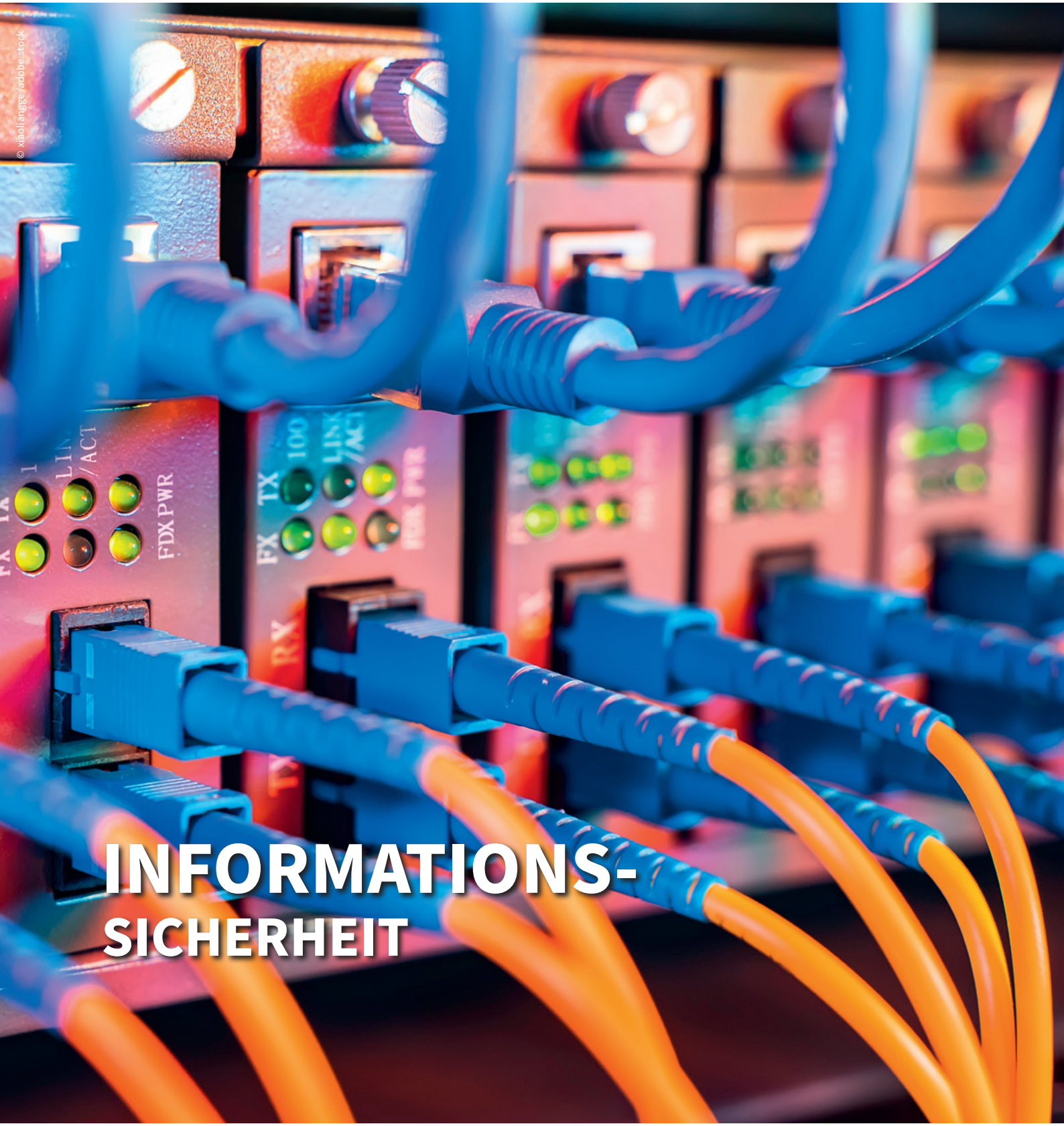
KAN Brief
Kommission Arbeitsschutz und Normung
3/23



INFORMATIONS-SICHERHEIT

Inhalt

© a_korn - stock.adobe.com

Titel

Themen

© GordonGrand - stock.adobe.com

© KAN

www_kan_de

Kommission Arbeitsschutz und Normung (KAN)

KAN_Arbeitsschutz_Normung

KAN – Kommission Arbeitsschutz und Normung

Benjamin Pfalz
Vorsitzender der KAN
IG Metall

Cybersecurity: eine regulative und betriebliche Herausforderung

Unternehmen müssen sich mehr denn je vor Cyberangriffen schützen. Dabei handelt es sich längst auch um eine Frage des Arbeitsschutzes. Durch die Interaktion zwischen Mensch und Maschine, aufgrund ferngesteuerter Arbeitsmittel, vernetzter Produktionsanlagen und des zunehmenden Einsatzes von maschinellem Lernen muss Cybersicherheit immer öfter auch im Rahmen der betrieblichen Gefährdungsbeurteilung berücksichtigt werden. Grundsätzlich spielen Maßnahmen zur Produktsicherheit eine besondere Rolle.

Die Regelsetzung hat diese Aspekte zunehmend aufgenommen. Für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen beispielsweise konkretisiert die TRBS 1115 die Betriebssicherheitsverordnung bezüglich der Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen. Gleichzeitig behandeln die neue EU Maschinen- und die kommende KI-Verordnung das Thema. Der sogenannte Cyber Resilience Act ist auf den Weg gebracht, um das Inverkehrbringen von Produkten und Vorprodukten mit digitalen Elementen zu regeln.

Die Normung muss die Verordnungsebene nun angemessen untersetzen. Der Normungsauftrag zum KI-Verordnungsentwurf adressiert das Thema Cybersecurity deutlich. Die europäischen Normungsorganisationen reagieren darauf bereits mit der Überprüfung des vorhandenen Normenwerks und der Zuschreibung des Themas innerhalb ihrer Strukturen.

Die Stimme des Arbeitsschutzes darf dabei keinesfalls fehlen! Die KAN widmet sich dem Thema daher auf allen Ebenen, beispielsweise durch ein Fachgespräch zur arbeitsschutzrelevanten Normung im Kontext der KI-Verordnung noch im laufenden Jahr. «

EU-Verordnung: Die vernetzte Geräte- und Maschinenwelt soll sicherer werden

Hersteller von Produkten „mit digitalen Elementen“ müssen die Cybersicherheit künftig während des ganzen Lebenszyklus gewährleisten, plant die EU-Kommission mit dem Cyber Resilience Act.

Die EU-Kommission macht angesichts anhaltender Online-Angriffe etwa mit Verschlüsselungstrojanern weiter Druck beim Absichern von IT-Sicherheitslücken. Nach Gesetzen wie dem 2019 beschlossenen Cybersecurity Act, mit dem die Basis für ein EU-weites Zertifizierungsschema für die IT-Sicherheit vernetzter Geräte, Systeme und Dienste steht, oder der jüngsten Novelle der Richtlinie über die Netzwerk- und Informationssicherheit (NIS2) hat sie im September 2022 einen Entwurf für einen Cyber Resilience Act (CRA)[1] auf den Weg gebracht. Laut der geplanten Verordnung zur Cyber-Widerstandsfähigkeit sollen Produkte „mit digitalen Elementen“ wie Hard- und Software künftig „mit weniger Schwachstellen auf den Markt kommen“.

Breit ist der Geltungsbereich des Entwurfs. Die Kommission will etwa „jedes Software- oder Hardware-Produkt und dessen Ferndatenverarbeitungslösungen“ einschließlich zugehöriger Komponenten erfassen, selbst wenn sie getrennt in Verkehr gebracht werden. Ein Schwerpunkt dürfte auf dem Internet der Dinge liegen oder auf privaten Kleinroutern („Plaste-Routern“), die aufgrund vieler eingebauter Sicherheitslücken bislang häufig einfach angreifbar sind. Außen vor bleiben sollen Produkte, „die ausschließlich für die nationale Sicherheit oder für militärische Zwecke entwickelt wurden“, oder die speziell für die Verarbeitung von Verschlusssachen bestimmt sind. Auch Sektoren wie die Luftfahrt, Medizinprodukte oder Kfz sind nicht betroffen, da für sie schon eigene einschlägige Anforderungen gelten.

Erfasste Hersteller müssen dem Vorhaben zufolge künftig grundlegende Cybersicherheitsanforderungen für das Design, die Entwicklung und den Fertigungsprozess erfüllen, bevor sie ein Gerät auf den Markt bringen. Sie sollen angehalten werden, Schwachstellen während des gesamten Lebenszyklus des Geräts zu überwachen und durch automatische und kostenlose Updates zu beheben. Dazu kommt eine Pflicht für die Hersteller, der EU-Agentur für Cybersicherheit ENISA binnen knapp bemessener 24 Stunden jeden Vorfall zu melden, der sich auf die Sicherheit einer Hard- und Software auswirkt. Generell soll eine koordinierte Linie zur Offenlegung von Schwachstellen eingeführt werden.

Angriffsflächen bei den einbezogenen Geräten müssten laut dem CRA begrenzt, die Auswirkungen von Zwischenfällen minimiert werden. Die erfassten Produkte sollen die Vertraulichkeit der Daten etwa durch Verschlüsselung sicherstellen. Pflicht werden soll der Schutz der Integrität und Verarbeitung von Informationen und Messwerten, die für das Funktionieren eines Artikels unbedingt erforderlich sind.

Über diese Basisauflagen hinaus hat die Brüsseler Regierungsinstitution besonders kritische Hochrisikobereiche ausgemacht. Die entsprechenden Produkte teilt sie in zwei Klassen, für die ein unterschiedliches Konformitätsverfahren eingeführt werden soll. Zur Kategorie I gehören Identitätsmanagementsysteme, Browser, Passwortmanager, Antiviren-Programme, Firewalls, virtuelle private Netzwerke (VPNs), Netzwerkmanagement, umfassende IT-Systeme, physische Netzwerkschnittstellen, Router und Chips. Dazu kommen Betriebssysteme etwa für Smartphones oder Desktop-Rechner, Mikroprozessoren und das Internet of Things (IoT) in Unternehmen, die nicht als besonders empfindlich gelten.

Die höhere Risikoklasse II beinhaltet Desktop- und Mobilgeräte, virtualisierte und etwa in Maschinen eingebaute Betriebssysteme, Aussteller digitaler Zertifikate, Allzweck-Mikroprozessoren, Kartenlesegeräte, Robotersensoren und intelligente Messgeräte. Ferner sollen darunter IoT-Geräte, Router und Firewalls für den industriellen Einsatz fallen, der generell als „sensible Umgebung“ gilt. Denn IT-Sicherheitslücken haben längst auch massive Auswirkungen auf Maschinen und Anlagen, die zunehmend vernetzt und nicht mehr nur innerhalb des Betriebsgeländes erreichbar sind, und so auch auf den Arbeitsschutz.

Hersteller sollen Konformitätsbewertungen ihrer Produkte über ein internes Verfahren oder eine Prüfung durch anerkannte Stellen durchführen. Wenn der Produzent auf harmonisierte Normen setzt oder bereits ein Zertifikat im Rahmen eines europäischen Zertifizierungssystems für Cybersicherheit erhalten hat, ist davon auszugehen, dass die entsprechende Hard- oder Software mit der Verordnung übereinstimmt. Importeure und Händler werden verpflichtet, die Einhaltung der einschlägigen Verfahren durch den Produzenten und die CE-Kennzeichnung des Geräts zu überprüfen. Für wenig kritische Produkte dürften Hersteller selbst eine Konformitätserklärung erstellen. In der Risikoklasse II soll eine Bewertung durch Dritte nötig sein.

Die Kommission sieht Handlungsbedarf, da die verstärkte Cyberkriminalität schon bis 2021 zu geschätzten jährlichen Kosten in Höhe von 5,5 Billionen Euro geführt habe. In einem vernetzten Umfeld könne ein Cybersicherheitsvorfall bei einem Produkt ein ganzes Unternehmen oder eine ganze Lieferkette in Mitleidenschaft ziehen und sich oft innerhalb weniger Minuten über die Grenzen des Binnenmarktes hinweg ausbreiten, wie etwa im Falle des Computerschädlings WannaCry. Wirtschaftliche und soziale Aktivitäten würden so unterbrochen, sogar Leben bedroht.

Kritik am Verordnungsentwurf

Die Deutsche Gesetzliche Unfallversicherung (DGUV) kritisiert in einer Stellungnahme[2], dass bereits der Kernbegriff Cyber-Security nicht klar definiert sei. Darunter werde in verschiedenen Normen und Verordnungen wechselweise ein Zustand, eine Tätigkeit oder ein Produkt verstanden. Problematisch seien generell Wörter, die aus „Cyber“ zusammengesetzt, aber nicht genau umrissen würden. So würden – je nach Quelle – Angriffe per Funk oder USB-Schnittstellen mit dem Begriff Cyber-Security nicht betrachtet.

Kritisch sieht die DGUV auch die Pflicht für Hersteller, binnen 24 Stunden umfangreiche Details zu einer Sicherheitslücke zu melden. In dieser kurzen Zeit sei eine Prüfung in vielen Fällen nicht realistisch. Gleichzeitig sei die Weiterleitung von

© a_korn - stock.adobe.com

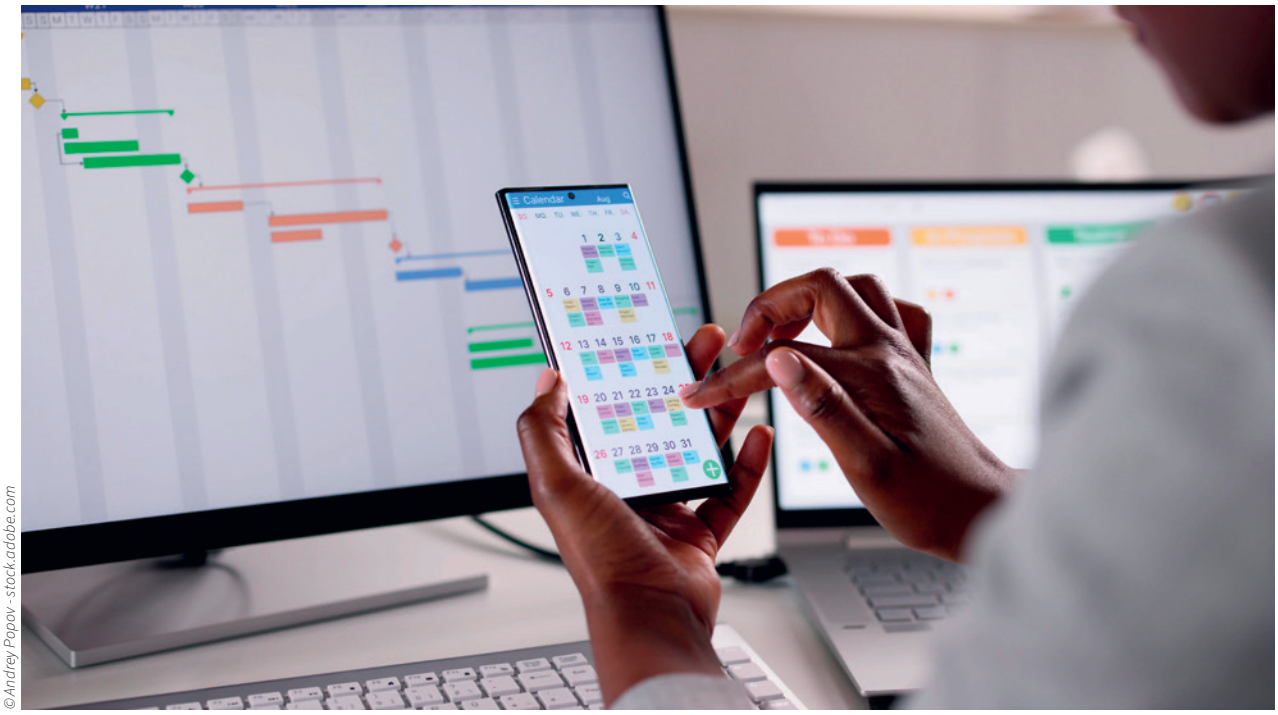
Details, die für Angriffe genutzt werden können, nicht unbedingt notwendig. In ihrer Stellungnahme plädiert die DGUV dafür, nur Daten zu übermitteln, die die Behörden wirklich benötigen, etwa zur Produktwarnung oder zur Abschätzung der Auswirkungen einer Schwachstelle. Auch das vorgesehene Zeitfenster von zwei Jahren, um sich auf die neuen Anforderungen einzustellen, hält die Gesetzliche Unfallversicherung für Hersteller zu knapp bemessen, die von anderen Produkten abhängig sind und etwa auf eine Konformitätsbewertung warten müssen.

Betriebssysteme könnten nicht sinnvoll geprüft werden, da sie sich ständig weiterentwickelten, moniert Jonas Stein, Leiter des Arbeitskreises Security der DGUV, ferner. Oft seien sie zudem – etwa bei Linux – von Open Source abhängig. Bei freier Software gebe es aber nicht einen einzelnen Hersteller, der für das Konformitätsverfahren zuständig wäre. Die Open-Source-Szene selbst befürchtet, in die Haftungsfalle zu tappen, da viele einzelne Entwickler zu Gemeinschaftswerken beitrügen und alle für potenzielle Lücken geradestehen müssten. Die Free Software Foundation Europe (FSFE) beklagt: „Aufgrund des Mangels an Finanzmitteln und Ressourcen, um die vorgeschlagenen Verfahren zur CE-Konformität zu durchlaufen, müssen einige dieser Projekte möglicherweise vollständig eingestellt werden."

Der EU-Ministerrat und der federführende Industrieausschuss des Europäischen Parlaments haben Mitte Juli zu dem Kommissionsvorschlag Position bezogen, sodass bald die Verhandlungen über einen finalen Kompromiss starten können. Die Mitgliedsstaaten plädieren etwa für eine vereinfachte Konformitätserklärung, mehr Unterstützung für kleine Unternehmen sowie eine Klarstellung der erwarteten Produktlebensdauer durch die Hersteller. Ausgenutzte Schwachstellen oder Sicherheitsvorfälle sollen zudem nicht an die ENISA, sondern an die zuständigen nationalen Behörden gemeldet werden müssen. Die Abgeordneten wiederum fordern präzisere Definitionen, praktikable Zeitpläne und eine gerechtere Verteilung der Verantwortlichkeiten. Andererseits drängen sie darauf, etwa auch Geräte fürs intelligente Heim, Smartwatches und private Sicherheitskameras in die Hochrisikokategorie aufzunehmen.

Dr. Stefan Krempl
Freier Journalist
sk@nexttext.de

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
2 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen/F3376532_de



©Andrey Popov - stock.adobe.com

Bewährtes Wissen in neuen Spezifikationen zu Industrial Security

Komponenten der funktionalen Sicherheit schützen das Leben und die Gesundheit von Personen, etwa indem sie den Zugang zu gefährlichen Bereichen von Maschinen und Anlagen verhindern. Wichtig ist, dass auch Manipulationen von außen die Sicherheit nicht beeinträchtigen. Dazu muss der Stand der Technik konsequent umgesetzt werden und Hersteller und Betreiber müssen im Falle von Sicherheitslücken angemessen darauf reagieren.

Damit Sicherheitsfunktionen von Steuerungen zuverlässig funktionieren können, muss auch die Steuerung selbst sicher sein – geschützt also vor Ausfall und Manipulation. Die steigende Frequenz neuer Katastrophenmeldungen im Bereich Industrial Security wirkt erschreckend. Doch es gibt Grund zur Hoffnung, denn fast alle Sicherheitslücken können nach dem Stand der Technik eigentlich sehr leicht vermieden werden, wie folgendes typische Beispiel zeigt.

Bereits 1883 stellte Auguste Kerckhoffs sechs Grundvoraussetzungen für eine vertrauliche Kommunikation auf. Die zweite lautete „Das System darf keine Geheimhaltung erfordern und muss ohne Nachteil in die Hände des Feindes fallen können“. Diese Schrift kannte Guglielmo Marconi offensichtlich nicht. Seine Telegraphie zur vertraulichen Kommunikation erforderte, dass niemand in Besitz eines der Geräte kommt oder eines nachbaut und auf die gleiche Frequenz einstellt. Nevil Maskelyne machte 1903 auf das Problem aufmerksam, indem er während Marconis Vorführung unflätige Nachrichten dazwischen morste, und gilt dadurch als einer der ersten Hacker. Obschon die sichere Verschlüsselung mit kryptographischen Methoden lange bekannt ist, findet sich der gleiche Designfehler auch heute noch etwa in Funksteuerungen für Ampelsysteme[1] oder Industriekranen[2].

Es fehlt an einheitlicher Definition der Begriffe

Der Navigator für Normen mit Bezug zu Security von der Universität Bremen[3] hat aktuell rund 800 Normen und über 2000 Treffer zu Rechtsvorschriften in einer Datenbank erfasst. Problematisch ist, dass die Dokumente unterschiedliche Begriffe verwenden und zum Teil nicht eindeutig definieren. Während manche Dokumente umfassend von Security oder Informationssicherheit handeln, erfinden andere neue Begriffe als Kofferwort aus „Cyber“ und einem weiteren Wort. Diese neu geschaffenen Wörter müssen im Dokument genau definiert werden, da sie für sich keine eindeutige Bedeutung haben. Mal ist „Cybersicherheit“ eine Tätigkeit, mal ist es eine Maßnahme gegen Angriffe aus dem Internet, ein anderes Mal ein Zustand, bei dem das Produkt vor Angriffen über Funk geschützt ist.

Besser als neue Wörter zu erzeugen ist es, mit den eindeutigen Begriffen Informationssicherheit oder Security zu arbeiten. Muss der Bedeutungsumfang etwa auf Angriffe über Funk reduziert werden, sollte die Einschränkung klar benannt werden. Einen anderen sehr eleganten Weg hat die EU-Maschinenverordnung gewählt, indem sie in Anhang III 1.1.9 einen „Schutz gegen Korrumpierung“ fordert und in diesem Punkt auch deutlicher ist als die bisherige EU-Maschinenrichtlinie. Dabei fokussiert sie sich auf das Schutzziel, dass etwa bei Fernzugriff keine gefährlichen Situationen entstehen dürfen und lässt offen, wodurch die Korrumpierung im Detail hervorgerufen wird.

Schnelle Kommunikation ist entscheidend

Eine schnelle und effektive Kommunikation ist der Schlüssel zur angemessenen Reaktion auf Sicherheitslücken. Wie schlecht es jedoch um die Kommunikation bestellt ist, zeigte sich im Dezember 2021, als eine Sicherheitslücke in der Softwarebibliothek Log4J Schlagzeilen machte. Diese Softwarebibliothek ist nicht nur Bestandteil vieler Serverdienste, sondern auch vieler Industriekomponenten. Während einerseits Vorwürfe laut wurden, dass die Bibliothek falsch eingesetzt wurde und die Sicherheitsprobleme durch Lesen der Dokumentation verhindert worden wären, rätselten gleichzeitig viele Hersteller, ob sie von Sicherheitslücken betroffen sind. Nicht selten brauchten Hersteller viele Monate, bis sie wussten, ob ihre Produkte betroffen sind.

Zusammengefasst fehlte es an

- einem Notfallkontakt für Security innerhalb des Unternehmens,
- einem einheitlichen Format für Handlungsempfehlungen und
- einem Standard, nach dem Hersteller auch mitteilen können, dass ein bestimmtes Produkt nicht von einer Sicherheitslücke betroffen ist.

Der Mangel an einheitlichen Informationen und Schnittstellen wird durch einen Satz offener Spezifikationen behoben, die von verschiedenen Zusammenschlüssen von Unternehmen, Behörden und Organisationen erarbeitet wurden und die jedes Unternehmen ab sofort umsetzen kann (siehe Tabelle). Ein Notfallkontakt nach der IETF-Spezifikation RFC 9116 wird in einer einfachen security.txt-Datei auf der Webseite hinterlegt[4]. Darin kann ein Hersteller auch auf seine Liste der Handlungsempfehlungen (CSAF) verweisen. Jedes Hardware- und Softwareprodukt bekommt eine weltweit eindeutige Identifikation (CPE), damit die Internationalen Warnmeldungen (CVE) automatisch den exakten Produkten und Versionen zugeordnet werden können. Die Kritikalität der Sicherheitslücke wird durch einen weltweit einheitlichen Index (CVSS) so gut es eben geht eingestuft. Anhand der offenen Spezifikation SPDX kann zu jedem Projekt maschinenlesbar dokumentiert werden, welche Bibliotheken verwendet wurden. Auf Betreiberseite kann dann ein Programm zu allen Produkten regelmäßig abfragen, ob Sicherheitswarnungen vorliegen und die Handlungsempfehlungen anzeigen.

Einige große Unternehmen setzen bereits auf diese Spezifikationen. Entscheidend ist nun, dass auch alle anderen Unternehmen schnell folgen, damit die Information zu Sicherheitsproblemen schnell und kostensparend erfolgt.

Als ersten Schritt sollten Unternehmen jetzt zumindest die Erreichbarkeit bei Sicherheitsvorfällen sicherstellen und einen Notfallkontakt bekannt machen. Mit der Anleitung auf https://cert.dguv.de kann das in wenigen Minuten umgesetzt werden.

Jonas Stein

Leiter des Prüflabors für Industrial Security und Leiter des Arbeitskreises Security der DGUV

Jonas.Stein@dguv.de

Offene Spezifikationen zur Informationssicherheit

Eingangsinformation	Gepflegt durch	Spezifikation
Eigener Notfallkontakt	Hersteller, Betreiber	„security.txt“ RFC 9116
Produktkennung / ID (Herstellername, Produktname, Version, Sprachausführung, ...)	Hersteller	CPE
Softwareliste (Software Bill of Materials – SBOM)	Hersteller	SPDX
Warnmeldung zur Sicherheitslücke	CVE-Nummerierungsstellen	CVE
Security Advisory (Handlungsempfehlung zur CVE)	Hersteller	CSAF
Eigenschaften zur Bewertung der Kritikalität	Hersteller	CVSS

Satz offener Spezifikationen, die gemeinsam einen entscheidenden Beitrag zur Industrial Security liefern werden. Sie werden die Kommunikation zu Sicherheitslücken in den kommenden Jahren auf die dringend erforderliche Geschwindigkeit beschleunigen.

1 ARD-Reportage 2021, https://ardmediathek.de „Hacker schalten Ampeln in Hannover auf Grün“
2 Andersen et al, 2019 “A Security Analysis of Radio Remote Controllers for Industrial Applications”, https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
3 https://cybersecurity-navigator.de
4 Kritische Sicherheitslücken an Maschinen und Anlagen und Kontaktstandard security.txt; https://cert.dguv.de

Die neue Maschinenverordnung – Konsequenzen für die harmonisierte Normung

In wohl kaum einem anderen Industriesektor haben Normen eine ähnlich hohe Bedeutung wie im Maschinenbau. Die neue EU-Maschinenverordnung stellt die Normenausschüsse vor die große Aufgabe, die Normen auf ihre Konformität mit der neuen gesetzlichen Grundlage zu überprüfen und ggf. Maßnahmen zu ihrer Anpassung vorzunehmen.

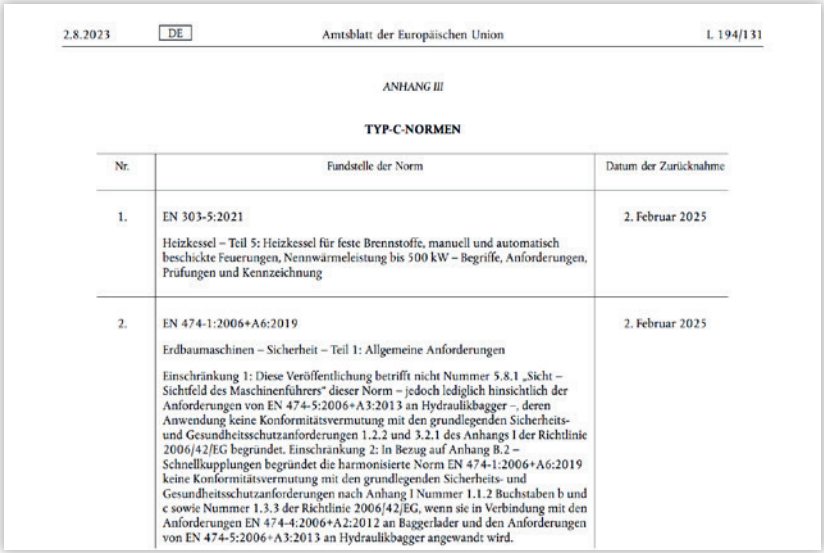
Das hohe Sicherheitsbedürfnis der Anwender beim Umgang mit Maschinen – in Kombination mit der Vielfalt an Maschinentypen – hat über die Jahre zu der erstaunlich großen Anzahl von mehr als 800 harmonisierten Normen unter der europäischen Maschinenrichtlinie geführt. Ihre Anwender dürfen davon ausgehen, dass die darin enthaltenen Lösungen und Maßnahmen geeignet sind, die gesetzlichen Anforderungen der Verordnungen oder Richtlinien zu erfüllen, für welche sie erarbeitet wurden. Von diesen über 800 Normen befassen sich etwa 100 sogenannte B-Normen mit bestimmten Sicherheitsaspekten oder Schutzeinrichtungen, die eine Vielzahl von Maschinen betreffen. Mehr als 700 Normen beschreiben Anforderungen und technische Lösungen für konkrete Maschinentypen (C-Normen). Im Zusammenspiel zwischen Maschinenrichtlinie und harmonisierten Normen hat sich über die Jahre ein bewährtes System etabliert, welches für Maschinenprodukte ein weltweit anerkanntes hohes Sicherheitsniveau gewährleistet.

Normung steht vor einer Mammutaufgabe

Mit der am 29. Juni 2023 im Amtsblatt der EU veröffentlichten neuen Verordnung (EU) 2023/1230 über Maschinen (MaschVO) hat die EU-Kommission nun ein neues gesetzliches Kapitel aufgeschlagen. Die Maschinenverordnung löst zum 20. Januar 2027 per Stichtagsregelung – also ohne Übergangsfrist – die aktuell noch gültige Maschinenrichtlinie 2006/42/EG (MRL) ab. Neben zahlreichen formellen und konzeptionellen Anpassungen des Rechtstexts wurden auch im Anhang I der MRL, der die wesentlichen Sicherheitsanforderungen (EHSR – Essential Health and Safety Requirements) beschreibt, signifikante Änderungen vorgenommen. In der MaschVO finden sich die EHSR im neuen Anhang III. Die Erfüllung dieser Sicherheitsanforderungen ist die Hauptaufgabe der harmonisierten Normen. Durch die Änderungen stellen sich unweigerlich folgende Fragen:

Welche unmittelbaren Auswirkungen haben die neuen und veränderten EHSR auf die Inhalte der heutigen harmonisierten Normen? Und können die unter der MRL harmonisierten Normen unter der MaschVO weiterverwendet werden und behalten sie ihre Konformitätsvermutung?

Die Beantwortung der ersten Frage ist nicht trivial, denn die praktische bzw. normative Umsetzung der neuen EHSR „Schutz gegen Korrumpierung“, „Überwa-



2.8.2023 DE Amtsblatt der Europäischen Union L 194/131

ANHANG III

TYP-C-NORMEN

Nr.	Fundstelle der Norm	Datum der Zurücknahme
1.	EN 303-5:2021 Heizkessel – Teil 5: Heizkessel für feste Brennstoffe, manuell und automatisch beschickte Feuerungen, Nennwärmeleistung bis 500 kW – Begriffe, Anforderungen, Prüfungen und Kennzeichnung	2. Februar 2025
2.	EN 474-1:2006+A6:2019 Erdbaumaschinen – Sicherheit – Teil 1: Allgemeine Anforderungen Einschränkung 1: Diese Veröffentlichung betrifft nicht Nummer 5.8.1 „Sicht – Sichtfeld des Maschinenführers“ dieser Norm – jedoch lediglich hinsichtlich der Anforderungen von EN 474-5:2006+A3:2013 an Hydraulikbagger –, deren Anwendung keine Konformitätsvermutung mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen 1.2.2 und 3.2.1 des Anhangs I der Richtlinie 2006/42/EG begründet. Einschränkung 2: In Bezug auf Anhang B.2 – Schnellkupplungen begründet die harmonisierte Norm EN 474-1:2006+A6:2019 keine Konformitätsvermutung mit den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen nach Anhang I Nummer 1.1.2 Buchstaben b und c sowie Nummer 1.3.3 der Richtlinie 2006/42/EG, wenn sie in Verbindung mit den Anforderungen EN 474-4:2006+A2:2012 an Baggerlader und den Anforderungen von EN 474-5:2006+A3:2013 an Hydraulikbagger angewandt wird.	2. Februar 2025

Mögliche Lösung für harmonisierte Normen unter der EU-Maschinenverordnung: Listung im Amtsblatt mit Einschränkung der Vermutungswirkung, ähnlich wie bei formellen Einwänden

chungsfunktion bei autonomen mobilen Maschinen“ oder „Vermeidung des Risikos des Kontakts mit stromführenden Freileitungen“ wird im Detail noch intensiv diskutiert.

Ein grober Überblick über die Geltungsbereiche der Normen zeigt aber: Kaum eine Maschinengattung dürfte von den neuen oder stark veränderten EHSR komplett unberührt bleiben. Es müssten also sämtliche harmonisierten Normen auf die Relevanz der neuen EHSR überprüft und im Falle ihrer Betroffenheit sowohl inhaltlich als auch formell gemäß den Verfahrensregeln der EU-Kommission (tabellarischer Anhang ZA, datierte Verweise) angepasst werden. Dazu wäre theoretisch eine Überarbeitung nahezu aller rund 800 harmonisierten Normen erforderlich – jeweils einschließlich der umfangreichen Assessments durch die HAS-Consultants. Eine Aufgabe, die in den verbleibenden dreieinhalb Jahren bis zur verbindlichen Anwendung der MaschVO völlig unrealistisch ist.

Eingeschränkte Listung als mögliche Zwischenlösung

Daher plant die EU-Kommission – Stand August 2023 – in einer außerordentlichen Aktion, sämtliche europäischen Normen (sowohl EN als auch EN ISO), die zu einem noch zu bestimmenden Zeitpunkt in der ersten Jahreshälfte 2026 unter der MRL harmonisiert sind, en bloc als harmonisierte Normen unter die neue MaschVO zu transferieren. Einzige Einschränkung: Diese Normen können natürlich nur für jene EHSR eine Harmonisierung gewährleisten, die sie auch schon unter der MRL adressieren. Um dies bei der Listung im Amtsblatt für Normennutzer kenntlich zu machen, wird es unerlässlich sein, dass die verantwortlichen Technischen Komitees (TCs) ihr jeweils gesamtes Normenportfolio einer Überprüfung (NICHT notwendigerweise einer Überarbeitung) unterziehen, um die jeweiligen Lücken zur neuen MaschVO zu identifizieren. Gleichzeitig werden bei CEN und CENELEC Arbeiten gestartet, um normative Lösungen zu den neuen bzw. signifikant modifizierten EHSR zu erstellen, so dass die identifizierten Lücken geschlossen werden können.

Derzeit wird mithilfe des koordinierenden CEN/CENELEC-Sektorforums „Machinery“ eine Handlungsanleitung erstellt, um den TCs Hilfestellung bei dieser sehr ambitionierten Aufgabe zu geben. Die Anleitung soll spätestens gegen Ende 2023 verfügbar sein.

Natürlich ist es bereits heute möglich und ratsam, bei anstehenden Normrevisionen oder neuen Projekten die Konformität mit der neuen MaschVO anzustreben. Somit ist zu hoffen, dass bis Anfang 2027 tatsächlich ein gewisser Anteil von Normen an die neue MaschVO angepasst ist. Für das Gros der harmonisierten Normen wird dies aber erst möglich sein, wenn die MaschVO bereits angewendet werden muss.

Ein genauerer Zeitrahmen zu zukünftigen Normenrevisionen wird mit dem neuen Normungsauftrag der Europäischen Kommission zur MaschVO erwartet, der im kommenden Jahr verfügbar sein soll. Im Gegensatz zu den früheren Mandaten ist dieser Normungsauftrag zeitlich begrenzt (vermutlich zwischen 5 und 10 Jahren). Er bildet die juristische Basis, auf deren Grundlage harmonisierte Normen unter der neuen MaschVO erstellt werden dürfen. Seit Ende Juni ist ein erster Entwurf des Normungsauftrags veröffentlicht. Die Kommentare der interessierten Kreise werden voraussichtlich im Herbst in den zuständigen Kommissionsgremien diskutiert.

Als weitere Maßnahme soll schließlich der Übergang der harmonisierten Normen von der MRL zur MaschVO für Normanwender erleichtert werden. Normen, welche von 2024 bis zur 1. Hälfte 2026 veröffentlicht werden, sollen mit zwei Anhängen ZA ausgestattet werden – je einem für die MRL und einem für die MaschVO – aus denen hervorgeht, welche Abschnitte der Norm welche Rechtsvorschriften abdecken. Auch hierzu werden die betroffenen Normen-TCs zeitnah informiert.

All diese beschriebenen Maßnahmen tragen dazu bei, einen möglichst reibungslosen Übergang der harmonisierten Normen von der alten MRL zur neuen MaschVO zu erreichen.

Dr. Frank Wohnsland

VDMA

Vorsitzender des CEN/CENELEC-Sektorforums „Machinery“

frank.wohnsland@vdma.org

Digitale Ergonomie: KAN-Projekt gibt Überblick zum Forschungsstand

Die BioMath GmbH hat im Auftrag der KAN untersucht, wo die Forschung zu Schnittstellen und Datenformaten bei digitalen Menschmodellen und Systemen zur Bewegungserfassung steht.

Im Arbeitsschutz werden digitale Modelle und Methoden zur Planung und Beurteilung von Produkten und Prozessen genutzt. Digitale Menschmodelle simulieren physische Aspekte der Arbeit. Zudem gibt es Systeme, die anhand von Koordinaten der menschlichen Gelenke im dreidimensionalen Raum Bewegungen erfassen. Diese Daten können dann in ein digitales Menschmodell eingespeist werden. Fachleute leiten daraus Maßnahmen für die sichere und gesundheitsgerechte Gestaltung von Arbeitsplätzen ab.

Sowohl Forschungseinrichtungen als auch Unternehmen verfügen über Methoden und Werkzeuge zur Analyse, Beurteilung und Darstellung der Daten aus digitalen Menschmodellen und Systemen zur Bewegungserfassung. Häufig handelt es sich aber um Insellösungen, die aufgrund unterschiedlicher Datenformate untereinander nicht kompatibel sind. Seit den 1960er Jahren wurden rund 150 unterschiedliche digitale Menschmodelle für verschiedene Zwecke entwickelt (die jedoch nicht mehr alle genutzt werden).

Eine Standardisierung der Schnittstellen

- zwischen digitalen Menschmodellen untereinander,
- zwischen Systemen zur Bewegungserfassung untereinander und
- zwischen digitalen Menschmodellen und Systemen zur Bewegungserfassung

wäre für den Arbeitsschutz hilfreich, da eine belastbarere Datengrundlage zur Ableitung von Maßnahmen für die menschengerechte Arbeitsgestaltung geschaffen werden könnte. Mit Hilfe einheitlicher Schnittstellen und Datenformate könnten Bewegungsdaten aus verschiedenen Quellen zusammengefügt und für übergreifende Auswertungen genutzt werden.

KAN-Projekt zeigt Vielfalt der Modelle auf

Im Rahmen eines KAN-Projektes hat die BioMath GmbH wissenschaftliche Publikationen zur digitalen Ergonomie erfasst und ausgewertet. Es galt dabei auch herauszustellen, welche arbeitswissenschaftlichen Erkenntnisse in Bezug auf digitale Menschmodelle und die digitale Erfassung, Bewertung und Darstellung von Bewegungsdaten als gesichert anzusehen sind.

Der Bericht[1] gibt einen Überblick über digitale Menschmodelle und deren Eigenschaften und Möglichkeiten. Die Studie zeigt, dass digitale Menschmodelle auf anthropometrische Maße aus unterschiedlichen Datenbanken zurückgreifen, die verschiedene Bevölkerungsgruppen abbilden. Zudem sind die Daten teils sehr unterschiedlich gruppiert und/oder aufgeschlüsselt. Die Qualität der Daten bestimmt auch die Qualität der digitalen Menschmodelle.

Außerdem wurde analysiert, welche Systeme zur Bewegungserfassung bereits in Studien untersucht wurden. Dabei ging es vorrangig um Möglichkeiten zum Datenaustausch. Hier zeigte die Recherche, dass es bislang kein einheitliches Vorgehen gibt.

In zukünftigen Forschungsprojekten sollten daher u.a. folgende Punkte näher beleuchtet werden:

- Für den Austausch von Daten zwischen digitalen Menschmodellen wäre es sinnvoll, ein herstellerneutrales, gut dokumentiertes, standardisiertes Format zu haben.

- Begriffsdefinitionen und mögliche Detailgrade z.B. für bestimmte Teile eines digitalen Menschmodells sollten festgelegt werden.

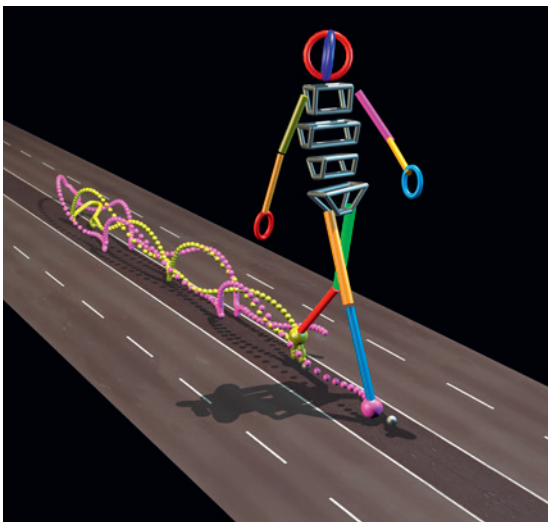
- Da es für die Eigenschaften und Konfiguration von Menschmodellen verschiedene Ansätze gibt, wären Festlegungen zur Struktur der Modelle wichtig, die die Vergleichbarkeit fördern.

Wie geht es weiter?

Die Projektnehmerin hat die Ergebnisse der Recherche in einem Bericht zusammengefasst, in dem die derzeitige Ausgangslage und Ansätze zur Harmonisierung einheitlicher Schnittstellen und Datenformate beschrieben werden. Die Inhalte dieses Berichts sollen in Form eines technischen Reports (DIN/TR) verfügbar gemacht werden. Dazu wird die KAN den Text aufbereiten und einen Antrag bei DIN stellen. Langfristiges Ziel ist es, grundlegende Normen für digitale Menschmodelle, Schnittstellen und Datenformate zu schaffen. Eine vollständige Harmonisierung der Anforderungen ist aus Sicht der KAN jedoch aktuell noch nicht möglich.

Katharina von Rymon Lipinski
vonrymonlipinski@kan.de

1 www.kan.de/fileadmin/Redaktion/Dokumente/KAN-Studie/de/2023_KAN-Projekt_Digitale_Ergonomie_bf_final.pdf



© vrx123 - stock.adobe.com

Der ASGA – ein neuer Ausschuss für übergreifende Arbeitsschutzthemen

Der staatliche Ausschuss für Sicherheit und Gesundheit bei der Arbeit (ASGA) kam 2021 zu den bestehenden Arbeitsschutzausschüssen beim Bundesministerium für Arbeit und Soziales (BMAS) hinzu. Was sind seine Aufgaben und was war der Anlass für seine Gründung?

Die staatlichen Ausschüsse[1] sind in Deutschland dafür zuständig, (technische) Regeln zu erarbeiten, die die allgemeinen Schutzziele der Einzelverordnungen unter dem Arbeitsschutzgesetz konkretisieren. Koordiniert von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) behandeln sie potentielle Gefährdungsfaktoren des Arbeitssystems wie Gefahrstoffe, Biostoffe, Arbeitsstätten und Betriebsmittel. Die Regeln stellen Arbeitgebern prozess- und gestaltungsbezogene Anforderungen bereit, mit deren Einhaltung die Inhalte der Einzelverordnungen zum Arbeitsschutzgesetz erfüllt werden (Vermutungswirkung).

Durch die Diversifizierung der Arbeitsformen, die Digitalisierung und klimabedingte Einflüsse auf die Arbeitsumgebung ist die bisher konsequent vertikal ausgerichtete Vorgehensweise der Regelsetzung nicht mehr ausreichend, um die aktuellen und zukünftigen Einwirkungen auf die Beschäftigten umfassend zu beurteilen und geeignete Maßnahmen abzuleiten. Auch bei klassischen Themen wie der Gefährdungsbeurteilung und der Unterweisung sind die Anforderungen unabhängig von einzelnen Gefährdungsfaktoren und sollten damit auch aus mehreren Perspektiven (horizontal) betrachtet werden.

Während der Corona-Krise und den damit einhergehenden neuen Herausforderungen an den betrieblichen Arbeits- und Gesundheitsschutz wurde dieser Bedarf besonders offensichtlich. Die SARS-CoV-Regel war die erste Regel, die gezielt faktorenübergreifend ausgelegt wurde. Der erfolgreiche betriebliche Einsatz dieser Regel machte deutlich, dass es sinnvoll ist zu prüfen, für welche weiteren Themenbereiche die Erarbeitung horizontaler Regeln für den betrieblichen Arbeits- und Gesundheitsschutz zielführend ist.

Aus diesem Grund verankerte die im Dezember 2020 veröffentlichte Ergänzung des § 24 a den ASGA[2] direkt im Arbeitsschutzgesetz. Zu den Aufgaben des neuen Ausschusses gehört es unter anderem – soweit kein anderer staatlicher Ausschuss zuständig ist – Regeln und Erkenntnisse zu erarbeiten, wie die im Arbeitsschutzgesetz gestellten Anforderungen erfüllt werden können.

© GordonGrand - stock.adobe.com

Ein zweiter Anlass zur Etablierung des neuen Ausschusses ist der Mangel an Kohärenz im bestehenden Regelwerk, der mit der streng vertikalen Ausrichtung der etablierten Ausschüsse zusammenhängt. Bereits im Jahr 2011 formulierte das „Leitlinienpapier zur Neuordnung des Vorschriften- und Regelwerks im Arbeitsschutz“ das Anliegen, das autonome Satzungsrecht der Unfallversicherungsträger und das staatliche Regelwerk inhaltlich besser abzustimmen – sowohl miteinander als auch innerhalb der beiden Regelungsbereiche. Der Weg dahin ist in zentralen Handlungsfeldern, wie z. B. der Gefährdungsbeurteilung, immer noch nahezu unbetreten. Es besteht Konsens innerhalb des ASGA, dieses Anliegen konsequent in den Blick zu nehmen.

Zusammensetzung und Arbeitsweise

Die Zusammensetzung des ASGA unterscheidet sich nicht von jener anderer Arbeitsschutzausschüsse. Im Ausschuss sind vom BMAS berufene Fachleute der öffentlichen und privaten Arbeitgeber, der Gewerkschaften, der Landesbehörden, der gesetzlichen Unfallversicherung und der Wissenschaft vertreten. Dem Ausschuss gehören 15 Mitglieder und 15 stellvertretende Mitglieder an.

Die Ausschussvorsitzende koordiniert neben der Leitung des ASGA auch die Zusammenarbeit aller Arbeitsschutzausschüsse in einem Steuerkreis. Dieses Gremium übernimmt eine zentrale Funktion bei der Erarbeitung fachübergreifender, horizontaler Regeln. Die Ausschüsse bringen ihre fachbezogene Expertise über mandatierte Personen direkt in die jeweiligen Projektgruppen ein. Sie sind so von der Erarbeitung der Projektskizze bis zur Verabschiedung der neuen Regel unmittelbar eingebunden. Das ist ein Novum.

Der ASGA tagt zwei Mal im Jahr. Der Steuerkreis fasst seine Argumente und Voten in entsprechende Empfehlungen und legt diese dem ASGA-Koordinierungskreis vor. Der Koordinierungskreis sondiert die aktuellen Themen und Aufgaben und bereitet die Beschlussvorlagen für die ASGA-Sitzungen vor.

Projekte und Schwerpunkte

Der ASGA hat sich – wie alle anderen Ausschüsse auch – ein Arbeitsprogramm für die aktuelle Berufungsperiode gegeben. Kernthemen sind die Gefährdungsbeurteilung, psychische Belastungen, effiziente und zeitgemäße Unterweisungen, ortsflexible Bildschirmarbeit außerhalb von Arbeitsstätten und Auswirkungen des Klimawandels auf Sicherheit und Gesundheitsschutz bei der Arbeit. Ziel ist die Entwicklung von staatlichen Regeln, die sich kohärent in das bestehende Regelwerk einfügen.

Herausforderungen gibt es aktuell zahlreiche, denn Veränderungsprozesse laufen nie ganz reibungslos ab. Ziel ist es, den richtigen Weg in eine gute, wertschätzende Ausschusskultur zu finden, um im Konsens das ambitionierte Arbeitsprogramm zu erfüllen. Der ASGA-Vorsitz muss zudem die Entwicklung geeigneter und transparenter Prozesse und Handlungshilfen vorantreiben, die diese Kulturentwicklung unterstützen.

Die Projektgruppe „Gefährdungsbeurteilung“ arbeitet bereits an der Konzeptionierung und inhaltlichen Ausgestaltung einer ASGA-Regel. Die Projektgruppe „Psychische Belastung“ wird voraussichtlich noch in diesem Jahr ihre Arbeit antreten.

Prof. Dr. Anke Kahl

Lehrstuhl für Arbeitssicherheit der Bergischen Universität Wuppertal

Vorsitzende des ASGA

1 www.bmas.de/DE/Arbeit/Arbeitsschutz/Arbeitsschutzausschuesse/arbeitsschutzausschuesse.html
2 www.baua.de/DE/Die-BAuA/Aufgaben/Geschaeftsfuehrung-von-Ausschuessen/ASGA/ASGA_node.html

Reform des EU-Produkthaftungsrechts

Die EU-Kommission hat im Herbst 2022 eine Modernisierung der EU-Produkthaftungsregelungen angestoßen. Nachdem sie Entwürfe für eine novellierte Produkthaftungsrichtlinie und eine neue KI-Haftungsrichtlinie veröffentlicht hat, beschäftigen sich EU-Ministerrat und Parlament damit nun intensiver.

Der Übergang in das digitale Zeitalter macht eine Anpassung nicht nur der Rechtsvorschriften für das Inverkehrbringen, sondern auch des Haftungsrechts erforderlich. Die alte Produkthaftungsrichtlinie, immerhin von 1985, die in Deutschland 1989 mit Erlass des Produkthaftungsgesetzes umgesetzt wurde, ist nicht mehr in der Lage, alle durch Produkte verursachten Schäden abzudecken. Resultat sind Rechtsunsicherheiten für Unternehmen und eine zunehmende Anzahl von Produkten, bei denen der Verbraucher keinen Rechtsanspruch auf Kompensationen für durch das Produkt verursachte Schäden hat.[1] Daneben soll die Richtlinie an die kürzlich aktualisierte Produktsicherheitsverordnung und an die Marktüberwachungsverordnung angeglichen werden.

Mehr Produkte und Schadensfälle im Fokus

Es ist davon auszugehen, dass die neue Produkthaftungsrichtlinie auf alle Arten von Produkten anwendbar sein wird – auch solche, die bisher nicht erfasst waren. Darunter fallen dann z.B. auch smarte Produkte, Softwareupdates, KI-Systeme und digitale Services, aber auch wiederaufbereitete Produkte und solche, die wesentlich modifiziert wurden. Hersteller der Kreislaufwirtschaft werden jedoch nicht für Schäden haften müssen, die durch nicht-modifizierte Teile des Produktes entstanden sind.

Bei Produkten aus Drittstaaten, die z.B. per Onlinehandel direkt von Verbrauchern in die EU importiert werden, werden Haftungsansprüche ausgeweitet. Zusätzlich zu den derzeit haftenden Importeuren gelten sie künftig für Herstellervertreter und weitere Akteure wie Online-Plattformen, die in der EU ansässig sind. Zudem sind prozessrechtliche Änderungen vorgesehen: Um die Informationsasymmetrie zwischen Hersteller und Verbraucher zu verringern, können die Wirtschaftsakteure zur Offenlegung von Beweismitteln verpflichtet werden. Insgesamt wird es eine deutliche Beweiserleichterung zu Gunsten der Geschädigten geben, jedoch ohne dass es zu einer Beweislastumkehr kommt. Die bisher vorgesehenen Grenzen zu Haftungshöchstbetrag und Selbstbeteiligung fallen im Entwurf weg.

Angepasste Haftungsregelungen

Ersatzansprüche auf Grundlage des Entwurfs der Produkthaftungsrichtlinie entstehen nur bei Personenschaden (einschließlich psychischer Gesundheitsschäden), Sachbeschädigung und Datenverlust. Es handelt sich um eine strenge Produkthaftung, die verschuldensunabhängig gegen den Hersteller und weitere Wirtschaftsakteure greift. Ansprüche können nur von natürlichen Personen geltend gemacht werden und auch nur, wenn das Produkt nicht ausschließlich für berufliche Zwecke genutzt wird.

Neue KI-Haftungsrichtlinie ergänzt den Rechtsrahmen

Begleitet werden soll die neue Produkthaftungsrichtlinie durch eine KI-Haftungsrichtlinie. Sie soll es Geschädigten im Falle von Schäden durch KI-Systeme deutlich erleichtern, ihre Ansprüche auf einer anderen Rechtsgrundlage als dem Produkthaftungsrecht geltend zu machen, z.B. bei Grundrechtsverletzungen oder zivilrechtlichen Haftungsregelungen.

Um eine Rechtzersplitterung zwischen den EU-Mitgliedsstaaten zu verhindern, soll ein harmonisierter Rechtsrahmen für die Haftung von Herstellern, Betreibern oder Nutzern von Künstlicher Intelligenz vorgegeben werden. Es ist vorgesehen, dass bei Schadensfällen die KI als verursachend angenommen wird. Geschädigte müssen dann nur noch zeigen, dass Anbieter, Betreiber oder Nutzer der KI eine relevante Verpflichtung schuldhaft nicht eingehalten haben und ein Kausalzusammenhang wahrscheinlich ist. Zudem sollen die Hersteller oder Zulieferer von Hochrisiko-KI verpflichtet werden, im Falle eines Prozesses alle relevanten Produktinformationen bereitzustellen.

Die KI-Haftungsrichtlinie allein bietet noch keine rechtlichen Schadenersatzansprüche, sondern sie ergänzt bestehende nationale verschuldensabhängige Haftungsregelungen bei Rechtsverletzungen durch KI. Die neuen, verschuldensabhängigen Haftungsregelungen erlauben eine vereinfachte Geltendmachung von Schadenersatzansprüchen, auf die sich alle natürlichen und juristischen Personen berufen können.

Verhandlung in den EU-Institutionen

Der EU-Ministerrat hat sich bereits mit dem Kommissionsentwurf der Produkthaftungsrichtlinie befasst und stimmt diesem weitgehend zu. Die Diskussion im Europäischen Parlament ist ebenfalls angelaufen, wird aber noch einige Monate in Anspruch nehmen. Die KI-Haftungsrichtlinie soll erst in einem zweiten Schritt verhandelt werden.

Freeric Meier
meier@kan.de

1 Evaluierungsstudie und Richtlinienvorschläge: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_5807

UK verlängert Gültigkeit der CE-Kennzeichnung

Das Ministerium für Wirtschaft und Handel des Vereinigten Königreichs hat angekündigt, die Anerkennung der CE-Kennzeichnung für Produkte, die in Großbritannien (England, Schottland, Wales) auf den Markt gebracht werden, auf unbestimmte Zeit über Dezember 2024 hinaus zu verlängern. Für Nordirland war dies bereits zuvor der Fall. Die Regelung gilt für 18 Verordnungen im Zuständigkeitsbereich des Ministeriums, unter anderem für Maschinen, persönliche Schutzausrüstung, Druckgeräte, Niederspannungsgeräte, ATEX und Gasgeräte.

Ursprünglich sollte die Anerkennung der CE-Kennzeichnung in Großbritannien Ende 2024 auslaufen und durch eine verpflichtende UKCA-Kennzeichnung (UK Conformity Assessed) abgelöst werden. Mit der neuen Regelung können Unternehmen künftig zwischen beiden Kennzeichnungen wählen. Dies ist sowohl für Unternehmen in der EU als auch für britische Unternehmen von Vorteil, da sie ihre Produkte nicht doppelt zertifizieren lassen müssen, um sie in den jeweils anderen Wirtschaftsraum zu exportieren.

Weitere Informationen (auf Englisch): www.gov.uk/government/news/uk-government-announces-extension-of-ce-mark-recognition-for-businesses

Neue Kampagne der EU-OSHA

Die Europäische Agentur für Sicherheit und Gesundheit am Arbeitsplatz (EU-OSHA) startet im Oktober 2023 ihre zweijährige Kampagne „Sicher und gesund arbeiten in Zeiten der Digitalisierung“. Die EU-OSHA und ihre nationalen Kontaktpunkte organisieren eine Vielzahl von europäischen und nationalen Veranstaltungen, um bei Beschäftigten, Unternehmen, und politischen Entscheidungsträgern das Bewusstsein für Sicherheit und Gesundheit bei der Arbeit zu schärfen.

Inhaltliche Schwerpunkte der Kampagne sind die Arbeit auf digitalen Plattformen, Automatisierung von Aufgaben, mobiles und hybrides Arbeiten, Personalmanagement mit Hilfe künstlicher Intelligenz und intelligente digitale Systeme. Ziel ist es, zu diesen Themen Daten und Fakten zur Verfügung zu stellen, die die Entwicklung relevanter Rechtsvorschriften, Leitlinien, Sensibilisierungs- und Unterstützungsmaßnahmen sowie neuer Dienstleistungen und Produkte befördern können.

Informationen zur Kampagne: https://healthy-workplaces.osha.europa.eu/de

A+A 2023: Die KAN ist dabei!

Vom 24. bis 27. Oktober 2023 findet die Fachmesse A+A in Düsseldorf statt. Die KAN befindet sich auf dem Gemeinschaftsstand der DGUV, der sich in diesem Jahr zum ersten Mal in Messehalle 5, Stand 5C06 dem Publikum zeigt. Wir informieren Sie über unsere aktuellen Arbeitsgebiete wie fahrerlose selbstfahrende Maschinen, Infektionsschutzmasken oder Gasgrills, stellen Ihnen unsere Publikationen vor und beantworten gern Ihre Fragen rund um Arbeitsschutz und Normung.

„Genormter Mensch – Körpermaße im Wandel“ ist das KAN-Thema in der „Sprech-Stunde Sicherheit und Gesundheit“ am Donnerstag, 26. Oktober um 10 Uhr auf der Bühne des DGUV-Gemeinschaftsstandes.

Auf dem zeitgleich stattfindenden A+A-Kongress ist die KAN mit folgenden Vorträgen vertreten:

- 25. Oktober 2023: VISION ZERO versus Standardization: A Position Statement
- 26. Oktober 2023: Arbeitsschutzrelevante Managementnormen abseits der ISO 45001

Wir freuen uns auf Ihren Besuch!

Weitere Informationen zum Programm finden Sie unter www.aplusa.de.

Normungsarbeit im Arbeitsschutz – Grundlagen- und Aufbauseminar

In Zusammenarbeit mit dem Institut für Arbeit und Gesundheit der DGUV (IAG) bietet die KAN zwei Seminare zur Normungsarbeit im Arbeitsschutz an.

Das **Grundlagenseminar** richtet sich an aktive Mitglieder von Normungsgremien und an alle, die sich zum Nutzen von Sicherheit und Gesundheit mit der Normung befassen möchten. Sie lernen im Seminar die Abläufe der Normenerarbeitung und Ihre Einflussmöglichkeiten in den verschiedenen Phasen kennen. Tipps, Tricks und der Austausch untereinander unterstützen Sie bei der erfolgreichen Mitarbeit in der Normung. Das Grundlagenseminar findet vom 25. bis 27. Oktober 2023 in Dresden statt.

Sie kennen sich mit den Grundlagen der Normungsarbeit gut aus und wollen Ihre Kompetenzen erweitern? Im **Aufbausemi-nar** treffen Sie auf andere erfahrene Normungsexpertinnen und -experten und überlegen gemeinsam, mit welchen Strategien Sie Ihre (Mit)arbeit weiter optimieren können. Sie tauschen Erfahrungen über den Normungsprozess und die Möglichkeiten der Einflussnahme aus und erhalten aktuelle Informationen aus dem Bereich der Normung.

Die Präsenzphase des Aufbauseminars findet am 5. und 6. Dezember 2023 in Dresden statt. Die weiteren Seminarteile sind online oder als Selbstlernphase geplant.

Informationen und Anmeldung: https://asp.veda.net/webgate_dguv_prod, Veranstaltungsnummer 570044 (Grundlagen) und 570139 (Aufbau)

Europäische Änderungen an IEC-Normen

Elektrotechnische Normen sollen nach dem Frankfurter Abkommen bevorzugt auf internationaler Ebene bei IEC erarbeitet und parallel von CENELEC als identische europäische Normen (EN IEC) übernommen werden. In manchen Fällen sind jedoch bei der Übernahme von IEC-Normen europäische Änderungen notwendig, um Anforderungen der Binnenmarktrichtlinien oder -verordnungen zu genügen.

Dass eine solche Abweichung vorliegt, ist daran erkennbar, dass CENELEC diese Normen dann nicht als **EN IEC** 6xxxx, sondern nur als **EN** 6xxxx herausgibt – jedoch mit der gleichen Nummer wie bei IEC.

Termine

18.-20.10.23 » Dresden

Seminar
Manipulation an Maschinen und Anlagen: Risiken erkennen, Maßnahmen ergreifen
IAG
https://asp.veda.net/webgate_dguv_prod
🔎 570089

19.10.23 » Bern

Tagung
Schweizerische Tagung für Arbeitssicherheit
SUVA
www.suva.ch 🔎 Tagung

24.-27.10.23 » Düsseldorf

Messe und Kongress / Trade fair and Congress
A+A 2023
Messe Düsseldorf
www.aplusa.de

25.10.23 » Online

Informationsveranstaltung
Dresdner Treffpunkt „Kollege Roboter – Mensch-Roboter Interaktion in der betrieblichen Praxis“
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Kollege Roboter

25.-27.10.23 » Dresden

Seminar
Grundlagen der Normungsarbeit im Arbeitsschutz
IAG/KAN
https://asp.veda.net/webgate_dguv_prod
🔎 570044

26.10.23 » Düsseldorf

Kongress
GfA-Herbstkongress 2023 „Nachhaltige Sicherheit und Gesundheit bei der Arbeit“
Gesellschaft für Arbeitswissenschaft (GfA)
www.gesellschaft-fuer-arbeitswissenschaft.de

02.11.23 » Berlin

Nationaler Kick-off der EU-OSHA-Kampagne 2023-25
Sicher und gesund arbeiten in Zeiten der Digitalisierung
BAuA/DGUV/EU-OSHA
www.baua.de 🔎 Nationaler Kick-off

13.11.23 – 18.01.24 » Dresden/Online

Seminar
Normungsarbeit im Arbeitsschutz weiterdenken – Aufbauseminar
IAG/KAN
https://asp.veda.net/webgate_dguv_prod 🔎 570139

15.11.23 » Online

Informationsveranstaltung
Dresdner Treffpunkt „Die neue europäische Maschinenverordnung“
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Maschinenverordnung

27.-28.11.23 » Bonn

Seminar
Maschinenanlagen/Technische Anlagen
MBT
www.maschinenbautage.eu/seminare/seminarmaschinenanlagen

29.11.-01.12.23 » Dresden

Seminar
Sicherer Einsatz von kollaborierenden Robotern
Institut für Arbeit und Gesundheit der DGUV (IAG)
https://asp.veda.net/webgate_dguv_prod
🔎 570164

04.-07.12.23 » Sankt Augustin

Seminar
Sicherheitstechnik von Maschinen
Institut für Arbeitsschutz der DGUV (IFA)
https://dguv.converia.de/frontend/index.php?sub=94

Bestellung

www.kan.de » Publikationen » KANBrief » KANBrief-Bestellservice (kostenfrei)

Gefördert durch: Bundesministerium für Arbeit und Soziales aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

Herausgeber
Verein zur Förderung der Arbeitssicherheit in Europa e.V. (VFA)
mit finanzieller Unterstützung des Bundesministeriums für Arbeit und Soziales

Redaktion
Kommission Arbeitsschutz und Normung (KAN), Geschäftsstelle
Sonja Miesner, Michael Robert
Tel. +49 2241 231 3450 · www.kan.de · info@kan.de

Verantwortlich
Angela Janowitz, Alte Heerstr. 111, D – 53757 Sankt Augustin

Publikation
vierteljährlich

ISSN: 2702-4024 (Print) · 2702-4032 (Online)