FREDERICK RAFFEL, LL. M. (CUHK HONG KONG)/DR. KRISTINA SCHREIBER*

IT-Sicherheitsrecht für den Maschinen- und Anlagenbau

Neue sektorspezifische Pflichten durch die Umsetzung der NIS-2-Richtlinie

Die Bedeutung der Informationssicherheit nimmt mit fortschreitender Digitalisierung in allen Sektoren fortlaufend zu. Auch den Maschinen- und Anlagenbau bedrohen Angriffe auf die digitalen Systeme, sog. „Cyberattacken" im Sprachgebrauch der EU. Mit ihrer Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, die sog. NIS-2-Richtlinie, hat die EU daher auch den Maschinen- und Anlagenbau teils erstmalig mit spezifischen Pflichten im Bereich der Informationssicherheit belegt. Der deutsche Gesetzgeber arbeitet derzeit an der Umsetzung dieser NIS-2-Richtlinie in das deutsche Recht. Seit Ende Juli 2024 liegt ein abgestimmter Regierungsentwurf vor, der jetzt in das parlamentarische Verfahren geht und voraussichtlich im Frühjahr 2025 in Kraft treten wird. Gerade Unternehmen, die erstmalig von den informationssicherheitsrechtlichen Pflichten erfasst werden, müssen sich frühzeitig mit der Umsetzung beschäftigen. Wir geben einen Überblick, welche Anforderungen aus dem neuen Recht für den Maschinen- und Anlagenbau besonders wichtig werden.

The importance of information security is continuously increasing with ongoing digitalization in all sectors. Also the mechanical and plant engineering industry is threatened by attacks on digital systems, known as "cyberattacks" in EU terminology. With its Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the European Union, the so-called NIS-2 Directive, the EU has therefore imposed specific obligations in the area of information security on the mechanical and plant engineering industry, in some cases for the first time. The German legislator is currently working on implementing this NIS-2 Directive into German law. Since the end of July 2024, a coordinated government draft has been available, which is now entering the parliamentary process and is expected to come into force in spring of 2025. Especially companies that are subject to information security obligations for the first time must start early with the implementation. We provide an overview, which requirements from the new law will become particularly important for the mechanical and plant engineering industry.

*) Frederick Raffel, LL. M. (CUHK Hong Kong), ist Syndikusrechtsanwalt bei der SMS group GmbH in Mönchengladbach; Dr. Kristina Schreiber ist Rechtsanwältin, Fachanwältin für Verwaltungsrecht, CIPP/E und Partnerin bei Loschelder Rechtsanwälte und auf die regulatorische Beratung von Unternehmen im IT- und Datenschutzrecht spezialisiert.

I. Die Entwicklung des Informationssicherheitsrechts

[1] Gesetzliche Vorgaben zur Informationssicherheit gibt es bereits seit vielen Jahren. Erste EU-Vorgaben zur Sicherheit in der Informationstechnik wurden 2016 mit der NIS-1-Richtlinie festgelegt.[1] Anders, als die derzeit in Umsetzung befindliche NIS-2-Richtlinie[2], adressierte die NIS-1-Richtlinie aber nur wenige besonders zentrale Dienste, die für die Aufrechterhaltung kritischer gesellschaftlicher und / oder wirtschaftlicher Tätigkeiten unerlässlich sind.

[2] Auf nationaler Ebene wurde die NIS-1-Richtlinie durch das NIS-Umsetzungsgesetz vom 23. Juni 2017 umgesetzt,[3] das in Artikel 1 als zentrales Element das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) an die neuen EU-rechtlichen Vorgaben anpasste. Das BSIG legt seither insbesondere die informationsrechtlichen Sicherheitspflichten für Kritische Infrastrukturen, die sog. KRITIS, fest. Welche Dienste im Detail als KRITIS qualifiziert werden, konkretisiert die auf Grundlage des BSIG erlassene Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV). Adressiert werden darin besonders bedeutsame Dienste in den Sektoren Energie, Wasser, Ernährung, ITK, Gesundheit, Finanz- und Versicherungswesen, Transport- und Verkehr sowie Siedlungsabfallentsorgung.

[3] Angesichts der Entwicklungen der letzten Jahre mit einer zunehmenden Bedrohung der digitalen Sicherheit einerseits und der fortschreitenden Digitalisierung andererseits forciert die EU mit ihrer aktuellen Cybersicherheitsstrategie[4] eine Verbesserung des EU-weiten Sicherheitsniveaus. Als ein wesentliches Element dieser Strategie legte die EU-Kommission im Dezember 2020 einen ersten Entwurf für eine NIS-2-Richtlinie vor.[5] Nach einem knapp zwei Jahre andauernden Gesetzgebungsverfahren wurde die finale Version der NIS-2-Richtlinie am 27. Dezember 2022 im Amtsblatt der EU veröffentlicht.

[4] In Kraft getreten ist diese im Januar 2023, die Umsetzungsfrist endet am 17. Oktober 2024. Zur nationalen Umsetzung der Richtlinie liegt seit dem 24. Juli 2024 ein Entwurf der Bundesregierung für ein „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" (NIS2UmsuCG) vor, dessen Artikel 1 ebenfalls als maßgebliches Element eine Novellierung des BSIG vorsieht.[6] Seit dem 16. August 2024 läuft das parlamentarische Gesetzgebungsverfahren hierzu.[7] Eine wesentliche Änderung zur bisherigen Rechtslage liegt im deutlich erweiterten Anwendungsbereich der Richtlinie: Zum einen werden mehr Sektoren und Branchen erfasst – u. a. auch der Maschinenbau. Zum anderen wird jetzt zwischen wesentlichen und wichtigen Einrichtungen differenziert, wozu neben Betreibern kritischer Anlagen auch zahlreiche große und mittlere Unternehmen zählen; Unternehmen ab 50 Mitarbeitenden oder 10 Mio. Euro Jahresumsatz werden bereits erfasst.[8] Der Begriff der Kritischen Infrastruktur wird ersetzt durch die Kritische Anlage, die weiterhin besonders strengen Pflichten unterliegt.[9] Diese Anlagen stehen nicht mehr selbst im Fokus der neuen Regelungen, sondern ihre jeweiligen Betreiber, denen bereits bekannte, aber auch neue Pflichten auferlegt werden. Für die KRITIS-Betreiber werden neben den neuen Vorgaben aus dem NIS2UmsuCG die derzeit parallel erarbeiteten Anforderungen des KRITIS-Dachgesetzes greifen, das in Umsetzung der CER-Richtlinie erlassen werden wird.[10]

[5] Wie notwendig eine Stärkung der Cybersicherheit in deutlich mehr Unternehmen ist, zeigen aktuelle Studien, insbesondere der aktuelle BSI-Lagebericht 2023: Die Lage ist angespannt wie noch nie. Zunehmenden Angriffen stehen zunehmende Sicherheitslücken in der verwendeten Software gegenüber. Während die meisten Schadprogramme die Büronetze allgemein angreifen, wurden in einem Fall sogar Spezial-Schadprogramme wie Industroyer2 für Prozesssteuerungsanlagen entdeckt.[11]

II. Adressaten aus dem Bereich des Maschinen- und Anlagenbaus

[6] Mit der Erweiterung des Adressatenkreises durch die NIS-2-Richtlinie und damit auch mit Artikel 1 des NIS2UmsuCG, der das BSIG novelliert („BSIG-E"), einher geht auch eine neue Bedeutung des Informationssicherheitsrechts für den Maschinen- und Anlagenbau. Eine Hilfestellung für eine erste Betroffenheitsanalyse bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI).[12] Die Adressaten der Vorgaben des BSIG-E werden in § 28 BSIG-E legaldefiniert: Besonders wichtige Einrichtungen nach Absatz 1 der Norm und wichtige Einrichtungen nach Absatz 2. Adressiert sind damit insbesondere Unternehmen aus den in Anlage 1 oder Anlage 2 BSIG-E gelisteten Sektoren, wenn diese 50 oder mehr Mitarbeitende beschäftigen oder einen Jahresumsatz oder eine Jahresbilanzsumme von über 10 Mio. Euro aufweisen.

[7] Bei der Bestimmung von Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme ist gem. § 28 Abs. 3 BSIG-E auf die der Ein-

1) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.
2) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148.
3) Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, BGBl. 2017 I Nr. 40, S. 1885.
4) Strategie abrufbar unter digital-strategy.ec.europa.eu/de/policies/cybersecurity-strategy (zuletzt abgerufen am 12. September 2024).
5) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final.
6) Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (im Folgenden: Regierungsentwurf), abrufbar unter: www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 12. September 2024).
7) BR-Drs. 380/24.
8) Kipker/Dittrich, MMR 2023, 481 (482).
9) Kipker/Dittrich, MMR 2023, 481.
10) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates; KRITIS-Dachgesetz derzeit offiziell vorliegend im Referentenentwurf vom 21. Dezember 2023, www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG-2.pdf;jsessionid=4A928A7B113E7604CAB2A4BBF513FFDC.live871?__blob=publicationFile&v=5 (zuletzt abgerufen am 12. September 2024). Parallel dazu kursiert derzeit ein inoffiziell verbreiteter Entwurf vom 10. April 2024.
11) www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410 (zuletzt abgerufen am 12. September 2024).
12) www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html (zuletzt abgerufen am 12. September 2024).

richtungsart zuzuordnende Geschäftstätigkeit abzustellen und gem. der Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 auch die jeweilige Kennzahl verbundener Unternehmen mit einzubeziehen: Gem. Art. 3 Abs. 2-3 Anhang zur Empfehlung sind verbundene Unternehmen und Partnerunternehmen gemeinsam zu betrachten. Dies sind Unternehmen mit kontrollierendem Einfluss, sei es wegen einer Beteiligung von über 25 % oder anderen Kontrollrechten.

[8] Adressiert wird als wichtige Einrichtung die juristische Person, die entsprechende Waren oder Dienstleistungen in dem gelisteten Sektor anbietet. Eine generelle Differenzierung danach, ob überwiegend eine bestimmte Leistung erbracht wird, ist nicht vorgesehen. Für die Adressierung des Unternehmens insgesamt ist es mithin bereits ausreichend, wenn auch Leistungen aus einem Segment gem. Anlage 1 oder 2 erbracht werden. Allerdings sollen die Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nicht über das gesamte Unternehmen berechnet werden, wenn nur ein Teilbereich im adressierten Sektor – also etwa dem Maschinenbau – tätig ist: „Bei der Bestimmung der maßgeblichen Mitarbeiterzahlen und des Umsatzes sind nur diejenigen Teile der Einrichtung einzubeziehen, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind, Querschnittsaufgaben wie beispielsweise Personal, Buchhaltung etc. sind hierbei anteilig zu berücksichtigen. Hierdurch wird sichergestellt, dass Einrichtungen, die insgesamt die Größenschwelle für Mitarbeiteranzahl, Jahresumsatz oder Jahresbilanzsumme überschreiten, deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 … zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden."[13]

1. Maschinenbau nach NACE Rev. 2

[9] Anlage 1 BSIG-E listet insbesondere die Sektoren, die auch bisher schon als KRITIS adressiert waren, nun mit teils niedrigeren Schwellenwerten. Für den Maschinen- und Anlagenbau ist dies von neuer Relevanz, wenn danach adressierte Unternehmen beliefert werden.[14] Unmittelbar adressiert wird in Anlage 2 BSIG-E neben etlichen anderen Sektoren in Nr. 5.4 der „Maschinenbau", legaldefiniert in Nr. 5.4.1 als „Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben".

[10] Die NACE Rev. 2 wurde durch Verordnung (EG) Nr. 1893/2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige eingeführt und dient zuvörderst statistischen Zwecken. Für die Bestimmung des Anwendungsbereiches des neuen BSIG-E wird sie erst über die konkrete Verweisung relevant. Elementar ist dann, dass eine Qualifikation einheitlich für ein Unternehmen erfolgt – in anderem Kontext getroffene Festlegungen müssen einheitlich auch für die Klassifizierung unter dem neuen BSIG-E erfolgen (oder – begründet – insgesamt revidiert werden).

[11] Erfasst ist in diesem Abschnitt die Herstellung von Maschinen für diverse Einsatzbereiche bis hin zum Auffangtatbestand in 28.99 NACE Rev. 2: „Herstellung von Maschinen für sonstige bestimmte Wirtschaftszweige", die anderweitig nicht genannt sind.

[12] Im Bereich des Maschinenbaus bestimmt sich die Klassifizierung damit letztlich ausschließlich nach der Größe: Unternehmen im Bereich des Maschinenbaus sind gem. § 28 Abs. 2 Satz 1 Nr. 3 i.V. m. Anlage 2 Ziff. 5.4 BSIG-E wichtige Einrichtungen, wenn sie im Geschäftsbereich Maschinenbau mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Mio. Euro aufweisen.

2. Lieferkette

[13] Auch unabhängig von einer unmittelbaren Adressatenstellung unter dem BSIG-E kommt eine Verpflichtung von Unternehmen nach dem neuen Recht in Betracht: Besonders wichtige und wichtige Einrichtungen nach § 28 BSIG-E müssen nach § 30 BSIG-E insbesondere ein Risikomanagement sicherstellen. Dies umfasst nach Absatz 2 Nr. 4 der Norm u. a. die „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern".

[14] Wenn mithin etwa ein Unternehmen aus dem Anlagenbau oder ein Zulieferer Adressaten unter dem BSIG-E beliefert, sollte sich auch dieses Unternehmen materiell auf verschärfte Anforderungen einstellen. Diese werden dann allerdings vom Vertragspartner zivilrechtlich auferlegt und nicht als gesetzliche, bußgeldbewehrte Pflicht aus dem BSIG-E. Trotz entsprechender Forderungen im Gesetzgebungsverfahren[15] ist eine gesetzliche Verpflichtung in der Lieferkette, wie sie etwa im Datenschutzrecht aus Art. 28 DSGVO bekannt ist, nicht aufgenommen worden.

[15] Das unmittelbar vom BSIG-E adressierte Unternehmen muss für seine Lieferkette im Rahmen des nach § 30 BSIG-E verpflichtenden Risikomanagements ein sog. „Cyber-Supply Chain Risk Management" vorsehen, kurz C-SCRM. Welche Anforderungen hier konkret erforderlich sind, ist vom Einzelfall abhängig. Das BSI hat etwa aktuelle Technische Richtlinien für den Erwerb von Software veröffentlicht.[16] Diese konturieren den Stand der Technik zur Absicherung in der Lieferkette aus Sicht des BSI für dieses Produkt. Anbieter von Software, die ihre Produkte an Adressaten unter dem BSIG-E vertreiben, müssen sich auf entsprechende Anforderungen einstellen. Aber auch außerhalb dieses Bereiches zeigen die Richtlinien beispielsweise Zulieferern für Maschinenbauunternehmen, welche Risikomanagementanforderungen auf sie in der Lieferkette zukommen können, wenn ihre Kunden die Anforderungen des BSIG-E umsetzen. Weitere, allgemeinere Anhaltspunkte ergeben sich auch aus dem BSI-Standard 200-4 zu Outsourcing und Lieferketten. Danach ist es erforderlich, an alle Unternehmen in der Lieferkette solche Anforderungen an das Business Continuity Management zu stellen, die die eigene Arbeitsfähigkeit absichern. Zu

13) Regierungsentwurf, Stand 22.7.2024, Zu § 28, Zu Absatz 3, S. 156.
14) Zu den Anforderungen an das Risikomanagement in der Lieferkette noch sogleich, II. 2.
15) Etwa vom DAV, Stellungnahme Nr. 37/2024, S. 4 ff. für sog. Auslagerungsunternehmen, www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/CI1/NIS-2-umsetzungs-cybersicherheit/NIS2UmsuCG070524_DAV_pdf.pdf;jsessionid=8AD3448562F5007335C76225BD548844.live872?__blob=publicationFile&v=3 (zuletzt abgerufen am 12. September 2024).
16) BSI-TR-03183, abrufbar unter www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html (zuletzt abgerufen am 12. September 2024).

erwarten sind vertragliche Pflichten zur Bereitstellung notwendiger Ressourcen und zur Durchführung eigener hinreichender Risikomanagementprozesse einschließlich Notfallplänen, umfassender Informationspflichten und weitreichender Berechtigungen zu regelmäßigen Audits inklusive Penetrationstests u. ä.

III. Informationssicherheitspflichten für den Maschinen- und Anlagenbau

[16] Fällt ein Unternehmen in den Anwendungsbereich des BSIG-E, sind je nach Klassifizierung als KRITIS, besonders wichtige oder wichtige Einrichtung unterschiedliche Pflichten zu erfüllen. Diese umfassen stets Registrierungspflichten, Vorgaben zum Risikomanagement und Meldepflichten, die Umsetzung wird durch begleitende Pflichten abgesichert. Für die im Maschinen- und Anlagenbau häufigen wichtigen Einrichtungen gelten im Vergleich zu den besonders wichtigen Einrichtungen, die auch KRITIS umfassen, niederschwellige Pflichten.

1. Risikomanagementmaßnahmen

[17] Kern des neuen Pflichtenkreises ist die Implementierung angemessener Risikomanagementmaßnahmen nach § 30 BSIG-E. Besonders wichtige Einrichtungen und wichtige Einrichtungen sind nach Absatz 1 Satz 1 der Norm „verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen … zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten". Diese Maßnahmen beziehen sich auf „sämtliche informationstechnischen Systeme, Komponenten und Prozesse …, die von der jeweiligen Einrichtung für die Erbringung ihrer Dienste genutzt werden". Als Diensteerbringung sollen dabei „sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden", verstanden werden.[17] Das Risikomanagement ist auf Ebene der gesetzlichen Verpflichtungen neu, in der Sache aber angelehnt an die bekannten Maßnahmen aus der ISO27001-Zertifizierung und den IT-Grundschutz des BSI. Niederschlagen muss sich das Risikomanagement in das interne Compliance-System, welches als Dach der insgesamt notwendigen Prozess- und Strukturmaßnahmen dienen kann.

[18] Die Umsetzung der Risikomanagementmaßnahmen ist von der Geschäftsleitung zu überwachen, die für Verletzungen ihrer Überwachungspflicht haften muss; § 38 BSIG-E etabliert damit den sog. Cyber-Vorstand und erhebt das Risikomanagement zweifelsfrei zur organspezifischen Pflicht. Damit die Geschäftsleitung diese Pflicht auch erfüllen kann, ist sie nach § 38 Abs. 3 BSIG-E zur Schulung verpflichtet.

2. Registrierungspflichten

[19] Besonders wichtige Einrichtungen und wichtige Einrichtungen sind nach § 33 Abs. 1 BSIG-E verpflichtet, sich zu registrieren. Übermittelt werden müssen neben Name und Anschrift der relevante Sektor, die geographischen Tätigkeitsbereiche und die Aufsichtsbehörden. Das Verfahren wird nach § 33 Abs. 6 BSIG-E vom BSI im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegt und auf der Homepage veröffentlicht.

3. Melde- und Unterrichtungspflichten

[20] Besonders wichtige und wichtige Einrichtungen müssen erhebliche Sicherheitsvorfälle dem BSI melden, § 32 BSIG-E. Ein erheblicher Sicherheitsvorfall ist ein Sicherheitsvorfall, der (a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder (b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann (§ 2 Nr. 11 BSIG-E). Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden, oder kriminelle Handlungen, wie zB Angriffe auf Server, der Diebstahl von vertraulichen Informationen sowie Sabotage oder Erpressung mit IT-Bezug.[18]

[21] Die Meldepflicht gliedert sich in eine frühe Erstmeldung nach spätestens 24 Stunden, die reguläre Meldung nach spätestens 72 Stunden und die Abschlussmeldung nach spätestens einem Monat. Die Meldepflicht besteht isoliert neben weiteren Meldepflichten, insbesondere nach Datenschutzvorfällen gem. Art. 33 DSGVO. Mit jeder Meldung muss die Informationsdichte erhöht werden. In der frühen Erstmeldung fokussiert sich die Meldung auf Angaben zu etwaigen Anhaltspunkten auf rechtswidrige oder böswillige Handlungen und mögliche grenzüberschreitende Auswirkungen. In der Meldung nach 72 Stunden kommt dann eine erste Bewertung des Sicherheitsvorfalls hinzu, in der u. a. Hinweise zu Schweregrad und Auswirkungen zu geben sind. Die Abschlussmeldung muss dann eine ausführliche Beschreibung des Vorfalls, Angaben zur Art der Bedrohung und der Ursache, den Abhilfemaßnahmen und den Auswirkungen enthalten.

[22] Bei erheblichen Sicherheitsvorfällen kann das BSI anordnen, dass die Kunden unterrichtet werden, § 35 BSIG-E. Auch diese Pflicht besteht isoliert von und parallel zu Art. 34 DSGVO.

4. Risiken bei Pflichtverletzungen: Von Anordnungs-, Untersagungs- und Bußgeldrisiken

[23] Das BSI ist befugt, die Umsetzung der Pflichten zum Risikomanagement, zu Meldungen und Schulungen des Cyber-Vorstands auch ggü. wichtigen Einrichtungen durchzusetzen, § 62 BSIG-E. Die Befugnisse des BSI ggü. besonders wichtigen Einrichtungen sind gem. § 61 BSIG-E noch weitreichender. Diese zentralen Pflichten des BSIG-E sind gem. § 65 BSIG-E auch mit Bußgeldern belegt, mit bis zu 7 Mio. Euro oder 1,4 % des Jahresumsatzes für wichtige Einrichtungen.

IV. Praktische Hinweise für die Umsetzung in Industrie- und Infrastrukturprojekten

[24] Die praktische Umsetzung von Cybersecurity-Maßnahmen im Maschinen- und Anlagenbau erfordert eine umfassende Betrachtung der oben beleuchteten Aspekte. Soweit Handeln erforderlich ist als unmittelbar betroffenes Unternehmen oder mittelbar innerhalb der Lieferkette, steht übergeordnet zunächst die Einrichtung

17) Regierungsentwurf, Stand 22.7.2024, Zu § 30, Zu Absatz 1, S. 160.
18) DER.2.1: Behandlung von Sicherheitsvorfällen (bund.de), abrufbar unter www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2021.pdf?__blob=publicationFile&v=2 (zuletzt abgerufen am 12. September 2024).

einer Projektgruppe, die durch den Cyber-Vorstand eingerichtet werden muss (siehe III. 1.). Die Experten sollten aus verschiedenen Fachrichtungen innerhalb des Unternehmens zusammengestellt werden (zB Compliance, IT, Recht, aber auch Experten für physische Gebäudesicherheit).

[25] Im Einzelnen erforderlich werden können im Rahmen einer individuellen Bedarfsanalyse beispielsweise die Überarbeitung bestehender Sicherheitssysteme, die physische und rechtliche Integration von Komponenten unterschiedlicher Hersteller und die Sicherstellung der Zukunftssicherheit. Dabei muss auch die Größe des Unternehmens berücksichtigt werden, um Maßnahmen effektiv und effizient umsetzen zu können.

[26] Vor dem Hintergrund sich ständig weiterentwickelnder rechtlicher Rahmenbedingungen sowie dem rasanten technologischen Fortschritt ist die Gewährleistung der Zukunftssicherheit essentiell in Projekten mit langer Lebensdauer. Unternehmen müssen langfristige Cybersecurity-Strategien entwickeln. Um bestehende Sicherheitssysteme auf dem neuesten Stand zu halten, sollten Unternehmen regelmäßige Sicherheitsaudits (intern und extern) durchführen. Insbesondere müssen Technologien wie Firewalls, Intrusion Detection Systems (IDS)[19] (zB auch durch Implementierung eines Patch-Management-Systems) stetig beobachtet und aktualisiert werden. Der Einsatz von Virtual Patching kann eine temporäre Lösung bieten, bis umfassendere Nachrüstungen durchgeführt werden können. Anlagen sollten zudem darauf ausgerichtet werden, dass veraltete Komponenten vereinfacht ausgetauscht werden können.

[27] Gleichzeitig erfordert die oftmals in Maschinen- und Anlagenbauprojekten notwendige physische und rechtliche Integration von Komponenten unterschiedlicher internationaler Hersteller eine sorgfältige Planung und Umsetzung. Neben entsprechenden klaren vertraglichen Regelungen und Audits, können Sicherheits-Gateways und Protokollkonverter unterstützen, unterschiedliche Sicherheitsstandards zu harmonisieren und zu überwachen. Bei der Durchführung hilft es, eine eigene Stabsstelle für die Überwachung einzurichten.

[28] Schließlich muss die Größe des Unternehmens bei der Umsetzung aller Maßnahmen berücksichtigt werden. Kleine und mittelständische Unternehmen sollten auf Arbeitsgruppen und skalierbare Sicherheitslösungen setzen und bei Bedarf externe Experten hinzuziehen, um spezialisierte Sicherheitskompetenzen zu integrieren. Managed Security Services können hierbei eine kosteneffiziente Möglichkeit bieten, umfassende Sicherheitsmaßnahmen zu implementieren. Als Best-Practice bei größeren Unternehmen wird sich die Erweiterung der Rechtsabteilung oder des IT-Sicherheitsteams erweisen.

[29] Eine besondere Herausforderung ergibt sich zudem daraus, dass das BSIG-E keine individuellen Regelungen für Unternehmensgruppen mit diversen verbundenen Unternehmen enthält: Jedes vom BSIG-E adressierte Unternehmen einer Unternehmensgruppe ist individuell registrierungspflichtig und bei Sicherheitsvorfällen meldepflichtig. Die Durchführung des Risikomanagements und die Implementierung der entsprechenden Prozesse und Maßnahmen kann indes dennoch in der gesamten Unternehmensgruppe erfolgen und lässt sich so oftmals auch einfacher umsetzen.

[30] Im Falle einer konkreten Cyberattacke sind die notwendigen Maßnahmen sehr individuell und können hier nicht abschließend beleuchtet werden.[20] Entscheidend ist es, bereits vor Eintritt eines Cybervorfalls eine klare Strategie zu haben. Hierzu sollte ein Incident-Response-Team eingerichtet werden, das schnell auf Bedrohungen reagieren kann. Darüber hinaus sollte jeder IT-Anwender entsprechend geschult sein.[21]

V. Fazit und Ausblick

[31] Durch eine ganzheitliche Herangehensweise können Unternehmen im Maschinen- und Anlagenbau ihre Cybersecurity-Strategien effektiv stärken und den Anforderungen der NIS2-Richtlinie und ihrer Umsetzung im BSIG-E gerecht werden. In den kommenden Beiträgen werden wir tiefer in spezifische Maßnahmen zur Verbesserung der Cybersecurity eintauchen, einschließlich detaillierter Fallstudien und Best Practices. Wir werden auch rechtliche Implikationen und praxisnahe Lösungsansätze für den Maschinen- und Anlagenbau betrachten, um ein umfassendes Verständnis und konkrete Handlungsanweisungen zu bieten.

19) www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/IDS02/gr1_htm.html (zuletzt abgerufen am 12. September 2024).
20) Weitergehende Hinweise: www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/TOP-12-Massnahmen/top-12-massnahmen_node.html (zuletzt abgerufen am 12. September 2024).
21) Auch hilfreich kann eine sog. „IT-Notfallkarte" sein: www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html (zuletzt abgerufen am 12. September 2024).