VDMA-Positionspapier

Technik, Umwelt und Nachhaltigkeit

Cybersecurity – Betreiber- und Arbeitgeberpflichten im Sinne gemeinsamer Anstrengungen

Cybersecurity ist für den Maschinenbau von hoher Bedeutung, daher hat der VDMA mit dem Positionspapier „Cybersecurity – eine Voraussetzung für Digitalisierung“ vom 15. Juli 2019 klare politische Forderungen zu erforderlichen gesetzlichen Bestimmungen für die Vermarktung von Produkten kommuniziert. Dieser vom VDMA geforderte Rechtsakt soll den Prinzipien des New Legislative Framework folgen. Die darin geforderten öffentlich-rechtlichen Bestimmungen sollen die Bedingungen für das Inverkehrbringen von vernetzten oder zur Vernetzung bestimmten Produkten regeln und gleichzeitig Herstellerpflichten enthalten, mit denen die betriebsbegleitende Unterstützung zum Erhalt dieser Widerstandsfähigkeit eine gesetzliche Grundlage erhält.

Cybersecurity ist ein „moving target“, das von allen Akteuren ein spürbares Engagement abverlangt. Zur Schaffung und zum Erhalt der erforderlichen Cybersecurity sind die Akteure auf unterschiedliche Weise gefordert. Daher verfolgt der VDMA die Strategie, dass einerseits gesetzliche Regelungen die Widerstandsfähigkeit eines Produktes zum Zeitpunkt des Inverkehrbringens erfassen. Ergänzend dazu soll nach den Bestimmungen eines weiteren Rechtsaktes die Widerstandsfähigkeit nach der Inbetriebnahme aufrechterhalten werden. Dieses Aufrechterhalten der Widerstandsfähigkeit erfolgt betriebsbegleitend.

Für die Arbeitssicherheit spielt der Erhalt der Cybersicherheit eine wichtige Rolle. Dieses VDMA-Positionspapier zu den Betreiber- und Arbeitgeberpflichten geht auf die Pflichten zum cybersicheren Betrieb von Produkten und Arbeitsmitteln ein, damit Cybersecurity im Sinne von gemeinsamen Anstrengungen erreicht werden kann und so einen wichtigen Beitrag zur Arbeitssicherheit geleistet werden kann. Mit der VDMA-Forderung nach einem zweiten, an Betreiber und Arbeitgeber gerichteten, Rechtsakt soll das bewährte Prinzip der Trennung von Beschaffenheits- und Betriebsanforderungen weitergeführt und auf den Bereich der Cybersecurity ausgedehnt werden. Da maschinenbaurelevante Betriebsanforderungen auf europäischer Ebene mehrheitlich an den Arbeitgeber gerichtet sind, konzentriert sich dieses Papier auf diesen Bereich. Gleichwohl können die Forderungen dieses VDMA-Positionspapiers analog auch auf die Rolle des Betreibers übertragen werden. Daher wird im Folgenden der Arbeitgeber genannt.

Für den cybersicheren Betrieb von Produkten und Arbeitsmitteln wird u.a. vorausgesetzt, dass Arbeitgeber Informationen des Herstellers der eingesetzten Produkte genau beachten.

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:
Dr. Sarah Brückner

Präsident:
Carl Martin Welcker
Hauptgeschäftsführer:
Thilo Brodtmann

Das gilt insbesondere für die bestimmungsgemäße Verwendung, die jeweils vom Hersteller festgelegt wird, als auch für andere Informationen, die bestimmte Lebensphasen des verwendeten Produktes betreffen, wie Wartung, Instandsetzung oder Reparaturen, sofern sie nicht vom Hersteller durchzuführen sind. Es wird auch davon ausgegangen, dass Arbeitgeber die Verantwortung für die Verwendung eines Produktes übernehmen, die außerhalb der bestimmungsgemäßen Verwendung liegt oder die vom Hersteller nicht vernünftigerweise angenommen werden kann.

Die Forderungen des VDMA nach einem Rechtsakt zur Vermarktung von cyberrelevanten Produkten und einem zweiten Rechtsakt, der an Arbeitgeber gerichtet ist, zielen auf die Schaffung einer Infrastruktur rechtlicher Art ab, damit die Digitalisierung im Maschinenbau zügig weiter vorangetrieben werden kann. Arbeitgeber und Hersteller haben eine wichtige Verantwortung, die Widerstandsfähigkeit der Maschinen, Anlagen, Systeme und Komponenten zu realisieren, aber auch im Betrieb zu erhalten. Arbeitgeber haben auf der Grundlage dieses geforderten Rechtsakts auch die Verantwortung, alle erforderlichen Maßnahmen zu treffen, um Produkte und Arbeitsmittel cybersicher verwenden zu können. Diese Maßnahmen treffen sie aufgrund ihrer Risikobetrachtung und den Informationen des Herstellers eines Produktes oder Arbeitsmittels. Beides zusammen, also der Erhalt der Widerstandsfähigkeit und das Treffen der betreiberseitig notwendigen Maßnahmen, haben einen Einfluss auf die sichere Verwendung von Produkten, die bei der Arbeit verwendet werden.

Auch wenn es gemeinsame Anstrengungen von Herstellern und Arbeitgebern erfordert, Cybersecurity in der täglichen Praxis zu realisieren, so ist es eben auch erforderlich, die Pflichten des jeweiligen Akteurs klar zu definieren. Eine knapp umrissene Pflicht, dass der Arbeitgeber die Unterstützung des Herstellers zum Erhalt der Widerstandsfähigkeit eines Produktes zu nutzen hat, greift viel zu kurz. Sowohl gesetzliche Bestimmungen, die an Arbeitgeber gerichtet sind, als auch technische Voraussetzungen, die für den sicheren Betrieb von Maschinen und Anlagen zu beachten sind, lassen eine solch vereinfachte Betrachtung und Herangehensweise nicht zu. Hinzukommt, dass bei der Balance von Maschinen- und Anlagensicherheit einerseits sowie der Cybersecurity andererseits durchaus Zielkonflikte entstehen können, die gelöst werden müssen, um der Anlagen- und Maschinensicherheit, dem sicheren Betrieb solcher Einrichtungen und dem Erhalt der Widerstandsfähigkeit der Cybersecurity Rechnung tragen zu können. Auch andere Einflussgrößen mögen bei dieser Balance zu beachten sein.

Aufgrund der Erfahrungen aus der Praxis sind die folgenden Aspekte bei der Festlegung gesetzlicher Pflichten für Arbeitgeber im Bereich der Cybersecurity als Voraussetzungen zu berücksichtigen:

Pflicht zur Nutzung der Herstellerunterstützung zum Erhalt der Cyber-Widerstands-fähigkeit
Die Cyber-Widerstandsfähigkeit eines Produktes kann nicht aufrechterhalten werden, wenn der Arbeitgeber die Unterstützung des Herstellers zum Erhalt genau dieser Widerstandsfähigkeit nicht nutzt und Hinweise des Herstellers ignoriert. Daher ist eine gesetzliche Pflicht erforderlich, die den Arbeitgeber grundsätzlich zur Nutzung der oben genannten Unterstützung des Herstellers verpflichtet. Damit wird erreicht, dass gemeinsame Anstrengungen von Arbeitgebern und Herstellern wirken, um den cybersicheren Betrieb von Maschinen und Anlagen nach dem Stand der Technik zu gewährleisten.

Verbunden mit dieser grundsätzlichen Pflicht zur Nutzung der Herstellerunterstützung bedarf es jedoch bestimmter Freiheitsgrade für den Arbeitgeber, um beispielsweise dem Zielkonflikt

bestehend aus Anlagen- und Maschinensicherheit, dem sicheren Betrieb solcher Einrichtungen und dem Erhalt der Widerstandsfähigkeit der Cybersecurity Rechnung tragen zu können. Dazu ist die freie Wahl des Zeitpunktes zur Nutzung der Herstellerunterstützung wichtig. Der genannte Zielkonflikt kann weitere Aspekte, wie Maschinenfunktionen, die Leistungsfähigkeit der Maschine und wirtschaftliche Fragestellungen betreffen.

Freie Wahl des Zeitpunkts zur Nutzung der Herstellerunterstützung
Zur Nutzung der Herstellerunterstützung zum Erhalt der Widerstandsfähigkeit sind sehr oft Betriebsunterbrechungen erforderlich. Bei diesen Unterbrechungen können dann z.B. Software Updates oder Patches installiert oder Hardwarekomponenten erneuert werden, mit denen das System wieder die erforderliche Widerstandsfähigkeit erlangt und sicher betrieben werden könnte. Arbeitgebern muss die Gelegenheit gegeben werden, in Abhängigkeit vom Grad der Gefährdung, den Zeitpunkt der Nutzung der Herstellerunterstützung frei zu wählen.

Planung einer möglichen Betriebsunterbrechung
Betriebsunterbrechungen müssen vom Arbeitgeber gut geplant werden können, damit die betrieblichen Belange berücksichtigt werden. Dabei spielen auch Pflichten des Arbeitgebers eine Rolle, um dem Kunden gegenüber versprochene Lieferzusagen einhalten zu können. In einem anderen Fall könnte die Installation solcher Updates bei geplanten Betriebsunterbrechungen stattfinden, bei denen ohnehin Prüf-, Wartungs- und Reparaturarbeiten durchgeführt werden.

Risiko-Einschätzung des Arbeitgebers zur Cyber-Angriffslage
Ob die Herstellerunterstützung zum Erhalt der Widerstandsfähigkeit ein sofortiges Handeln erfordert oder ob sie zu einem späteren Zeitpunkt genutzt werden kann oder ob sie für die konkrete Anwendung überhaupt erforderlich ist, muss der Entscheidung des Arbeitgebers obliegen. Diese Entscheidung trifft er auf der Grundlage einer Risikoeinschätzung, die er aufgrund der Bedrohungslage durchführt. Dabei wird der Arbeitgeber auch behördliche Informationen berücksichtigen sowie seine organisatorischen Maßnahmen und eigene Erkenntnisse zur individuellen und aktuellen Bedrohungslage. Weitere Informationen aus Fachkreisen der Cybersecurity mögen bei dieser Entscheidung des Arbeitgebers Berücksichtigung finden.

Auswertung von behördlichen Informationen
EU-Kommission und Bundesregierung haben die Notwendigkeit einer infrastrukturellen und operativen Unterstützung der Wirtschaft erkannt. Die EU-Behörde European Union Agency for Cybersecurity (ENISA) erhält mit den Bestimmungen des Cybersecurity Act (CSA) umfassende Befugnisse, um eine Bedrohungslage zu ermitteln, Maßnahmen zu ergreifen und Handlungsempfehlungen für Behörden und Wirtschaftsakteure aussprechen zu können. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dieses Handlungsspektrum auf nationaler Ebene, wobei künftig eine verbesserte Absprache mit der Europäischen Agentur erfolgen soll. Diese Informationen und Handlungsempfehlungen werden vom Maschinenbau begrüßt und im Sinne einer Infrastruktur zur sicheren Nutzung des Netzes wahrgenommen.

Überprüfung der Wirksamkeit/Umsetzung organisatorischer Maßnahmen
Ein weiterer wichtiger Aspekt für die sichere Nutzung der Herstellerunterstützung zum Erhalt der Widerstandsfähigkeit zur Cybersecurity ist die Überprüfung der Maßnahmen, wie Software Updates. Dabei geht der Arbeitgeber davon aus, dass der Hersteller die Maßnahmen zum Erhalt der Widerstandsfähigkeit auf Wirksamkeit und ordnungsgemäße Funktion überprüft hat. Bei dieser Überprüfung durch den Hersteller, die vor der Bereitstellung und auf der Grundlage des Konformitätsbewertungsverfahrens erfolgt, wird die bestimmungsgemäße

Verwendung und eine Verwendung zugrundgelegt, die vernünftigerweise für den Hersteller vorhersehbar ist. Der Arbeitgeber prüft dann, ob die Funktionen und die Prozesse der Anlage oder Maschine in der gewünschten Art weiterhin zur Verfügung stehen, ob sich durch das Update beispielsweise das funktionale Verhalten der Anlage oder der Maschine geändert hat oder ob sich sogar Fehler eingeschlichen haben, die vor der erneuten Inbetriebsetzung noch Korrekturmaßnahmen erfordern. Diese Prüfung bezieht sich insbesondere auf eine Verwendung, die von der bestimmungsgemäßen Verwendung abweicht, sowie auf Maßnahmen, die der Arbeitgeber und in Abweichung zu Herstellerangaben getroffen hat. Auch ist zu prüfen, ob die Maßnahmen insgesamt den erforderlichen Schutz gegen unerwünschte Cyberaktivitäten bieten.

Die Herstellerunterstützung zum Erhalt der Widerstandsfähigkeit kann auch organisatorische Maßnahmen oder Änderungen solcher Maßnahmen des Arbeitgebers erfordern. Auch diese Maßnahmen sind auf ihre Wirksamkeit hin zu prüfen. Alle die genannten Prüfungen und Korrekturen sind vor der erneuten Inbetriebsetzung vom Arbeitgeber umzusetzen. Daher benötigen diese Wirtschaftsakteure die erforderliche Entscheidungsfreiheit, damit diese Maßnahmen wirksam durchgeführt und Zielkonflikte aufgelöst werden können.

Störungen, die von Arbeitsmitteln und Produkten ausgehen, die nicht durch Arbeitgeber betrieben werden

Aus Sicht des Maschinenbaus kann auch ein Regelungsbedarf für den Betrieb von Produkten bestehen, die keine Arbeitsmittel sind oder für den Betrieb von Produkten, die von Privatpersonen verwendet werden. Die Widerstandsfähigkeit im Bereich der Cybersecurity hat demnach noch eine weitere Dimension: Die Störung anderer mit dem Internet verbundener Produkte.

Um alle Ursachen erfassen zu können, die sowohl von Arbeitsmitteln als auch von anderen Produkten ausgehen, sind die Bestimmungen zum Vermeiden und Abstellen von Störungen an Arbeitgeber, Betreiber und ggf. an Privatpersonen zu richten. Betreiber können professionelle Produkte verwenden, ohne Beschäftigte zu haben und ohne eine Arbeitgeberrolle einzunehmen. Privatpersonen können Produkte verwenden, von denen Störungen ausgehen, die einen signifikanten Einfluss auf die Cybersecurity im Netz haben oder sogar auf die Cybersecurity von Arbeitsmitteln.

Es liegt im öffentlichen Interesse und im Interesse der Wirtschaft, dass Produkte, die mit dem Internet verbunden sind, keine Störungen bei anderen Produkten, die mit dem Internet verbunden sind, verursachen. Dabei ist unerheblich, ob Produkte, die Störungen verursachen, beruflich oder privat verwendet werden. Bekanntermaßen können Produkte durch Cyberangriffe gekapert und in ein sogenanntes „Botnet“ integriert werden. Ziel dieser Einbindung ist es, andere Produkte und Dienste zu stören, zu beeinträchtigen, zu blockieren oder anzugreifen.

Diese störenden Produkte werden von Personen verwendet, die zunächst keine Kenntnis von dem „Botnet“ haben und daher von diesen unerwünschten Aktivitäten während des Betriebes überrascht werden. Daher können zunächst auch keine Maßnahmen gegen Störungen durch die Personen ergriffen werden.

Wenn solche „Botnet’s“ gefunden werden, liegt es im öffentlichen Interesse und im Interesse der Wirtschaft, dass sie ausgeschaltet oder in ihrer Funktion sehr eingeschränkt werden, damit von ihnen keine weiteren Störungen mehr ausgehen können. Ziel dieser Überlegungen ist es, dass es dadurch keine Störungen im Netz gibt oder etwaige Störungen wirksam beseitigt werden.

Als Analogie können Regelungen anderer Bereiche herangezogen werden, wie der elektromagnetischen Verträglichkeit und der Funkkommunikation. Im deutschen Gesetz zur elektromagnetischen Verträglichkeit und im Funkanlagen-Gesetz, die die nationale Umsetzung europäischer Harmonisierungsrechtsvorschriften sind, gibt es gesetzliche Bestimmungen, dass die zuständige Behörde gegen Störungen von Rundfunk und Funkkommunikation vorgehen kann.

In anderen Jurisdiktionen gelten bereits Bestimmungen, die das Abschalten von gehackten privaten IoT-Geräten durch Behörden erlauben. Die Übernahme und Erweiterung um Anforderungen zur Störungsbehebung an Betreiber von IoT-Geräten sind im Sinne der Stabilität von Industrie 4.0 Kommunikation zu berücksichtigen.

Die Integration der oben genannten Bestimmungen in Vorschriften zum Inverkehrbringen von Produkten ist gewählt worden, um den für die Marktüberwachung zuständigen Behörden die gesetzliche Grundlage zum Handeln zu geben. Werden die Pflichten für die Cybersecurity, die an Arbeitgeber gerichtet sind, durch einen europäischen Rechtsakt separat zum Inverkehrbringensrecht geregelt, der national umgesetzt werden muss oder eine direkte Rechtswirkung in den Mitgliedstaaten entfaltet, können Bestimmungen zum Eliminieren von Störungen auch durch diesen Rechtsakt erfasst werden. Da die Beseitigung der genannten Störungen nicht zwingend durch Marktüberwachungsbehörden vollzogen werden muss, können auch andere Behörden diese Aufgaben erfüllen.

30. Juli 2020

Kontakte im VDMA:

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

Steffen Zimmermann
Industrial Security @ VDMA
+49 69 6603 1978
E-Mail steffen.zimmermann@vdma.org