VDMA-Positionspapier

Technik, Umwelt und Nachhaltigkeit

Cybersecurity – eine Voraussetzung für Digitalisierung

Cybersecurity ist nicht nur für das „Internet of Things“, sondern auch für Industrie 4.0 ein essenzielles und sektorenübergreifendes Thema. Die mit der Digitalisierung der Industrie einhergehende Vernetzung ermöglicht mehr Produktivität, höhere Ressourceneffizienz und neue Geschäftsfelder. Es entstehen aber auch neue Risiken durch immer mehr Akteure, Schnittstellen, Datenaustausch und Cyberattacken. Die Akteure sind insbesondere durch Cyberattacken mit Risiken konfrontiert, die sie nicht immer ausreichend abschätzen können, die eine steigende sowie wechselnde Bedrohung darstellen können und die auch außerhalb ihres Einflussbereiches liegen. Bereits heute ist der Maschinenbau mit Risiken aus dem Bereich Cybersecurity konfrontiert, wenn Kunden für Maschinen oder Anlagen einen Fernzugriff fordern, wenn z.B. die Unterstützung des Herstellers für die Störungsbeseitigung oder Wartungstätigkeiten gewünscht ist.

Die Forderungen des VDMA zielen auf die Schaffung einer Infrastruktur rechtlicher Art ab, damit die Digitalisierung im Maschinenbau zügig weiter vorangetrieben werden kann. Hersteller und Betreiber haben eine wichtige Verantwortung, die Widerstandsfähigkeit der Maschinen, Anlagen, Systeme und Komponenten zu realisieren, aber auch im Betrieb zu erhalten. Cybersecurity ist ein „moving target“, das von allen Akteuren ein spürbares Engagement zur Cybersecurity abverlangt. Zur Schaffung und zum Erhalt der erforderlichen Cybersecurity sind die Akteure auf unterschiedliche Weise gefordert. Daher verfolgt der VDMA die Strategie, dass gesetzliche Regelungen die Widerstandsfähigkeit eines Produktes zum Zeitpunkt des Inverkehrbringens erfassen, aber auch Bestimmungen zum Erhalt der Widerstandsfähigkeit nach der Inbetriebnahme, also betriebsbegleitend, enthalten.

Rolle der Akteure

Der Hersteller hat die Verantwortung, seine Produkte, ob verwendungsfertig oder nur zum Einbau vorgesehen, mit einer Widerstandsfähigkeit auszustatten, die eine sinnvolle Nutzung in der Praxis erlaubt. Die Randbedingungen für die Nutzung legt der Hersteller im Rahmen der bestimmungsgemäßen Verwendung fest. Produkte, die zum Einbau vorgesehen sind, müssen eine Widerstandsfähigkeit aufweisen, die ihrer Konzeption und Einbausituation entsprechen. Der Betreiber hat die Verantwortung Informationen zur Widerstandsfähigkeit und Maßnahmen zum Erhalt der Widerstandsfähigkeit des Herstellers bei der Verwendung zu berücksichtigen und seine Maßnahmen auf dieser Grundlage zu treffen. Durch diese gemeinsamen Anstrengungen kann die erforderliche Widerstandsfähigkeit einer Maschine, einer Anlage oder eines Systems realisiert und aufrechterhalten werden. Jeder Akteur hat seine Verantwortung wahrzunehmen und auch den nächsten Akteur in der Kette mit den erforderlichen Informationen und Maßnahmen zu versorgen.

VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main, Germany
Telefon +49 69 6603-1907
E-Mail tu@vdma.org
Internet www.vdma.org
Vereinsregister AG Frankfurt/Main, Nr. VR4278

Technik, Umwelt und Nachhaltigkeit
Abteilungsleiterin:
Naemi Denz

Präsident:
Carl Martin Welcker
Hauptgeschäftsführer:
Thilo Brodtmann

Gesellschaft und Wirtschaft fordern bessere Cybersecurity
Produktions- und Geschäftsprozesse können daher nur dann erfolgreich digitalisiert werden, wenn grundlegende Security-Schutzziele erfüllt werden. Cybersecurity ist daher ein strategischer Baustein für die Wettbewerbsfähigkeit europäischer Unternehmen. Zwar investieren Unternehmen bereits in Security zur Wahrnehmung ihrer Geschäftsinteressen und Security-Aspekte werden zu wichtigen Bestandteilen innerhalb der Wertschöpfungsketten. Dennoch ist der europäische Gesetzgeber gefordert, die für die Digitalisierung erforderlichen Rahmenbedingungen zu schaffen. Dazu sind die Definition von Schutzzielen für die Cybersecurity und gesetzliche Regelungen zu grundlegenden Anforderungen an die Widerstandsfähigkeit von vernetzbaren Produkten erforderlich.

Aktuelle Fälle von Cyberangriffen führen immer wieder zu öffentlichen Diskussionen und der Forderung, dass staatliche Maßnahmen zur Abwehr und Sanktionierung von Cyberangriffen und zur Schaffung und Förderung der Cybersecurity erforderlich sind und Cybersecurity als staatliche Schutzpflicht im Rahmen der Daseinsvorsorge verstanden wird.

Ist das Erreichte ausreichend?
Im Rahmen der „Digitalen Agenda“ und des „Digitalen Binnenmarkts“ ist Europa in Bezug auf ein harmonisiertes Regelwerk für die Digitalisierung ein gutes Stück vorangekommen, etwa durch die Regelungen zum Datenschutz, zu Plattformen oder zum grenzüberschreitenden Datenverkehr. Auch im Bereich Security wurden beispielsweise mit der NIS-Richtlinie und dem Cybersecurity Act wichtige Schritte getan. Die Erfolgsgeschichte „Europäischer Binnenmarkt“ mit seiner Vielzahl harmonisierter Rechtsvorschriften wird so um die digitalen Komponenten ergänzt und soll als „Binnenmarkt 4.0“ fortgeschrieben werden.

Trotz dieser grundsätzlich positiven Entwicklung ist der Binnenmarkt im Bereich Cybersecurity unvollständig. Während das Erreichen wichtiger Schutzziele beispielsweise im Bereich der Produktsicherheit einheitlich europäisch geregelt ist, fehlen erforderliche gesetzliche Regelungen für Cybersecurity. Vernetzung und Internetzugang ist heute eine Selbstverständlichkeit, daher ist Cybersecurity fester Bestandteil einer Daseinsfunktion. Lücken im Bereich der öffentlich-rechtlichen Regelungen in Europa treten deutlicher zu Tage denn je.

Die Maschinenforderungen zu Cybersecurity
Der Cybersecurity Act verspricht zwar Abhilfe, in dem er eine Harmonisierung der Zertifizierung anstrebt. Der VDMA stimmt vom Grundsatz mit der Zielsetzung überein, hält aber den bewährten Weg der Vorschriften nach dem New Legislative Framework für richtig. Daher fordert der VDMA eine Harmonisierungsrechtsvorschrift zur CE-Kennzeichnung in Form einer Richtlinie oder EU-Verordnung nach dem Prinzip des New Legislative Framework, um den Aspekt Cybersecurity von Produkten zu erfassen – also eine Binnenmarktvorschrift. Der Maschinenbau ist sehr stark exportorientiert und KMU-geprägt. Um für die Beschaffung von Maschinen und für deren Vermarktung ein „Level-Playing-Field“ zu schaffen, ist eine öffentlich-rechtliche Regelung zur Cybersecurity, namentlich zur Widerstandsfähigkeit der Produkte gegen Cyberangriffe erforderlich. Das gilt auch für Bauteile, die in Maschinen integriert werden und für Komponenten, die vernetzt der Datenkommunikation dienen. Jede Art dieser vernetzten Datenkommunikation sollte durch technologieneutrale Anforderungen erfasst werden. Eine solche Regelung muss aus Sicht des Maschinenbaus auch global anschlussfähig sein, da der Maschinenbau sehr stark exportorientiert ist und die Lieferketten global angelegt sind. Dabei spielt das bewährte Instrument der Normung eine bedeutende Rolle, um die grundlegenden Cybersecurity-Anforderungen zu konkretisieren, den Stand der Technik fortzuschreiben und eine Angleichung oder gar Harmonisierung technischer Anforderungen im globalen Umfeld zu erreichen. Damit wird nach Auffassung des VDMA das Vertrauen innerhalb der weltweiten digitalisierten Wertschöpfungsketten gestärkt und

Innovationen sowie Wettbewerbsfähigkeit unterstützt. Eine solche öffentlich-rechtliche Vorschrift zur Vermarktung von Produkten, die auch Pflichten für den Hersteller zu Informationen und Maßnahmen zum Erhalt der Widerstandsfähigkeit enthält, darf jedoch nicht zu einer Ausdehnung von haftungsrechtlichen Ansprüchen führen, insbesondere hinsichtlich Vermögensschäden. Ein Vorschlag zu gesetzlichen Bestimmungen dieser Art, sollte diesem wichtigen Aspekt unbedingt Rechnung tragen.

Widerstandsfähigkeit und Erhalt der Widerstandsfähigkeit
Im Mittelpunkt einer solchen Rechtsvorschrift stehen grundlegende Anforderungen an die Widerstandsfähigkeit der Produkte gegen Cyberangriffe. Auswirkungen und Schwere der Bedrohungen können stark variieren und zu einem bestimmten Zeitpunkt der Nutzungsphase größer sein als die Widerstandsfähigkeit des Produktes. Experten sprechen vom „Moving target“, um die sich ändernde Bedrohung durch Cyberangriffe zu beschreiben. Daher spielt der Erhalt der Widerstandsfähigkeit eines Produktes hinsichtlich Cyberangriffen die zentrale Rolle. Da der Hersteller das Produkt konzipiert und auch ein vitales Interesse an der Verwendungsfähigkeit des Produktes hat, kann er für den Erhalt der erforderlichen Widerstandsfähigkeit am besten sorgen und den Kunden betriebsbegleitende Unterstützung, z.B. in Form von Informationen zu entstandenen Lücken in der Widerstandsfähigkeit oder Updates bieten.

Eine betriebsbegleitende Unterstützung, die der Funktionserweiterung dient, sollte von dem vorgeschlagenen Rechtsakt ausdrücklich nicht erfasst werden. Der Hersteller sollte über die Dauer der betriebsbegleitenden Unterstützung oder des Datums, bis zu dem eine betriebsbegleitende Unterstützung gewährt werden kann, entscheiden können. Daher sollte eine Pflicht für den Hersteller bestehen, die Dauer dieser Unterstützung oder des Datums, bis zu dem die Unterstützung gewährt wird, zu nennen. Er sollte auch verpflichtet werden, dem Betreiber bzw. Verwender das vorzeitige Ende der Unterstützung anzukündigen, wenn die Widerstandsfähigkeit des Produktes aus technischen Gründen und der geänderten Bedrohungslage nicht mehr aufrechterhalten werden kann. Weiterhin sollte der Hersteller dem Betreiber bzw. Verwender auch die Gründe für die Beendigung der Unterstützung nennen. Die Festlegung von Kriterien, unter denen der Hersteller die Unterstützung vorzeitig beenden darf, ist derzeit schwierig. Sie ist jedoch ein Schlüsselelement für den fairen Wettbewerb.

Mit Blick auf den Umstand, dass sogenannte Schwachstellen durch Cyberangriffe von Dritten, also durch vorsätzlichen Missbrauch nach Inverkehrbringen der Produkte entstehen, darf eine Verpflichtung des Herstellers zu betriebsbegleitender Unterstützung nicht zu einer Erweiterung seiner Produkthaftung oder zu einer nachträglichen Qualifizierung des Produkts als nicht-konform im Sinne des öffentlichen (Inverkehrbringens-)Rechts führen.

Technologieneutrale grundlegende Anforderungen an die Cybersecurity
Die Erwartung an die Widerstandsfähigkeit eines Produktes orientiert sich am Stand der Technik und am Anwendungsfall und nicht an einer stetig wechselnden Bedrohungslage. Dieser Ansatz ermöglicht die Formulierung grundlegender Anforderungen an die erforderliche Widerstandsfähigkeit von Produkten – ganz gleich, ob verwendungsfertig oder für den Einbau in finale Produkte vorgesehen. Diese grundlegenden Anforderungen müssen daher technologieneutral formuliert werden, damit Hersteller die freie Wahl der Mittel haben, um diese Anforderung nach dem Stand der Technik zu erfüllen. Bei den Vorschriften zur CE-Kennzeichnung, die nach den Grundsätzen des New Legislative Framework abgefasst sind, hat sich dieses Konzept seit vielen Jahren bewährt und der europäischen Wirtschaft wachstumsstimulierende und innovationsfördernde Rahmenbedingungen gegeben.

Bei der Produktsicherheit wird seit vielen Jahren auf die Erfüllung grundlegender Anforderungen abgestellt, die nach dem Stand der Technik vom Hersteller beim Produkt zu erfüllen sind. Kein Produkt kann Sicherheit im absoluten Sinne bieten. Daher müssen Hersteller auch die Restrisiken benennen, die nach der Anwendung des Standes der Technik für die gesetzlich erforderlichen Schutzmaßnahmen verbleiben. Dieses bewährte Konzept ist für den Bereich Cybersecurity prädestiniert. Durch Normen kann der Stand der Technik definiert und damit auch erheblich schneller fortgeschrieben werden, wie durch Regelungen in Vorschriften.

Rolle der Software und Verbesserungsbedarf
Nach Auffassung des Maschinenbaus sollte auch separat vermarktete Software, die relevant für die Widerstandsfähigkeit ist, vom Anwendungsbereich des vorgeschlagenen Rechtsakts erfasst werden, wenn sie bei vernetzten Produkten zur Datenkommunikation eine bestimmte Rolle spielt und sehr oft das Ziel von Cyberattacken ist, indem Schwachstellen genutzt werden können, die die Widerstandsfähigkeit betreffen. Nach der Wahrnehmung vieler Anwender aus dem Maschinenbau sind im Bereich der Software noch große Verbesserungspotentiale vorhanden. Eine grundsätzliche Debatte zur Erweiterung des Produktbegriffs um den Bereich Software muss nach Meinung des VDMA dazu nicht geführt werden. Software, die in Produkte integriert oder eingebettet ist, wird ohnehin vom Produktbegriff erfasst.

Keine Erweiterung bestehender Vorschriften zur CE-Kennzeichnung
Bestehende Vorschriften zur CE-Kennzeichnung sollten nicht einfach um Cyberanforderungen oder um Anforderungen zur Widerstandsfähigkeit gegen Cyberangriffe erweitert werden. Zwei gewichtige Gründe sprechen eindeutig gegen diese verlockende und vermeintlich schnelle sowie smarte Lösung:

- Die betriebsbegleitende Unterstützung des Herstellers zum Erhalt der Widerstandsfähigkeit des Produktes gegen Cyberangriffe kann mit den bestehenden Vorschriften nicht abgebildet werden, da sie lediglich das Inverkehrbringen und die Inbetriebnahme erfassen. Die zum Erhalt der Widerstandsfähigkeit wichtigen Phase der Verwendung wird nicht erfasst.
- Würden bestehende Vorschriften zur CE-Kennzeichnung um Cyberanforderungen oder um Anforderungen zur Widerstandsfähigkeit gegen Cyberangriffe erweitert werden, käme es unweigerlich zu einer Fragmentierung dieser Anforderungen. Da die Vorschriften zu unterschiedlichen Zeitpunkten überarbeitet werden würden, wären Änderungen der Cybersecurity-Anforderungen unausweichlich. Auch Bemühungen, solche Anforderungen in einem Beschluss der Kommission als Musterbestimmungen zu fixieren, würde die Gefahr der Fragmentierung nicht beseitigen.

Da Hersteller auf ein Produkt oft mehr als zwei Vorschriften zur CE-Kennzeichnung anwenden müssen, hätte die Fragmentierung der Cybersecurity-Anforderung für die Umsetzung in der Praxis verheerende Folgen.

Anwendungsbereich einer Vorschrift zur Cybersecurity
Der Rechtsakt soll alle Produkte, die vernetzt kommunizieren, erfassen und deren Widerstandsfähigkeit bei einem Cyberangriff relevant ist. Dabei sollte jede Art der vernetzten Datenkommunikation erfasst werden, unabhängig davon, welche Technologie genutzt wird. Neben verwendungsfertigen Produkten sollten auch Komponenten erfasst werden, die in finale Produkte, wie Maschinen, eingebaut werden. Maschinenhersteller müssen sich auf die Widerstandsfähigkeit der Komponenten verlassen können, da ihre Kunden sich auch auf die Widerstandsfähigkeit des finalen Produktes, wie die einer Maschine, verlassen können müssen.

Bestimmte Produkte sollten aus dem Anwendungsbereich des Rechtsakts ausgenommen werden. Dabei können die folgenden Merkmale genutzt werden:

- Produkte, die vom Hersteller nicht für die direkte oder indirekte Kommunikation über das Internet vorgesehen sind und
- vernünftigerweise auch nicht für die Kommunikation über das Internet genutzt werden und
- zum Einbau vorgesehen und noch nicht verwendungsfertig sind und
- die durch zusätzliche Maßnahmen im finalen Produkt vor Cyberangriffen geschützt werden und
- bei denen der Hersteller klare Informationen über die fehlende Widerstandsfähigkeit mit dem Produkt bereitstellt (Betriebsanleitung) und
- das Produkt aufgrund seiner Konzeption und Architektur nicht geeignet ist, um es mit hinreichenden Maßnahmen für die Widerstandsfähigkeit gegen Cyberangriffe auszurüsten.

Die Ausnahme von Produkten aus dem Anwendungsbereich der vorgeschlagenen Rechtsvorschrift hat technische Gründe, die aufgrund der Konzeption des Produktes oder der seiner Anwendung bestehen. Sie liegen also nicht in der Wahlfreiheit des Herstellers. Als Übergangsfrist für den vorgeschlagenen Rechtsakt zur Cybersecurity werden 5 bis 6 Jahre einschließlich der Erarbeitung veranschlagt.

Welche Pflichten sollen Betreiber und Anwender erfüllen?

Vorschrift, die an den professionellen Verwender bzw. Betreiber, wie den Betreiber in seiner Rolle als Arbeitgeber gerichtet ist. Cybersecurity ist eine laufende Aufgabe, die sich nicht eben nur auf die betriebsbegleitende Unterstützung des Herstellers beschränken kann. Verantwortung für die Cybersicherheit tragen auch Betreiber und Anwender: Sie spielen bei der Aufrechterhaltung der Widerstandsfähigkeit eines Produktes, wie eines Arbeitsmittels, ebenfalls eine wichtige Rolle. Betreiber und Anwender setzen Maßnahmen aufgrund von Herstellerinformationen und Maßnahmen zum Erhalt der Widerstandsfähigkeit, die der Hersteller des Arbeitsmittels zur Verfügung stellt, zu einem Zeitpunkt ihrer Wahl um, damit die Widerstandsfähigkeit ihrer „Anwendung“ erhalten bleiben kann. Bei der Umsetzung können dadurch betriebliche Belange berücksichtigt werden.

Diese Pflichten können aber nicht Gegenstand einer Vorschrift zur Vermarktung von Produkten sein. Solche Pflichten können z.B. durch eine an den Arbeitgeber adressierte Vorschrift wirksam an den Betreiber oder Anwender in seiner Rolle als Arbeitgeber gerichtet werden. So gibt es bereits Vorschriften zur Verwendung von Arbeitsmitteln. Betreiberpflichten zum Erhalt der Widerstandsfähigkeit von Cybersecurity von Arbeitsmitteln können dort aufgenommen werden. Für kritische Infrastrukturen gibt es Vorschriften zum Erhalt der Widerstandsfähigkeit entsprechender Anlagen. Eine EU-weite einheitliche Lösung wird bevorzugt, da viele Betreiber mehrere Standorte in der Europäischen Union unterhalten und daher einheitliche Pflichten von Vorteil sind.

Ergänzung bestehender Instrumente, wie der Cyber Security Act

Die vorgeschlagene gesetzliche Regelung steht nicht im Widerspruch zum Cyber Security Act, sondern stellt eine horizontal wirkende Ergänzung dar. Durch die Konzeption einer horizontalen Vorschrift mit grundlegenden Anforderungen und der Anwendung langjährig bewährter Rechtsetzungsprinzipien des New Legislative Frameworks werden Ziele erreicht, die durch den Cyber Security Act nicht erreicht werden können, insbesondere die Aus-

dehnung des Binnenmarktes auf Digitalprodukte. Die Kohärenz mit dem Cyber Security Act für Produkt-Zertifizierungs-Schemes wird durch folgende weitere Aspekte gewährleistet:

- Grundsätzlich freiwillige Anwendung des Cyber-Acts, während der NLF-Rechtsakt verpflichtend in der Anwendung sein sollte
- Fokussierung des Cyber Security Acts auf kritikale Prioritäten wie etwa heutige kritische Infrastrukturen, SOGIS
- Schwerpunkt des Cyber Security Act sind Regelungen für die europäische Cyber-Behörde ENISA und weitere Aspekte der EU-Cyberinfrastruktur

VDMA-Forderungen:
Eine horizontale Cybersecurity-Rechtsvorschrift für vernetzbare Produkte würde nicht nur eine deutliche Lücke des digitalen Binnenmarkts schließen, sondern auch eine Reihe von praktischen Herausforderungen rund um Cybersecurity bei B2B-Produkten lösen. Folgende Bereiche werden durch die Maschinenbauforderungen wirksam erfasst:

I. Klare Definition der Verantwortlichkeiten der Wirtschaftsakteure, wie Softwarehersteller, Hersteller von Komponenten und gebrauchsfertigen Produkten, Betreiber
II. Festlegung von grundlegenden Anforderungen an die Widerstandsfähigkeit hinsichtlich der Cybersicherheit von Produkten in einer horizontalen Vorschrift
III. Aufrechterhaltung dieser Widerstandsfähigkeit von Produkten durch betriebsbegleitende Unterstützung des Herstellers
IV. Transparenz für Betreiber und Hersteller durch einheitliche Verpflichtung zur Information über die Cybersicherheit von Produkten und der Dauer betriebsbegleitender Unterstützung
V. Eignung für einen breiten Einsatz in heterogenen, international vernetzten und dynamischen Wertschöpfungsketten im Sinne einer Industrie 4.0
VI. Breite Akzeptanz und schnelles Roll-out durch Nutzung des in der Praxis bewährten Instrumentariums des New Legislative Framework
VII. Innovationsfreundliche und flexible gesetzliche Regelung, die den Wirtschaftsakteuren die notwendige Flexibilität und Schnelligkeit, aber auch Freiräume für Innovationen bietet
VIII. Entlastung von Mitgliedsstaaten, Kommission und ENISA durch den Wegfall ständiger Aktivitäten bei Einzelregelungen
IX. Schaffung einer wirksamen gesetzlichen Grundlage für Marktüberwachung und eines „Level-Playing-Fields“
X. Erhalt der Wettbewerbsfähigkeit für den Mittelstand und KMUs im Bereich der Cybersecurity durch klare und transparente öffentlich-rechtliche Regelungen

Kontakte im VDMA:
Naemi Denz
VDMA Technik, Umwelt und Nachhaltigkeit
+49 69 6603 1226
E-Mail naemi.denz@vdma.org

Thomas Kraus
VDMA Technik, Umwelt und Nachhaltigkeit
+49 69 6603 1602
E-Mail thomas.kraus@vdma.org

Kai Peters
VDMA European Office
+322 7068219

E-Mail kai.peters@vdma.org

15. Juli 2019