European Office

Cybersecurity - Eine umfassende strategische Aufgabe für Europa

VDMA-Stellungnahme zum „Cybersecurity Certification Framework“ (COM(2017) 477 final - Verordnung „Cybersecurity Act“)

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

Februar 2018

1. Einleitung: Cybersecurity - Eine umfassende strategische Aufgabe für Europa

Cybersecurity ist nicht nur für das „Internet of Things“, sondern auch für Industrie 4.0 und damit für den Maschinenbau ein essenzielles sektorenübergreifendes Thema. 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 werden in Netzwerken eingebunden und sind damit gefährdet.

Als Anbieter von intelligenten Produktionssystemen und Technologieintegrator nimmt der Maschinen- und Anlagenbau eine zentrale Rolle für die Digitalisierung der Industrie ein. In den vernetzten Fabriken entstehen nicht nur physische Produkte, sondern auch eine Vielzahl an Daten. Diese Daten steuern und beschreiben die Produktions- und Geschäftsprozesse in den Unternehmen und Netzwerken. Gleichzeitig sind die Produktionsdaten auch der Beginn des digitalen Lebenszyklus eines vernetzen Produktes. Industrial Security ist daher auch für den Maschinenbau ein Kernthema.

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,
- eine sichere Infrastruktur zur Datenübertragung,
- Vertraulichkeit
- die Erfüllung bestehender gesetzlicher und vertraglicher Verpflichtungen
- und die Transparenz und Standardisierung von Schnittstellen

gewährleistet sind. Cybersecurity trägt wesentlich - wenn auch in unterschiedlicher Ausprägung - zur Erfüllung dieser Ziele bei und ist damit eine strategische Aufgabe der Unternehmen.

Cybersecurity ist kein Selbstzweck: Sie schützt Systeme und Infrastrukturen vor Angriffen und trägt so dazu bei, Schutzziele wie Safety (Schutz von Menschen und Umwelt), Datenschutz und Verfügbarkeit öffentlicher und privater Dienste zu erreichen. Dies hilft bei der Verringerung von Risiken, die bei der Vernetzung von Produktions- und Geschäftsprozessen entstehen können.

Unternehmen investieren bereits in Security im Rahmen der Wahrnehmung ihrer Geschäftsinteressen und Security-Aspekte werden mehr und mehr Bestandteil der Qualitätsanforderungen innerhalb der Wertschöpfungsketten. Es kann daher davon ausgegangen werden, dass Securityziele in einigen Fällen bereits über etablierte Marktmechanismen und privatrechtliche Regelungen erreicht werden. Dennoch gibt es Bereiche, in denen der europäische Gesetzgeber gefordert ist, das Erreichen wichtiger übergeordneter gesellschaftlicher Schutzziele sicherzustellen. Wichtig dabei ist aber, dass die Gesetzgebung Security nicht als isolierten Teilbereich oder ausschließlich dem IT-Sektor zugehörig betrachtet, sondern als Teil des europäischen Binnenmarkts und globaler Wertschöpfungsketten.

2. Einordung: Erster Schritt, aber zweiter Aufschlag notwendig

Europa ist gefordert, eine Binnenmarktinfrastruktur für Cybersecurity zu schaffen, die global anschlussfähig ist, die das Vertrauen innerhalb digitalisierter Wertschöpfungsketten stärkt und die gleichzeitig Innovation und Wettbewerbsfähigkeit nicht unangemessen einschränkt.

Der in Titel III des „Cybersecurity Acts“ beschriebene Zertifizierungsrahmen („Cybersecurity Certification Framework“) ist aber nur für einen Teilbereich der von Cybergefahren bedrohten Produkte, Systeme und Prozesse geeignet. Der Vorschlag der Kommission erfüllt eher die Merkmale eines freiwilligen Gütesiegels für die Erfüllung von Cyberanforderungen, wobei diese jedoch noch nicht klar definiert werden können. Der Maschinenbau sieht jedoch den Bedarf für eine horizontale Cybersecurityvorschrift, die die Vermarktung von ICT-Produkten erfasst und den Binnenmarkt auf diesen Regelungsaspekt ausdehnt. Insbesondere für industrielle Business-to-Business-Netzwerke wie den Maschinenbau passt der Rahmen nur in wenigen Einzelfällen – unter anderem, weil das im Vorschlag präferierte Instrument der Zertifizierung nur für eine geringe Zahl von Anwendungen eine wirksame Lösung sein kann.

Der Vorschlag verzichtet leider auf eine Nutzung der erprobten Binnenmarktinfrastruktur des „New Legislative Framework“ („NLF“). Es fehlen essenzielle Elemente wie das bewährte Zusammenspiel zwischen Vorgaben von grundlegenden Anforderungen durch den Gesetzgeber und Konkretisierung dieser Vorgaben durch die Normungsorganisationen, die Verbindung zur Marktüberwachung und die Regelungen zur Konformitätsbewertung. Aus Sicht des VDMA ist der „Cybersecurity Act“ daher nicht der abschließende große Wurf und ist nicht für einen breiten Einsatz in heterogenen, international vernetzten und dynamischen Wertschöpfungsketten im Sinne einer Industrie 4.0 geeignet.

Der Vorschlag der Kommission bietet aber die Chance, aufkommende und bereits existierende Fragmentierung durch nationale Zertifizierungssysteme in der EU zu vermeiden. Positiv ist, dass dieser Ansatz das in den Mitgliedsstaaten vorhandene Wissen nutzt und die Möglichkeit bietet, dort voranzugehen, wo es die Mitgliedsstaaten und die betroffenen Sektoren für notwendig erachten. Es gibt zwar Nachbesserungsbedarf hinsichtlich der Einbindung der Wirtschaft und der internationalen Anschlussfähigkeit. Werden diese Punkte aber im weiteren gesetzgebenden Prozess entsprechend präzisiert und ergänzt, kann der Zertifizierungsrahmen zumindest ein erster akzeptabler Schritt sein.

Aus Sicht des VDMA müssen aber grundsätzlich 2 Ansätze unterschieden werden:

- **Der Kommissionsvorschlag zum Cybersecurity-Act muss aus Sicht des Maschinenbaus nachgebessert werden, um die globale Anschlussfähigkeit sicherzustellen, die Transparenz zu gewährleisten und die Governance zu verbessern. Dies kann am besten durch eine Binnenmarktvorschrift nach den Prinzipien des New Legislative Framework („NLF“) erreicht werden, die vom Hersteller auf ICT-Produkte anzuwenden ist. Eine solche Vorschrift wäre eine eigenständige gesetzgeberische europäische Lösung für Cybersecurity in Form einer horizontalen Cybersecurityvorschrift („Phänomenrichtlinie“).**
- **Soll jedoch keine Binnenmarktvorschrift für die Cybersecurity von ICT-Produkten angestrebt werden, sind freiwillig anzuwendende „Certification Schemes“, die auf der Grundlage des Zertifizierungsrahmens erstellt wurde, ein möglicher Kompromiss. In diesem Fall muss der Hersteller entscheiden können, ob das zu vermarktende ICT-Produkte das so geregelte „Gütesiegel“ tragen soll oder nicht.**

3. Kernbotschaften und Empfehlungen zum „Cybersecurity Act“

Als Bestandteil eines umfassenden Pakets der EU-Kommission zu Cybersecurity (JOIN(2017) 450 final) zielt der im „Cybersecurity Act“ vorgeschlagene Zertifizierungsrahmen darauf ab, Fragmentierung durch Regelungen auf Mitgliedsstaatsebene zu vermeiden. Diese Zielsetzung ist vom Grundsatz her richtig und der VDMA unterstützt dies ebenso wie die gesamte strategische Initiative der EU-Kommission zu Cybersecurity. Der VDMA sieht es aber als notwendig an, an den folgenden Stellen nachzubessern und präziser zu formulieren:

Zertifizierung - vor allem die von Produkten - ist nur eingeschränkt geeignet, der Herausforderung „Security“ gerecht zu werden. Nicht nur Zertifikate, sondern alle zur Verfügung stehenden Instrumente zur Konformitätsbewertung müssen genutzt werden – z.B. die Herstellerselbsterklärung. Die Wahl der Instrumente muss angemessen sein und überzogene Bürokratie, Kosten und Innovationsbarrieren vermeiden.

Der Vorschlag zum „Cybersecurity Act“ sieht nur eine Drittzertifizierung vor. Durch die sich ständig ändernde Bedrohungslage („Moving target“) und die hohe Innovationsgeschwindigkeit in den betroffenen Sektoren wie IT und IoT und im Rahmen der Digitalisierung generell ist es aber grundsätzlich fraglich, ob diese Fokussierung auf Zertifizierung passend und wirksam ist.

Zertifizierungen sind für die Hersteller teuer und zeitraubend. Sie verlängern die Zeit bis zur Produkteinführung, erzeugen hohen Aufwand und wirken innovationshemmend. Gerade im Maschinen- und Anlagenbau sind zudem häufig kundenspezifische Lösungen erforderlich, die für jeden Einzelfall ein Zertifikat und damit unverhältnismäßig hohen Aufwand erfordern könnten. Neue Technologien erfordern auch oft neue Prüfgrundlagen, die nicht oder nur nach erheblicher Verzögerung verfügbar sind. Die Einführung neuer Technologie, auch für bestehende ICT-Produkte, wird so zusätzlich behindert. Es besteht die Gefahr, dass Zertifizierungen die gerade für die Security so wichtigen Updates und Innovationsschübe sogar behindern. Label und Zertifikate bieten in B2B-Branchen wie dem Maschinenbau grundsätzlich nur selten Nutzen und werden von den Unternehmen eher negativ bewertet, wie eine kürzlich veröffentlichte Studie der Impuls-Stiftung des VDMA belegt[1].

Statt pauschal die Zertifizierung zu favorisieren, muss das erfolgreiche Element der Konformitätsbewertung genutzt werden. Die existierenden Module zur Konformitätsbewertung (768/2008/EC) bieten eine Bandbreite an, die es wesentlich erleichtern würde, passgenaue und der Problematik angemessenere Bewertungsverfahren anzuwenden. So erscheint beispielsweise die Nutzung der Module mit Bezug zur internen Fertigungskontrolle und Qualitätssicherung geeignet (Modul A zur internen Fertigungskontrolle bzw. Modul Moduls H zur Bewertung der Fähigkeiten des Herstellers).

Governance verbessern: Zertifizierung muss von Wirtschaftsakteuren getrieben werden, nicht von Behörden. Durchführungsrechtsakte dürfen nur grundlegende Anforderungen definieren, die Formulierung der konkreten Schutzziele muss im Rahmen der europäischen und internationalen Normung erfolgen.

Der vorgeschlagene Zertifizierungsrahmen sieht vor, dass die Zertifikatsysteme fast ausschließlich von Behörden auf nationaler und europäischer Ebene gestaltet werden. Auch

[1] https://www.vdma.org/documents/105628/21813053/IMPULS-Studie_Labels-deutsch_1510043826190.pdf/01680e2d-458c-43f0-9ce1-d6d472e5b597

ist eine Vergabe der Zertifikate durch Behörden vorgesehen. Staatliche Zertifizierungssysteme und behördliche Vergabe von Zertifikaten sind aber nicht vereinbar mit Anforderungen auf internationalen Märkten. Für wirksame und international anschlussfähige Systeme ist es unverzichtbar, dass die Zertifizierung maßgeblich von den Wirtschaftsakteuren getrieben und gestaltet wird. Der Vorschlag muss an dieser Stelle erheblich nachgebessert und teilweise neu formuliert werden.

Wichtig ist vor allem, die Definition der grundsätzlichen Anforderungen und die Formulierung konkreter Schutzmaßnahmen der jeweils geeigneten Ebene zuzuordnen. Staatsentlastend und zielführend sind hierzu Regelungsansätze, die lediglich grundlegende gesetzliche Anforderungen formulieren und ansonsten auf die europäischen Normungssysteme verweisen. Durchführungsrechtsakte und Komitologie bieten zwar Mitgliedsstaaten ein Mitbestimmungsrecht und somit die Chance, das bestehende Knowhow und die Fortschritte auf nationaler Ebene zu nutzen. Sie können aber nicht die Anforderungen der Wirtschaftsakteure und der internationalen Märkte abbilden.

Der VDMA schlägt daher vor, dass die vorgesehenen Durchführungsrechtsakte sich lediglich auf die Definition grundlegender Security-Anforderungen für den jeweiligen Anwendungsfall bzw. Produktkategorie eines „Schemes“ beschränken. Artikel 45 sollte dementsprechend überarbeitet werden. Die Liste von Cybersecurity-Anforderungen in der vorliegenden Form ist unvollständig und nicht flexibel genug, um auf neue Herausforderungen reagieren zu können (die Liste ist offenbar ein Sub-Set der Anforderungen aus der ISO/IEC 27001).

Nach Erteilung eines Normungsmandats muss dann die Formulierung konkreter Schutzmaßnahmen und des Stands der Technik durch die europäische Normung und vorzugsweise in Kooperation mit der internationalen Normung erfolgen. Durch die Nutzung solcher Normen oder Standards werden wirksame und innovative Lösungen für die Erreichung der Security-Schutzziele erschlossen und es wird verhindert, dass die europäische Wirtschaft von internationalen Entwicklungen abgeschnitten wird.

Beschreibung der Sicherheitslevel in Art. 46 überprüfen

Artikel 46 schlägt drei unterschiedliche „Assurance Level“ vor. Dies sollte grundsätzlich überdacht und korrigiert werden, da solch unterschiedliche Level am Markt eher verwirren als Klarheit schaffen: Ein hoher „Assurance Level“ kann zu der Einschätzung verleiten, dass er absolute Sicherheit garantiere, was nicht der Fall ist. Ein niedrigerer Level dürfte hingegen immer als “minderwertig” angesehen werden. Beispielsweise ist es fraglich, ob ein Zertifikat für ein „Assurance Level basic“ mit der Beschreibung „limited degree of confidence“ zur Erhöhung von Vertrauen beiträgt.

Ein künftiges Konformitätsbewertungsverfahren sollte sich vielmehr auf klare gesetzgeberische Anforderungen stützen. Der VDMA hält die Einführung unterschiedlicher Level in dieser Form nicht für notwendig.

Grundsätze guter Rechtssetzung anwenden, „Checks and Balances“ verankern, Transparenz sicherstellen

Obwohl freiwillig, sollen die angestrebten Systeme Vertrauen erzeugen und breite Akzeptanz finden. Dazu ist es unverzichtbar, dass die Verhältnismäßigkeit gewahrt bleibt und die Notwendigkeit bzw. Eignung eines Zertifikatsystems sorgfältig geprüft wird, bevor es zu einer Einführung kommt. Es ist daher unverzichtbar, den Prozess transparent zu gestalten und mit einem effektiven System der „Checks and Balances“ zu versehen. Art. 44 muss daher um die folgenden Elemente ergänzt werden:

- Die sorgfältige Prüfung der Notwendigkeit und Eignung eines Zertifikatsystems muss im Ablauf verankert werden und einem entsprechenden Prüfraster folgen. Die bereits erwähnte Studie der Impuls-Stiftung des VDMA zur Nutzung von Labels beschreibt ein solches Schema.
- Die regelmäßige Veröffentlichung eines Arbeitsplans, um für die Öffentlichkeit und alle interessierten Kreise nachvollziehbar und transparent darzustellen, in welchen Bereichen Zertifikate als Nächstes entwickelt werden sollen.
- Die Verankerung eines Kataloges von Qualitätskriterien guter Gesetzgebung in Art. 47 (2): bestimmte Grundprinzipien müssen bei der Entwicklung eines neuen Zertifikats berücksichtigt werden, damit keine ungewünschten Auswirkungen in Bezug auf den Wettbewerb, bestehende Gesetzgebung oder den Endkunden entstehen. Zu diesen Grundprinzipien gehören z.B. Technologieneutralität, Verhältnismäßigkeit, Schutz der Wettbewerbsfähigkeit der regulierten Branche und die Vermeidung von Doppelregulierung.

4. Zusammenfassung und Fazit:

Aus Sicht des VDMA ist der vorgeschlagene Zertifizierungsrahmen für eine wirksame Erhöhung der Cybersecurity in industriellen Wertschöpfungsketten und damit auch für den Maschinenbau weitgehend nicht geeignet, da er nur auf die eingeschränkt wirksame Zertifizierung abzielt und keine umfassende horizontale Binnenmarktlösung anstrebt.

Ideal wäre aus Sicht des VDMA eine eigenständige Binnenmarktvorschrift für Cybersecurity nach den Prinzipien des New Legislative Framework („NLF“). Eine solche Vorschrift für Cybersecurity bietet als innovationsfreundliche und flexible gesetzliche Regelung nicht nur den Wirtschaftsakteuren die notwendige Flexibilität und Freiräume für Innovationen, sondern entlastet auch Mitgliedsstaaten, Kommission und ENISA durch den Wegfall von ständigen Aktivitäten zur Erstellung der erforderlichen „Certification Schemes“.

Der Vorschlag zum „Cybersecurity Act“ kann aber ein erster akzeptabler Schritt sein, wenn es gelingt, im weiteren Gesetzgebungsprozess nachzubessern und insbesondere die rein behördliche Gestaltung der Zertifikatssysteme zu korrigieren. Zertifizierung - wenn sie denn als notwendig erachtet wird - muss von den Wirtschaftsakteuren vorangetrieben und konkrete Schutzziele und -maßnahmen müssen im Rahmen der Normung erarbeitet werden.

Kontakt:

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

Kai Peters
VDMA European Office
+322 7068219

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