STELLUNGNAHME

VGMS
Verband der Getreide-, Mühlen- und Stärkewirtschaft VGMS e.V.

Neustädtische Kirchstraße 7A
10117 Berlin

www.vgms.de | info@vgms.de
T 030 212 33 69-0 | F 030 212 33 69-99

Präsidium:
Jochen Brüggen, Gustav Deiters, Michael Gutting, Ralph Seibold

Geschäftsführung:
Dr. Peter Haarbeck

AG Charlottenburg VR 35572 B
Lobbyregister R003156

Berlin, 28. Mai 2024

Stellungnahme zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung – NIS2-UmsuCG

Die Sicherheit der eigenen IT-Infrastruktur und der Schutz vor Angriffen jeglicher Art ist wichtiges Anliegen aller Unternehmen, die sie im Eigeninteresse verfolgen. Dabei wird der Schutz vor Cyberangriffen immer wichtiger. Durch die Vernetzung von Wirtschaft, Gesellschaft und Verwaltung ist die Abwehr solcher Risiken aber vor allem auch eine wichtige gesamtgesellschaftliche Aufgabe. Der *Bundesverband der Deutschen Industrie (BDI)* hat eine sehr umfangreiche Stellungnahme zum Entwurf erstellt, die wir vollumfänglich teilen und unterstützen. Darüber hinaus sind für uns folgende Punkte wichtig:

Angesichts der stetig steigenden Cyberbedrohungslage unterstützten wir grundsätzlich die Bestrebungen, die Cyberresilienz von Staat und Wirtschaft durch das *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2-UmsuCG)* nachhaltig zu verbessern.

Dabei darf aber die Abwägung zwischen potentiellem Risiko und potentiellem Schaden auf der einen und den Kosten und der weiter steigenden Bürokratie auf der anderen Seite nicht unterbleiben. Die massive Ausweitung des Anwendungsbereiches der NIS-2-Richtlinie auf bis zu 40.000 Unternehmen ist grundsätzlich zu hinterfragen. Praxisnähe und Umsetzbarkeit müssen oberste Prämisse bei der Umsetzung des Gesetzes bleiben.

Anwendungsbereich der gesetzlichen Regelung

Die Getreide-, Mühlen- und Stärkewirtschaft ist mittelständisch geprägt. Die aktuelle Gesetzgebung (BSI-Gesetz, Kristis-VO) hat bislang nur einzelne Standorte der im VGMS zusammengeschlossenen Unternehmen betroffen. Unsere Unternehmen gehören zu der Gruppe der *„wichtigen Einrichtungen"*. Die neuen Größenklassen für die Betroffenheit bei Umsatz, größer 10 Millionen Euro, und Mitarbeitern, mehr als 50, werden zu einer deutlichen Ausweitung der betroffenen Unternehmen auch in der Getreide-, Mühlen- und Stärkewirtschaft führen. Für uns ist es daher unabdingbar, die Betroffenheit zu konkretisieren:

So sind richtigerweise *Handwerksbetriebe der Lebensmittelwirtschaft*, egal welcher Größe aus dem Anwendungsbereich des Umsetzungsgesetzes ausgenommen. In Anlage 2, Punkt 4.1.1. des *Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)* – Entwurf sind nur Lebensmittelunternehmen nach Artikel 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates, die im Großhandel sowie *in der industriellen Produktion und Verarbeitung t*ätig sind, betroffen.

Für kleine Betriebe der Getreide-, Mühlen- und Stärkewirtschaft, die nicht dem Handwerk angehören, stellt sich die Frage, ob der *Gesamtumsatz des Unternehmens* zugrunde gelegt wird, um in den Anwendungsbereich des Gesetzes zu fallen oder nur der Umsatz, der tatsächlich mit der *Produktion des Lebensmittels* generiert wird. Diese Betriebe erzielen einen Teil ihres Umsatzes über die Vermarktung von Futtermitteln oder durch den Betrieb eines „Mühlenladens", also im Einzelhandel.

Weiter ist zu fragen, ob Unternehmen, die an einem Standort Lebensmittel und Grundstoffe für die chemische Industrie herstellen, als ein Standort bewertet oder ob die jeweiligen Umsätze getrennt betrachtet werden. Diese Fragen werden unzureichend im Gesetzesentwurf beantwortet. Konkrete Abgrenzungskriterien sind für einen sicheren Vollzug allerdings notwendig.

Eins-zu-Eins-Umsetzung geboten

Bei der Umsetzung der EU-Richtlinie sollte, wie eigentlich in jedem Fall, eine Eins-zu-Eins-Umsetzung in deutsches Recht erfolgen, insbesondere und gerade mit Blick auf den Anwendungsbereich. Gerade für europaweit tätige Unternehmen ist eine europaweit einheitliche Umsetzung der NIS-2-Richtlinie in nationales Recht unabdingbar. Jeder Mehraufwand, der durch *nationale Alleingänge* bei der Umsetzung entsteht, ist für die Wirtschaft in Deutschland kontraproduktiv und in jedem Fall zu vermeiden.

Bußgeldrahmen zu hoch

Die Umsetzungsfrist der EU-Richtlinie läuft in weniger als sechs Monaten aus. Die Zeit zwischen Vorstellung des Entwurfs und in Krafttreten des deutschen Umsetzungsgesetzes sowie der Ablauf der Umsetzungsfrist ist viel zu knapp bemessen. Die Unternehmen, die durch die zeitgleiche Einführung und Umsetzung vieler weiterer neuer Regelungen bereits stark belastet sind, zu nennen sind hier die anstehenden Umsetzung der EU-Industrieemissionsrichtlinie, Regelungen im Kontext des Lieferkettengesetzes oder die Nachhaltigkeitsberichterstattung, stoßen hier an Grenzen, die eine gründliche Implementierung verunmöglichen. Dies gilt insbesondere für die vielen kleinen und mittleren Unternehmen. Auch ist festzuhalten, dass bei der Umsetzung der Maßnahmen KMU nicht auf eigene Fachleute zurückgreifen können, sondern Dienstleistungen extern einkaufen müssen. Die Verfügbarkeit dieser Fachkräfte ist jedoch stark beschränkt. Hinzu kommen Kostensteigerungen aufgrund des Fachkräftemangels. Mit Blick auf die drohenden, viel zu hoch angesetzten Bußgelder, ist eine praktikable Übergangsregelung durch den Gesetzgeber dringend geboten.

Die Bußgelddrohungen in § 61 BSIG sind absurd hoch. Für „wichtige Unternehmen" werden bis zu sieben Millionen Euro Bußgeld angedroht. Da bereits Unternehmen mit einem Jahresumsatz und einer Jahresbilanzsumme

von jeweils über 10 Millionen Euro in den Anwendungsbereich des Gesetzes fallen, sind solche Bußgelder existenzbedrohend.

Einbeziehung der öffentlichen Verwaltung geboten

Es fällt auf, dass eine Umsetzung der NIS-2-Richtlinie in der öffentlichen Verwaltung nicht geplant ist. Dies ist aus zweierlei Sicht nicht akzeptabel: Zum einen sind die Unternehmen auf eine funktionierende Verwaltung angewiesen. Sicherheitsmaßnahmen, wie sie der Wirtschaft auferlegt werden, sollten auch dazu beitragen, die IT-Sicherheit der Verwaltung robuster zu machen. Legen erfolgreiche Cyberattacken, wie sie in der Vergangenheit mehrfach zu beobachten gewesen sind, die Verwaltung lahm, sind alle gesellschaftsrelevanten Gruppen wie die Wirtschaft indirekt oder direkt betroffen, wenn Prozesse nicht mehr durchgeführt werden können.

Zum anderen trägt es zum wechselseitigen Verständnis bei, wenn die öffentliche Verwaltung die selben Maßnahmen umsetzen muss. Insbesondere die damit verbundene Bürokratie und etwaige Fallstricke bei der Umsetzung können so behördenseitig quasi hausintern verfolgt werden.

Daher sollten neben Bundesbehörden auch Behörden der Länder und Kommunen – insbesondere Genehmigungs- und Überwachungsbehörden, die sensible Daten verarbeiten und für besonders wichtige und wichtige Einrichtungen essenzielle Verwaltungsleistungen erbringen – als *besonders wichtige Einrichtungen* definiert werden und somit in den Anwendungsbereich des Gesetzes fallen.

Hinzu kommt, dass im Bereich der Genehmigung von Anlagen und der Anlagensicherheit, sowohl IT- als auch Betriebstechnologie (OT)-Sicherheit, Sicherheitsfragen im Zuge der Digitalisierung der Genehmigungsprozesse immer wichtiger werden. So müssen künftig zwingend sämtliche Antragsunterlagen im Rahmen der Öffentlichkeitsbeteiligung im Internet veröffentlicht werden (vgl. § 10 Abs. 3, S. 2 BImSchG (Neufassung m.W.v. 16.04.2024), § 27a VwVfG). Aus dem Blickwinkel der Cybersicherheit stellt das derzeit in den meisten Bundesländern angewandte elektronische Antragstellungsprogramm keinen umfassenden digitalen Prozess dar und hat erhebliche Mängel. Daher sollten einheitliche, klare Strukturen und Zuständigkeiten sowie praxisgerechte, sichere und vollständig digitale Prozesse etabliert werden. Darüber hinaus sollten die zuständigen Behörden, insbesondere das BSI, so fachlich und personell gestärkt werden, dass sie ihrer Beratungsfunktion auch tatsächlich gerecht werden können.

Weitergabe von Informationen an die Unternehmen

Das Umsetzungsgesetz legt den Unternehmen zahlreiche Dokumentations- und Berichtspflichten auf. Diese sind jedoch in diesem Umfang nur dann sinnvoll und zu rechtfertigen, wenn die so gewonnen Informationen zeitnah den Unternehmen wieder zur Verfügung gestellt werden, in Form von qualitativ hochwertigen Datensätzen zur Cybersicherheitslage. Diese Rückkoppelung muss zeitnah erfolgen, damit Unternehmen frühzeitig potentiellen Gefahren und Angriffe gewahr werden und diese abwehren können.

Vermeidung von Mehrfachprüfungen

Zum Ende möchten wir noch auf einen wesentlichen Aspekt hinweisen. Die Anzahl der durchzuführenden Audits in den Unternehmen steigt stetig, weil

der Gesetzgeber immer mehr entsprechende Vorgaben macht. Neben diesen Audits sind zwingend widerkehrende Prüfungen durchzuführen. Auch deren Anzahl erhöht sich ständig. Verschiedene Regelwerke wie die *Störfallverordnung*, die *Betriebssicherheitsverordnung*, und nun auch das *NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz* sehen widerkehrende Prüfungen vor. Hier besteht die Gefahr von *unnötigen Mehrfachprüfungen.* Aus Kosten- und Effizienzgründen aber auch aufgrund der immer größer werdenden Lücke zwischen Prüfanforderungen und fehlenden sachkundigen Prüfern gilt es, diese Mehrfachprüfungen zu unterbinden.

Der Grund dafür liegt darin, dass Überprüfungen aus diversen Rechtsgebieten aus unterschiedlicher Motivation heraus für ursprünglich unterschiedliche technische Maßnahmen durchgeführt werden. Aus dem obigen Beispiel:

- Systeme der funktionalen Sicherheit zur Störfallvermeidung (Störfallverordnung)
- Systeme zur Aufrechterhaltung der Arbeitssicherheit (Betriebssicherheitsverordnung)
- Systeme zur Aufrechterhaltung von kritischen Dienstleistungen, die für die Gesellschaft notwendig sind (NIS-2 Richtlinie in Verbindung mit der KRITIS-Verordnung)

Neue Bedrohungssituationen durch „cyberphysische Angriffe" stellen alle drei Rechtsgebiete, die zugehörigen Organisationen und Management-Systeme vor die Herausforderungen, sich auf diese Bedrohung einzustellen. Die Architektur der digitalen Infrastruktur, die von diesen Rechtssystemen betroffen ist,

- orientiert sich weniger an den Grenzen der Rechtssysteme und
- wird durch immer stärkere Vernetzung geprägt (horizontale und vertikale Integration).

Fragen der *Cybersecurity* leiten sich primär aus Datenstrukturen, der Architektur der digitalen Infrastruktur und der zugehörigen Prozesse und Organisationen ab, nicht aus den Strukturen der oben genannten Rechtsgebiete. Umgekehrt muss *Cybersecurity* nach den Zielvorgaben der verschiedenen Rechtsgebiete ausgerichtet werden. Wenn ein digitalisiertes System eine Funktion nach Störfallverordnung realisiert und eine weitere Funktion nach Betriebssicherheitsverordnung und eine dritte Funktion die sowohl nach Störfall, als auch nach Betriebssicherheitsverordnung zu prüfen wäre, dann soll dieses System die Zielvorgaben aller Funktionen erfüllen. Die Einhaltung dieser Zielvorgaben sollte jedoch nur einmal und nicht zwei oder gar viermal geprüft werden müssen.

Damit Mehrfachüberprüfungen vermieden werden und Prüfergebnisse anderer Prüfer und oder anderer Prüf- und Rechtsgebiete anerkannt werden können, müssen sich Prüfungsorganisationen und Anwender auf einen Kompromiss einigen können. Der Gesetzgeber ist hier gefordert, entsprechende Abstimmungen zu ermöglichen. Es ist niemandem gedient, wenn Unternehmen den gesetzlichen Anforderungen nicht nachkommen können, weil überflüssige Prüfungen wegen nicht ausreichender Prüfkapazitäten nicht durchgeführt werden können.

Über den Verband der Getreide-, Mühlen- und Stärkewirtschaft VGMS

Im VGMS sind rund 500 Unternehmen organisiert, von mittelständischen, familiengeführten Unternehmen bis hin zu großen internationalen Konzernen. In den Betrieben werden rund 15 Millionen Tonnen landwirtschaftlicher Rohstoffe verarbeitet, unter anderem Weizen, Roggen, Hafer, Hartweizen, Mais, Reis und Stärkekartoffeln. Die Unternehmen sind wichtige Partner der Landwirtschaft sowie von Lebensmittelhandwerk, Industrie und Handel.

Die Produktpalette reicht von Mehl über Haferflocken, Frühstückscerealien, Nudeln und Reis bis zu nativen und modifizierten Stärken sowie Stärkeverzuckerungsprodukten. In Deutschland und darüber hinaus versorgen die Unternehmen Tag für Tag Millionen Menschen mit hochwertigen, sicheren und zugleich preiswerten Lebensmitteln. Daneben stellen sie Produkte für die chemisch-technische und pharmazeutische Industrie sowie Einzelfuttermittel für die Tierernährung her.

Mit ihren rund 15.000 Mitarbeiterinnen und Mitarbeitern erwirtschaften die im VGMS zusammengeschlossenen Branchen einen Umsatz von etwa 7,5 Milliarden Euro, mit ihren Produkten sind sie weltweit erfolgreich. Der VGMS vertritt ihre wirtschafts- und sozialpolitischen Interessen gegenüber deutschen und europäischen Institutionen.

Für ein Gespräch zur Verdeutlichung unserer Position stehen wir jederzeit zur Verfügung.

Ansprechpartner:

Andreas Bolte
Umwelt & Energie

T 030 2123369 36
E andreas.bolte@vgms.de