die Wirtschaftsakteure auf etablierten, offenen, wirtschaftsgetragenen Normungs- und Standardisierungsplattformen erarbeitet werden.
5. Es darf keine undifferenzierten und voreilig eingeführten verpflichtenden Anforderungen oder gar eine Drittzertifizierung bzw. Labelpflicht geben. Instrumente der Konformitätsbewertung können nicht angedacht werden, bevor die Basis in Form definierter Anforderungen erarbeitet ist. Zertifizierung erzeugt unnötige Kosten und schränkt zudem den Lösungsraum für Innovationen ein. Gerade dort, wo es bereits übergeordnete gesetzgeberische Ebenen und sektor- und kontextabhängige Auflagen gibt, würden Komplexität und Kosten exponentiell zunehmen.
6. Falls der europäische Gesetzgeber ein Marktversagen feststellt und eine gesetzliche Regelung für erforderlich hält, wäre der geeignete Regelungsansatz aus Sicht des VDMA, ein branchenübergreifendes Vorgehen nach dem *New Legislative Framework* zu definieren. Erst dadurch können Diskussionen über das geeignete Konformitätsbewertungsverfahren geführt werden. Aus Sicht des VDMA wäre dann für den überwiegenden Teil der Investitionsgüterindustrie das Modul A (Selbsterklärung) angemessen.
7. Bei der Prüfung der Handlungsnotwendigkeit sollte der Gesetzgeber beachten, dass Cybersecurity in die Geschäftsmodelle und Innovationsprozesse der Unternehmen eingebunden ist. Im Kontext Industrie 4.0 ist die Vorgabe eines technischen

Schutzniveaus extrem schwierig. Es gibt eine Vielzahl von möglichen Konstellationen und sich stetig wandelnden Situationen. Es muss daher sorgfältig geprüft werden, wo ein Eingriff durch Regulierung notwendig ist. Im B2B-Kontext sollte es so weit wie möglich den privaten Akteuren überlassen bleiben, welches Schutzniveau im Rahmen ihrer Geschäftspolitik und Branchenspezifika angestrebt wird. Eine Vorgabe des Schutzniveaus durch den Gesetzgeber ist nur bei hohen gesellschaftlichen Risiken für das Allgemeinwohl, z.B. bei kritischen Infrastrukturen oder zur Erfüllung übergeordneter Schutzziele, gerechtfertigt.

8. Wir empfehlen, in einem ersten Schritt die Verbesserung der Transparenz und Vergleichbarkeit von Security-relevanten Fähigkeiten der IoT-Produkte anzustreben. Dies ermöglicht die einfachere Gegenüberstellung von Anforderungen des Verwenders und den (durch den Hersteller erklärten) Fähigkeiten des Produktes. Die transparente Dokumentation der Produktfähigkeiten ermöglicht dem Verwender einen einfachen Abgleich mit allen Security-Anforderungen über den gesamten Nutzungszeitraum, von allgemein formulierten Basisanforderungen bis hin zu seinen geschäftsprozessspezifischen (evtl. anwendungsspezifischen) Regeln. Diese zeitstabile Aussage der Security-Fähigkeiten unterstützt explizit eine mögliche Dynamik der Security-Anforderungen, sowohl im Produktlebenszyklus als auch im Verwendungszeitraum. Ein Label ist grundsätzlich nicht in der Lage, diese Dynamik abzubilden. Beispiele für diese Fähigkeitsbeschreibungen durch den Hersteller können sein: Zeitraum, wie lange nach dem Inverkehrbringen des Produkts Security-Maßnahmen angeboten werden - "End Of Support (EOS)"; Dokumentation von Schnittstellen, Protokollen und offenen/versteckten Ports.
9. Auf Ebene der Politik sollten Erhöhung von Awareness und Aufbau von Expertise gefördert werden. Etablierte Partnerschaften und Allianzen spielen hierbei eine wichtige Rolle. Die cPPP im Bereich Cybersecurity ist sinnvoll, um Forschungsaktivitäten auf EU-Ebene zu bündeln und so den EU-Markt für Cybersecurity voranbringen. Sie darf aber nicht die bestehenden industriegetriebenen Plattformen und Prozesse ersetzen und kann nicht die Definition der Anforderungen im Namen der Anwenderindustrien vornehmen.

Kontakt:

Steffen Zimmermann
VDMA Competence Center Industrial Security
+49 69 6603-1978

Naemi Denz
VDMA Technik, Umwelt und Nachhaltigkeit
+49 69 6603 1226

Kai Peters
VDMA European Office
+322 7068219