WIRTSCHAFTSRAT
Deutschland

Wirtschaftsrat der CDU e.V.

# Umsetzung der NIS-2-Richtlinie in Deutschland

Stellungnahme

*Die Stimme der Sozialen Marktwirtschaft*

**Wirtschaftsrat der CDU e.V.**
**Bereich Innovation und Digitales**
Luisenstr. 44
10117 Berlin
Tel.: +49 (0) 30 / 240 87 - 203
E-Mail: digitales@wirtschaftsrat.de

**Andreas G. Barke**
**Referent Innovation und Digitales**

Stand: 21.06.2023

# Stellungnahme
# zur Umsetzung der NIS-2-Richtlinie in Deutschland

Die **Network and Information Systems 2.0 Directive** (NIS-2-Richtlinie, NIS-2-RL)[1] hat als Gesetzgebung für die Europäischen Union (EU) das Ziel eine **ganzheitliche Stärkung der Cyber-Resilienz**, eine **höhere übergreifende Awareness** und ein **höheres und gemeinsames Niveau der Cybersicherheit** in den EU-Mitgliedsstaaten zu erreichen. In Deutschland erfolgt die **Implementierung in nationales Recht** durch das **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz** (NIS2UmsuCG).[2] Die hierfür gesetzte Frist sowie auch für die Umsetzung der betroffenen Einrichtungen ist der **17. Oktober 2024**.

Der **Wirtschaftsrat befürwortet** die Intention, die faktisch **unterschiedlichen Sicherheitsniveaus** in den EU-Mitgliedstaaten auf ein **einheitliches Level** zu heben. Wir unterstützen den Gedanken, **langfristig eine hohe Resilienz auch in die Breite unserer Wirtschaft** zu bringen. **Einheitliche Sicherheitsanforderungen** stellen für EU-weit agierende Unternehmen eine **erhebliche Erleichterung** dar, die entsprechenden **Anforderungen kohärent umzusetzen**. Sie tragen im Idealfall zu einer **geringeren Fragmentierung des digitalen Binnenmarktes** sowie zu einer **Reduktion von Wettbewerbsverzerrungen** bei.

**Der Wirtschaftsrat fordert die Bundesregierung auf, die Forderungen von Verbänden und Unternehmen bei der Umsetzung in nationales Recht zu berücksichtigen**.[3] Zuvorderst ist **Planungssicherheit für Unternehmen** sicherzustellen und die **Umsetzungsfristen** sind in einem **realistischen Zeitrahmen** mit Augenmaß klar zu definieren. In der Umsetzung sind außerdem **Überschneidungen und ungewollte Wechselwirkungen** verschiedener bestehender und angekündigter rechtlicher Vorgaben mit denen der NIS-2-Richtlinie im Sinne eines **möglichst geringen Erfüllungsaufwands für Unternehmen zu vermeiden**. Insbesondere **kleine und mittelständische Unternehmen** (KMU) sehen sich aufgrund noch unklarer Vorgaben im vorliegenden Entwurf des NIS2UmsuCG in bestimmten Fällen mit **übermäßigen Anforderungen und Risiken für die Geschäftspraxis** konfrontiert (z. B. vorgesehener Bußgeldrahmens und Managerhaftung). Ein „**Gold-Plating**"– also die Übererfüllung der EU-Vorgaben im Zuge der Umsetzung in nationales Recht – **sollte vermieden werden**.

Grundsätzlich kann die NIS-2-Richtlinie ihre volle Wirkung nur entfalten, wenn ihre Umsetzung vorausschauend in eine **konsistente und ganzheitliche Strategie** zur Verbesserung der Cybersicherheit in Deutschland als Teil der EU eingebettet wird. Wichtige Bausteine sind die Einführung **risikoadäquater Anforderungen** an Einrichtungen und Unternehmen, eine fortlaufende **Effizienzsteigerung** der vorhandenen und umzusetzenden Prozesse sowie die **Verstärkung der Kooperation von Staat und Wirtschaft** zum Ausbau des Cyberschutzes für den Industriestandort Deutschland. Die NIS-2-Richtlinie wurde vor der **politischen „Zeitenwende"** aufgrund des Kriegs in der Ukraine und der **signifikant verschärften Gefahrenlage** beschlossen. Umso wichtiger ist es nun, den **Einsatz von Kräften und Ressourcen auf Einrichtungen zu fokussieren**, die den **größten Cyberrisiken ausgesetzt** sind, also insbesondere auf Einrichtungen der **Kritischen Infrastrukturen (KRITIS)**. Die politisch-rechtliche Umsetzung an die sich veränderte Lage anzupassen, darf kein Tabu sein.

Der Implementierung der NIS-2-Richtlinie in nationales Recht muss also eine adäquate Einbindung von Verbänden, Unternehmen und Vertretern der Zivilgesellschaft vorausgehen. **Ziel ist eine fristgerechte, umfassende und nachhaltige Umsetzung der NIS-2-Richtlinie. Verbände, Unternehmen und Vertreter der Zivilgesellschaft möchten mitgestalten und produktiv im Interesse aller mitwirken!**[4]

## Forderungen des Wirtschaftsrates zur Umsetzung der NIS-2-Richtlinie in Deutschland:

**(1) Verantwortlichkeiten und Zuständigkeiten klären und ein hohes Niveau an Planungssicherheit für Unternehmen sicherstellen**

**(2) Umsetzungsfristen in einem realistischen Zeitrahmen klar definieren**

**(3) EU-weite Harmonisierung sicherstellen und Kategorisierung von Unternehmen möglichst einfach ausgestalten**

**(4) Automatisiertes und zentralisiertes Registrierungswesen, an den Bedürfnissen der Unternehmen ausgerichtet, möglichst effizient und digital angelegt**

**(5) Einheitliches, zentrales, praxisnahes und möglichst unbürokratisches Meldewesen mit Rückkanal installieren (im Sinne eines One-Stop-Shops)**

**(6) Lagebild als One-Stop-Shop für die digitale und analoge Sphäre in deutscher und englischer Sprache bereitstellen**

**(7) Verhältnismäßige, transparente und angemessene Kriterien für die Bemessung von Bußgeldern bei Verstößen einführen**

**(8) Vorgaben zur Managerhaftung beschränken**

**(9) Anordnungen weiterer regulatorischer EU-Sicherheitsanforderungen berücksichtigen und aufeinander abstimmen (z. B. CER, CRA, CSA)**

**(10) Rechtskonforme Überprüfung der Vertrauenswürdigkeit von Beschäftigten mit möglichst schnellen Bearbeitungszeiträumen ermöglichen (auf Basis einer eindeutigen Rechtsgrundlage)**

**(11) Klare Definition von Einrichtungen der öffentlichen Verwaltung mit eindeutigen und prüffähigen Merkmalen einführen**

**(12) Staatliche Unterstützung für Unternehmen (insbesondere KMU) mit rechtsverbindlichen und konkreten Umsetzungshilfen bereitstellen**

## (1) Verantwortlichkeiten und Zuständigkeiten

Es gilt in der Umsetzung und Anwendung der NIS-2-Richtlinie (sowie aller verwandten regulatorischen Maßnahmen) ein möglichst hohes Niveau an Rechts- und Planungssicherheit für Unternehmen in Deutschland sicherzustellen (siehe hierzu auch Forderung (12)). Im Zuge der Regulierung durch Behörden

und Bundesämter, wie z. B. dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) hinsichtlich des Dachgesetzes für Kritische Infrastrukturen (KRITIS-Dachgesetz), sind klare Verantwortlichkeiten und Zuständigkeiten zu schaffen, um unnötige und redundante Anforderungen an Unternehmen zu vermeiden und möglichst effiziente Verwaltungsverfahren zu implementieren.
Idealerweise sollte der bestehende Wildwuchs an Verantwortlichkeiten, Mitspracherechten und Zuständigkeitsfragen im Rahmen des Föderalismus abgebaut werden. Beispiele sind umständliche Meldewege und sich überlagernde Zuständigkeiten auf Bundes- und Landesebene in Cybernotfällen. Dem folgend sollten keine zusätzlichen landeseigenen Verwaltungsbehörden aufgebaut werden.[5] Im Sinne der Auftragsverwaltung soll sich der Bund den Kompetenzen der Länder bedienen können und eine zuständige Verwaltungsbehörde benennen.[6] Der bestehende und sich absehbar weiter verschärfende Fachkräftemangel erfordert einen möglichst ressourcenschonenden und gezielten Einsatz der existierenden Ressourcen auf Seiten der Unternehmen und der Behörden.[7]

Deutschland sollte die Umsetzung der NIS-2-Richtlinie zur Definition der behördlichen Zusammenarbeit und zur Optimierung der bestehenden Strukturen und Prozesse nutzen (siehe hierzu Nationale Sicherheitsstrategie der Bundesregierung vom 14. Juni 2023).[8]

### (2) Umsetzungsfristen mit realistischem Zeitrahmen

Die Umsetzungsfristen für die NIS-2-Richtlinie nach Verkündung und Inkrafttreten des Umsetzungsgesetzes sind möglichst schnell und klar zu regeln (siehe Erläuterungen zum regulatorischen/gesetzgeberischen Fahrplan auf Seite 12). In der Umsetzung gilt es die vorhandenen Ressourcen auf diejenigen Einrichtungen zu fokussieren, deren Beeinträchtigung im Falle eines erfolgreichen Cyberangriffs die vergleichsweise kritischsten Konsequenzen für Gesellschaft und Wirtschaft hätte, also insbesondere auf KRITIS.

Der zum aktuellen Stand vorgesehene Zeitrahmen von etwa sechs Monaten zwischen Verkündung und Inkrafttreten (März bis Oktober 2024) ist allein aufgrund des dramatischen Fachkräftemangels – sowohl für unternehmensinterne Mitarbeiter als auch bei den Beratern, die die konkrete Umsetzung in den Unternehmen begleiten könnten – kaum in Gänze von allen betroffenen Einrichtungen einzuhalten. Die Umsetzungsklausel NIS-2-Richtlinie (Art. 41 NIS-2-RL) sieht nach Ablauf der Umsetzungsfrist (17. Oktober 2024) keine daran anschließende Implementierungsphase für Behörden oder Unternehmen vor.[9]

Experten gehen davon aus, dass die Umsetzung in vielen betroffenen Einrichtungen und Unternehmen mindestens 12 bis 18 Monate dauern wird. Viele Einrichtungen müssten also de facto unmittelbar mit der Umsetzung beginnen, um zum Zeitpunkt der Meldung der nationalen Behörden gegenüber der EU-Kommission die Anforderungen erfüllt zu haben. Erschwerend kommt hinzu, dass nach Schätzung von Experten, bis zu 80 Prozent der von der NIS-2-Richtlinie betroffenen etwas 29.000 Unternehmen in Deutschland, derzeit noch gar nicht wissen, dass sie betroffen sind (siehe Forderung (4) Registrierungswesen).[10]

Um hier eine Entzerrung zu erreichen, empfehlen wir – gerade für KRITIS – der über den Kreis der vom IT-Sicherheitsgesetz 1.0 und 2.0 (IT-SiG 1.0 und IT-SiG 2.0) betroffenen Einrichtungen und Unternehmen hinausgeht, gestaffelte Umsetzungsfristen vorzusehen. Eine mögliche Staffelung könnte folgendermaßen ausgestaltet sein:

- Umsetzungsfrist bis Oktober 2024 für bereits vom IT-SiG 1.0 und IT-SiG 2.0 erfasste Einrichtungen (da diese Einrichtungen die geringsten Probleme in der Umsetzung haben dürften)
- Umsetzungsfrist bis Oktober 2025 für Einrichtungen mit mehr als 250 Mitarbeitern in besonders wichtigen Sektoren

- Umsetzungsfrist bis Oktober 2026 für Einrichtungen mit weniger als 250 Mitarbeitern in besonders wichtigen Sektoren und für Einrichtungen mit mehr als 250 Mitarbeiter in wichtigen Sektoren
- Umsetzungsfrist bis Oktober 2026 für Einrichtungen mit weniger als 250 Mitarbeitern in wichtigen Sektoren.

Eine solche Staffelung würde sowohl die aktuelle Gefährdungslage, den bestehenden Ressourcenmangel und den Reifegrad der Einrichtungen und Unternehmen berücksichtigen. Hierdurch würde eine unbedingt erforderliche risikoorientierte Umsetzung erfolgen. Ein sich möglicherweise ergebener Konflikt mit den Vorgaben der NIS-2-Richtlinie müssten von der Bundesregierung entsprechend politisch verarbeitet und begleitet werden.

Die Fristen zur Teilnahme am Informationsaustausch im Rahmen der Risikomanagementmaßnahmen (ein Jahr nach Inkrafttreten für besonders wichtige Einrichtungen gem. Art. 1 § 30 (10) NIS2UmsuCG) sowie die Fristen der Registrierungspflichten (drei Monate nach Inkrafttreten für wichtige und besonders wichtige Einrichtungen gem. Art. 1 § 32 (1) NIS2UmsuCG) wären ggf. entsprechend anzupassen. Bezugnehmend auf neu hinzugekommene kritische Anlagen könnte der im Umsetzungsgesetz genannte Stichtag ggf. ebenfalls angepasst werden (siehe Art. 1 § 28 (2b) NIS2UmsuCG).

### (3) EU-weite Harmonisierung und Unternehmenskategorien der NIS-2-Richtlinie und des IT-Sicherheitsgesetzes 2.0

Die NIS-2-Implementierung sollte sich so eng wie möglich am Anwendungsbereich der Vorgaben der NIS-2-Richtlinie orientieren. Darüber hinausgehende Sektoren sollten dem folgend nicht eingeführt bzw. fortgeführt werden. (Sub-)Sektoren, die auf EU-Ebene nicht als betroffene Einrichtungen gelistet sind, sollten aus dem Anwendungsbereich des NIS-2-Umsetzungsgesetzes herausgenommen werden. Dies bezieht sich z. B. auf den Logistiksektor. Dieser wird von der NIS-2-Richtlinie zutreffenderweise nicht als eigenständige Kategorie betrachtet. Insofern sollte der Logistiksektor nicht als eigenständiger Subsektor (entgegen der formulierten Einbeziehung in Art. 1 § 28 (4) 2 NIS2UmsuCG), sondern, wie in der BSI-Kritisverordnung (BSI-KritisV)[11] für bestimmte KRITIS-Bereiche angelegt, mittelbar innerhalb der Sektoren berücksichtigt werden (Beispiel Sektor Gesundheit: Anlage oder System zum Vertrieb von verschreibungspflichtigen Arzneimitteln).[12] Konkret ist hierbei der Querverweis in der Resilience of Critical Entities-Richtlinie (CER-Richtlinie)[13] auf „Betreiber intelligenter Verkehrssysteme“ zu klären (CER-Richtlinie, Anhang Sektoren 2. Verkehr d) Straßenverkehr), da entsprechende Logistikbetreiber (Luft- und Schifffahrt) teilweise für den NIS-2-Geltungsbereich erhalten bleiben.

Wie von diversen Verbänden in der jüngsten Vergangenheit gefordert, soll die Unterscheidung zwischen den Kategorien von Unternehmen im besonderen öffentlichen Interesse (UBI-Kategorien 1, 2 und 3), wie sie im IT-SiG 2.0 implementiert sind, im Zuge der Umsetzung der NIS-2-Richtlinie in Deutschland nicht mehr geführt werden. UBI sind bereits größtenteils in den betroffenen wesentlichen bzw. besonders wichtigen und wichtigen Einrichtungen enthalten.[14]

### (4) Automatisiertes und zentralisiertes Registrierungswesen

Jedes Unternehmen soll sich im Zuge der Umsetzung der NIS-2-Richtlinie zunächst selbst einschätzen und dann registrieren (Art. 1 § 30 u. § 32 NIS2UmsuCG). Für die Registrierung wird es voraussichtlich ein offizielles Internet-Portal geben (Art. 1 § 6 NIS2UmsuCG). Wesentlich ist eine möglichst automatisierte

Zurverfügungstellung von relevanten Informationen von staatlicher Seite gegenüber den betroffenen Unternehmen. Zur Selbsteinschätzung sollte es von staatlicher Seite ein kostenfreies und einfach zu bedienendes Online-Angebot geben (als Orientierung können „Quickcheck"-Angebote von privatwirtschaftlichen Unternehmen sowie Wirtschaftskammern in EU-Mitgliedsstaaten[15] dienen). Um die Erfüllungsaufwände für betroffene Einrichtungen und Unternehmen, die ihren Hauptniederlassung nicht in Deutschland sondern einem weiteren EU-Mitgliedsstaaten haben, möglichst gering zu halten, muss sichergestellt werden, dass diese nur einmalig eine entsprechende Bescheinigung ihrer jeweiligen zuständigen nationalen Behörde bei der in Deutschland zuständigen Behörde vorlegen müssen. Die Behörde in Deutschland kann die Vorlage einer neuerlichen Bescheinigung alle fünf Jahre einfordern (vgl. mit (5)).

Im Zuge des zeitgleichen Inkrafttretens und entsprechend der Umsetzung der NIS-2-Richtlinie sowie auch der CER-Richtlinie für KRITIS-Betreiber werden sich über die bisherigen Vorgaben des IT-SiG 2.0[16] hinausgehend weitere Unternehmen beim BSI sowie teilweise zusätzlich auch beim BBK selbst registrieren müssen. Diese Registrierungspflichten sollten an den Bedürfnissen der Unternehmen ausgerichtet und möglichst effizient und digital angelegt werden. Der Zugriff der zuständigen staatlichen Stellen sollte nach dem Need-to-know-Prinzip erfolgen. Die Bündelung aller relevanten Informationen zu einem Cybervorfall an einer zentralen Stelle hätte prozessuale Vorteile was die Effizienz und Effektivität anbelangt, soweit adäquate Sicherheitsstandards in der Informationsübertragung und -speicherung eingehalten werden (siehe in Forderung (5) Meldewesen geforderte Verpflichtung der Behörden zur Vertraulichkeit und zum Schutz der Unternehmens- und Kundendaten).

Aufgrund der hohen Zahl der voraussichtlich betroffenen Unternehmen (siehe Forderung (2) Umsetzungsfristen) sollte ein aktives Zugehen von Unternehmens- und Branchenverbänden auf Unternehmen in Erwägung gezogen werden.

## (5) Einheitliches, zentrales und praxisnahes Meldewesen[17]

Gemäß NIS-2-Richtlinie sollen betroffene Einrichtungen und Unternehmen mindestens drei und in bestimmten Fällen bis zu fünf Meldungen bzw. Berichte pro Cybersicherheitsvorfall vornehmen. Wir fordern einen möglichst einheitlichen, einfachen und digitalisierten Meldeweg, der in beide Richtungen läuft, also von betroffenen Unternehmen zu den Meldestellen und auch von den Meldestellen zu den Unternehmen (gem. Art. 1 § 36 (1) NIS2UmsuCG formal erfüllt, siehe auch Forderung (6) Lagebild als One-Stop-Shop). Im Sinne der Internationalisierung des Meldewesens auf organisatorischer und operativer Ebene sollten Meldungen sowohl in deutscher als auch englischer Sprache erfolgen können. Übergeordnete Ziele sind die Vereinfachung der unternehmensinternen Abstimmung der Meldungen und die grenzübergreifende Weitergabe von Informationen zwischen den Mitgliedsstaaten. Darüber hinaus sollte betroffenen Unternehmen im Zuge von Folge-Berichten stets Zugriff auf die bereits gemeldeten Informationen eingeräumt werden. Nachträglich sollten ggf. zusätzliche Eingaben und Korrekturen durch die Unternehmen möglich sein. Zwischenberichte sollten vom BSI und den Computer Security Incident Response Teams (CSIRTs) nur bei solchen Fällen eingefordert werden können, die einen entsprechenden Mehraufwand rechtfertigen.

Es muss in Abstimmung mit den weiteren EU-Mitgliedstaaten sichergestellt sein, dass betroffene Einrichtungen und Unternehmen, die neben ihrer Tätigkeit in Deutschland auch in anderen EU-Mitgliedsstaaten tätig sind, nur in dem Mitgliedstaat den entsprechenden Meldepflichten nachkommen müssen, in denen ihre Hauptniederlassung verortet ist (Art. 1 § 33 (1) NIS2UmsuCG). Übergeordnetes Ziel muss auch hier sein, die Erfüllungsaufwände für die betroffenen Einrichtungen und Unternehmen möglichst

gering zu halten. Ein Informationsaustausch zwischen den zuständigen nationalen Behörden ist entsprechend zu gewährleisten.[18]

Hinsichtlich der vorgeschriebenen Melde- und Dokumentationspflichten von Cybervorfällen durch die betroffenen Unternehmen gegenüber den zuständigen Behörden, wie dem BSI und dem BBK (vgl. mit (4) Registrierungswesen), ist eine klare Regelung zur Zusammenarbeit und eine Verpflichtung der Behörden zur Vertraulichkeit und zum Schutz der Unternehmens- und Kundendaten unbedingt erforderlich (siehe zum Aspekt der Vertraulichkeit Art. 1 § 16 (2) NIS2UmsuCG, sowie § 8e BSIG).

Es ist wahrscheinlich und bereits jetzt absehbar, dass insbesondere KMU in zahlreichen Fällen den Verpflichtungstatbeständen nicht innerhalb der rechtlich definierten Fristen nachkommen werden können. Um diese Problematik möglichst zu reduzieren, ist eine unbürokratische Umsetzung und Anwendung des Meldewesens erforderlich. Für Cybervorfälle sollte gemäß der NIS-2-Richtlinie (sowie auch gem. der CER-Richtlinie) eine einzelne Anlaufstelle auf Seiten der Bundesbehörden genannt werden, um nur jeweils einmalig melden bzw. berichten zu müssen, also eine Meldung für einen Vorfall (Once-Only-Prinzip). Hier könnte das BSI zum Knotenpunkt der Bund-Länder-Zusammenarbeit unter Nutzung kollaborativer IT-Anwendungen zum Informationsaustausch und hinsichtlich des Meldeverfahrens werden. Darüber hinaus braucht es einheitliche Begriffsdefinitionen (z. B. den Anwendungsbereich betreffend). Überschneidungen und Doppelstrukturen sollten im Zuge der Erarbeitung des KRITIS-Dachgesetzes weitgehend vermieden werden. Hierfür ist eine möglichst eindeutige und klare Definition für kritische Infrastrukturen erforderlich.[19]

Die in der NIS-2-Richtlinie empfohlene Verringerung des Verwaltungsaufwands hinsichtlich der Meldung von Vorfällen durch die betreffenden Einrichtungen und die Straffung der Abstimmungsprozesse der staatlichen Einrichtungen (Gründe 15, 30, 106 NIS-2-RL), also z. B. regionalen oder nationalen Anlaufstellen der Polizei oder der Bundes- bzw. die Landesdatenschutzbeauftragten, sind begrüßenswert. Da diese Vorgaben in der NIS-2-Richtlinie lediglich grob definiert sind, liegt es in der Hand der Behörden in Deutschland diese möglichst praxisnah auszugestalten. Für den Fall von grenzüberschreitenden Cybervorfällen ist eine zentralisierte Koordination in Englisch als Hauptsprache wünschenswert (entsprechend European cyber crisis liaison organisation network, abgekürzt EU-CyCLONe).

Zur möglichst praxisorientierten Ausrichtung der benannten Maßnahmen und Prozesse sowie zur Einbeziehung eines möglichst breiten Spektrums an Interessen von Stakeholdern können sogenannte Table-Top-Exercises (TTX) ein probates Mittel darstellen (siehe nationales Incident Response Framework in den USA).[20]

## (6) Lagebild als One-Stop-Shop

Aktuellen Informationen aus dem Bundesministerium des Innern und für Heimat (BMI) zufolge wird es voraussichtlich keine übergreifende Koordinierung zwischen den EU-Mitgliedstaaten bzgl. Initiativen zur zentralen Unterstützung von Unternehmen bei der Umsetzung geben (Stichwort „One-Stop-Shop“).

Umso drängender ist es, das in der Cybersicherheitsagenda des Bundesministeriums angekündigte BSI Information Sharing Portal (BISP) [21] im NIS2UmsuCG als geeigneten Ansatz einer zentralen Anlaufstelle für Unternehmen zur Beschaffung von kritischen Informationen umzusetzen und aufzubauen. Interfaces zu anderen relevanten Portalen sind hierbei zu schaffen und zu organisieren. Dieses Portal sollte auch Informationen zu Bedrohungen und Vorfällen in der „analogen Sphäre“ beinhalten, also z. B. Naturkatastrophen, Sabotage, entsprechend verursachte Ausfälle der digitalen Infrastruktur oder der Stromnetze

(Art. 1 § 6 NIS2UmsuCG). Hierbei gilt es grundsätzlich abzuwägen zwischen dem Mehrwert der entsprechenden Informationen und dem zusätzlichen bürokratischen und organisatorischen Aufwand.

Oberste Prämisse auf technischer Ebene sollte es also sein, relevante Informationen zur Prävention, Erkennung und Reaktion von und auf Cybervorfälle in einem nationalen, tagesaktuellen und für die Unternehmen möglichst kostengünstigen Lagebild ressourcenschonend und schnell abzubilden. Die Informationen sollten eine adäquate Spezifikation aufweisen, sodass diese möglichst schnell und effizient einer Auswertung zugeführt und ggf. entsprechende Maßnahmen eingeleitet werden können. Eine Konkurrenz zu kommerziellen Angeboten sollte durch eine zielgruppenorientierte Ausdifferenzierung verschiedener Angebote (z. B. für bestimmte Sektoren, KMU, etc.) möglichst vermieden werden.

Alle hier erwähnten Informationen sowie auch die interdependenten Informationen zwischen Staat und Industrie (z. B. Meldungen, Auditreports, etc.) sollten stets in deutscher und englischer Sprache vorliegen. Wenngleich dies mit erhöhten Aufwänden einherginge, ist dies eine Grundvoraussetzung, um dem Rahmen der EU-weiten Standardisierung von Maßnahmen zu entsprechen sowie den operativen Anforderungen der Unternehmen in der Cybersicherheitsbranche gerecht zu werden (vgl. mit Forderung in (5) Meldewesen). Der sich unmittelbar ergebene Trade-off zwischen Schnelligkeit und gegenläufigem Zeitaufwand zweisprachiger Bereitstellung der Informationen sollte durch einen möglichst hohen Grad an Automatisierung begegnet werden. Einer zentralen Stelle auf EU-Ebene sollten Vorfälle mit grenzüberschreitende Auswirkungen zur Verfügung gestellt werden, welche wiederum perspektivisch in ein EU-weites Lagebild einfließen.

## (7) Bußgeldrahmen

Derzeit sind im Umsetzungsgesetz (Art. 1 § 59 (5) NIS2UmsuCG) im Verweis auf das Gesetz über Ordnungswidrigkeiten (§ 30 (2) Satz 3 OWiG) für Unternehmen ohne Unterscheidung nach Einrichtung Bußgelder von bis zu 20 Millionen Euro vorgesehen.[22] Dieser Bußgeldtatbestand bezieht sich auf bestimmte Ausnahmefälle, in denen einer vorliegenden und vollziehbaren Anordnung des BSI durch eine Einrichtung zu wider gehandelt wird (z. B. hinsichtlich einer Mitwirkungspflicht bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit eines infiltrierten Systems). Sollten solche Bußgelder erhoben werden, könnten insbesondere KMU aus Gründen der finanziellen Tragfähigkeit einer existenziellen Bedrohungslage gegenüberstehen.

Der Wirtschaftsrat fordert, dass die Vorgaben der NIS-2-Richtlinie hinsichtlich der Bemessung von Geldbußen generell eng angewandt werden und in der rechtlichen Umsetzung in Deutschland darüber hinaus gehende Bußgeldbeträge ausgeschlossen sind.[23] Die Höchstgrenzen sind aufgrund der Formulierung „Höchstbeträge von mindestens“ in der NIS-2-Richtlinie nicht abschließend gesetzt. Höchstgrenzen sollten im Umsetzungsgesetz also klar als Höchstgrenzen gesetzt und entsprechend formuliert werden.[24] Mit Blick auf die oben genannten Bußgeldtatbestände ohne Unterscheidung der Einrichtung sollte eine Abstufung analog zu den Bußgeldtatbeständen für besonders wichtige und wichtige Einrichtungen in Erwägung gezogen werden.

Eine aktive Beteiligung der betreffenden Unternehmen an der Aufklärung durch die Schaffung von Transparenz bezüglich entsprechender Vorfälle sollte bei der Bemessung der Bußgeldhöhe grundsätzlich berücksichtigt werden (angelehnt an entsprechende Grundsätze im Strafrecht).

In der Festlegung des Bußgeldrahmens gilt es eine verhältnismäßige und angemessene Balance zwischen der Höhe der Bußgelder und dem Vergehen bzw. dem (potenziellen) Schaden herzustellen. Die mehrfache

Verhängung von Bußgeldern im Falle eines Verstoßes gegen die Vorgaben von zwei oder mehreren Regulierungen muss auch zukünftig ausgeschlossen sein (gem. Art. 35 (2) NIS-2-RL).

## (8) Managerhaftung

Hinsichtlich der in der NIS-2-Richtlinie vorgegebenen und im NIS2UmsuCG vorgesehenen „Billigungs- und Überwachungspflicht für Leitungsorganen“ bzw. Innenhaftung der Geschäftsleitung gegenüber der jeweiligen Gesellschaft ergibt sich folgender kritischer Punkt:

Das NIS-2-Umsetzungsgesetz geht mit der persönlichen Verantwortlichkeit für die Überwachung des Cyber-Risikomanagements, die für Geschäftsleitung von besonders wichtigen und wichtigen Einrichtungen vorgesehen ist – ohne die Möglichkeit der Übertragung dieser Verantwortung an Dritte – (NIS2UmsuCG Art. 1 § 38) über die in der NIS-2-Richtlinie gesetzten Vorgaben hinaus (vgl. mit Art. 20 NIS-2-RL). So ist konkret vorgesehen, dass die jeweilige Geschäftsleitung im Falle der Verletzung der Organpflichten persönlich für Schäden durch Cyberrisiken haftbar gemacht werden kann. Dies gilt sowohl in Bezug auf Regressansprüche als auch Bußgeldforderungen, denen die Gesellschaft bzw. das Unternehmen ausgesetzt ist. Es soll festgelegt werden, dass das Unternehmen weder auf Schadenersatzforderungen gegenüber dem Geschäftsleiter oder den Geschäftsleitern verzichten noch einen Vergleich in dieser Angelegenheit abschließen darf. Ein Verzicht ist lediglich für den Fall einer Insolvenz des Geschäftsleiters oder der Geschäftsleiter möglich (Art. 1 § 38 (3) NIS2UmsuCG). Im Hinblick auf Regressansprüche aus jedweden Gründen bestand innerhalb von Gesellschaften mit beschränkter Haftung (GmbHs) – mit einem Anteil von knapp 80 Prozent, die mit Abstand häufigste Rechtsform mit Handelsregistereintragung in Deutschland – rechtlich bislang einer gewisser Spielraum. Mit der Umsetzung der NIS-2-Richtlinie in Deutschland könnte dieser Spielraum erheblich eingeschränkt werden oder ggf. zukünftig gar gänzlich ausgeschlossen sein.

Zusammenfassend kann festgehalten werden, dass die persönliche Haftung von Geschäftsleitern für Schäden im Zusammenhang mit Cybersicherheitsverletzungen deutlich ausgedehnt wird. Das Ziel dieser Vorgabe ist es offensichtlich, Geschäftsleiter unvermeidlich haftbar zu machen, um ihr Engagement im Bereich der Risikovorbeugung und -steuerung zu verstärken.[25] Hier fordert der Wirtschaftsrat, dass die Vorgaben der NIS-2-Richtlinie den Grenzrahmen setzen und das NIS2UmsuCG nicht hierüber hinausgeht.

Neben der oben genannten Stelle in der NIS-2-Richtlinie (Art. 20 NIS-2-RL) gibt es noch eine weitere Stelle zur Haftung der Geschäftsleitung (Art. 32 (6) NIS-2-RL). Dort wird die Haftung für wesentliche bzw. besonders wichtige Einrichtungen definiert. Im NIS2UmsuCG fehlt hierfür eine eigene Umsetzung. Dadurch ist keine Differenzierung in der Haftung zwischen wesentlichen bzw. besonders wichtigen und wichtigen Einrichtungen vorgesehen. Hier fordert der Wirtschaftsrat, dass der in der NIS-2-Richtlinie offensichtlich vorgesehene Spielraum zur Differenzierung auch in der Implementierung in Deutschland berücksichtigt wird.

Ferner muss im NIS-2-Umsetzungsgesetz im vorliegenden Zusammenhang explizit sichergestellt werden, dass der Abschluss von sogenannten Directors- and Officers-Versicherung (kurz D & O-Versicherungen) auch zukünftig möglich ist. Diese Versicherungsform wird zumeist von der entsprechenden Gesellschaft für den Geschäftsführer abgeschlossen, so dass dieser im Falle von Regressforderungen nicht zwangsläufig die Gesamtsumme einer Regressforderung alleine tragen muss.

## (9) Anordnungen weiterer regulatorischer EU-Sicherheitsanforderungen (z. B. CER, CRA, CSA)

Der Wirtschaftsrat unterstützt die im Vordergrund stehende Harmonisierung der EU-Gesetzgebung grundsätzlich. Darüber hinaus befürwortet der Wirtschaftsrat die horizontale Konzeption des Cyber Resilience Act (CRA) mit dem Ziel der Vereinheitlichung der Produktanforderungen hinsichtlich Cybersicherheit und der Anhebung des Resilienzniveaus an der Schnittstelle zwischen allen relevanten Rechtsakten und Gesetzen auf EU-Ebene (neben der NIS-2-Richtlinie): New Legislative Framework (NLF), EU Cybersecurity Act (EU CSA), AI Act, EU Machinery Regulation.[26] Risikoadäquat cyberresiliente Produkte stellen eine Grundvoraussetzung für die wirksame Umsetzung technischer und organisatorischer Maßnahmen wie der NIS-2-Richtlinie dar. Dies ist zugleich ein übergeordneter Trend im Cybersicherheits-Recht.[27]

Der Wirtschaftsrat setzt sich neben der erwähnten Harmonisierung der EU-Gesetzgebung – wie auch mehrere andere Spitzen- und Branchenverbände in Deutschland – zugleich für eine möglichst innovationsfreundliche Regulierung ein. Konkret bezieht sich dies im vorliegenden Zusammenhang auf den European Cybersecurity Certification Scheme for Cloud Services (EUCS)[28], welches als ein Cybersicherheitszertifizierungsschema für Cloud-Dienste im Rahmen des CSA konzipiert ist und seit 2020 von der European Union Agency for Cybersecurity (ENISA) entwickelt wird. Die NIS-2-Richtlinie sieht die Möglichkeit vor, dieses und weitere Zertifizierungsschemata verpflichtend zu machen (Art. 24 NIS-2-RL, siehe entsprechend Art. 1 § 55 NIS2UmsuCG). Hier sollte eine sorgfältige Abwägung zwischen dem genannten Ziel einer Harmonisierung der EU-Gesetzgebung und des intendierten möglichst innovationsförderlichen regulatorischen Rahmens vorgenommen werden. Eine Überregulierung könnte ein verringertes Angebot an Cloud-Diensten aufgrund eines Rückzugs von Cloud Service Providern (CSPs) und damit einhergehend erheblich verringerte technologische Auswahlmöglichkeiten an innovativen Cloud-Lösungen für Anwender, ein erhöhtes Konzentrationsrisiko aufgrund des verminderten Angebots und steigende Kosten für die auf die diese Dienste zurückgreifenden und zu bedeutenden Teilen darauf angewiesenen Unternehmen nach sich ziehen.[29]

Im Zuge der Umsetzung der NIS-2-Richtlinie in Deutschland sollte eine EU-weit einheitliche Abstimmung und Einführung von Zertifizierungsschemata im Rahmen des CSA in Erwägung gezogen werden. Es ist im Anschluss hieran zu überlegen, ob Unternehmen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, nur dann zu einem einheitlichen Zertifizierungsschema, wie dem EUCS verpflichtet werden, wenn sich die freiwillige Anwendung von Zertifizierungsschemata hinsichtlich der Verbesserung der Cybersicherheit als ineffektiv herausstellen sollten.

## (10) Überprüfungsmöglichkeiten der Vertrauenswürdigkeit von Beschäftigten[30]

Der „Faktor Mensch“ ist nachweislich das Haupteinfallstor für Cyberangriffe. Hierauf aufbauend werden die technischen, organisatorischen und operativen Maßnahmen der NIS-2-Richtlinie sich als wenig effektiv erweisen, wenn neben den Wechselwirkungen zwischen technischen und organisatorischen Aspekten nicht auch adäquat und tiefergehend der personelle Aspekt berücksichtigt wird. Nicht nur durch Schulungen von Geschäftsleitern und Mitarbeitern (Art. 1 § 38 (4) NIS2UmsuCG) sind in diesem Zusammenhang die potentiellen Risiken zu minimieren. Dies gilt ebenfalls hinsichtlich der Gefahren die von nicht identifizierten Innentätern in Unternehmen ausgehen und den Wirtschaftsschutz kompromittieren können („Insider Threat“). Hierzu sollten alle Unternehmen, die dem Anwendungsbereich des NIS-2-Umsetzungsgesetzes unterliegen, die Möglichkeit erhalten, eine Sicherheitsüberprüfung für Beschäftigte bei den zuständigen Stellen zu beantragen.[31] Die rechtlichen Voraussetzungen in den betroffenen Gesetzen, insbesondere im Bundesdatenschutzgesetz (BDSG)[32], sind zu beachten und – sofern möglich – ggf. anzupassen.[33] Die

Verfahren von Sicherheitsüberprüfungen und die damit verbundenen Wartezeiten sollten zeitlich gestrafft und an den Bedarfen der Unternehmen ausgerichtet werden. Die Bereitstellung von angemessenen finanziellen und personellen Ressourcen auf staatlicher Seite ist sicherzustellen.

## (11) Einbeziehung der öffentlichen Verwaltung

Öffentliche Verwaltungen auf „zentraler" und „regionaler" Ebene fallen erstmals auch unter die NIS-2-Richtlinie. Hierbei überlässt die Richtlinie den EU-Mitgliedsstaaten einen gewissen Interpretationsspielraum. In Deutschland sollen nach aktuellem Stand Einrichtungen der Bundesverwaltung (Art. 1 § 29 NIS2UmsuCG) jedoch nicht der Länder und Kommunen einbezogen werden. Es sollte in Erwägung gezogen werden, eine genauere Definition der möglicherweise einzubeziehenden behördlichen Einrichtungen vorzunehmen und abzuwägen, inwiefern z. B. Landkreise und lokale öffentliche Verwaltungen, ebenfalls unter die Richtlinienvorgaben fallen sollten (etwa im Rahmen eines abgestuften Modells).[34]

Zu überlegen ist ferner die Einbeziehung von Hochschulen und Universitäten.[35] Dies ist notwendig, da diese Einrichtungen zunehmend von Cyberangriffen betroffen und damit potenziell wichtige Forschungsergebnisse (z. B. aus der Zusammenarbeit mit dem privaten Sektor) gefährdet sind. Zudem sind die Kosten eines ggf. auftretenden Bildungsausfalls eklatant. Hierbei gilt es jedoch die Bildungseinrichtungen finanziell mit den notwendigen Mitteln auszustatten und von staatlicher Seite zu unterstützen (Stichwort „Zukunftsvertrag" als Nachfolger des Hochschulpakts 2020).

## (12) Staatliche Unterstützung für Einrichtungen und Unternehmen (insbesondere KMU)

Ein Ziel muss es eine signifikante Erleichterung für Unternehmen sein. Dieses Ziel kann von staatlichen Unterstützungsleistungen hinsichtlich der technischen und organisatorischen Umsetzung NIS-2-Richtlinie flankiert werden. Rechtsfragen und ihre Auslegung stellen Unternehmen und insbesondere KMU regelmäßig vor große Herausforderungen. Um diesem Umstand zu begegnen bieten sich rechtsverbindliche und konkrete Umsetzungshilfen und ein offizieller Leitfaden von Seiten der zuständigen behördlichen Einrichtungen wie dem BSI – einhergehend mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes – an. Ein solcher Leitfaden sollte technologieneutral ausgestaltet sein und regelmäßig aktualisiert werden. Dies beinhaltet auch eine Erleichterung des Informationsaustausches zwischen den betroffenen Unternehmen und Behörden sowie die Verbesserung des Zugangs zu Expertenwissen für Firmen (siehe auch Forderung (4) Registrierungswesen). KMU sollten die Möglichkeit haben auf gezielte staatliche Förderprogramme im Zuge der Umsetzung der Richtlinie bei Bedarf zurückzugreifen.

Eine wesentliche Bedeutung in der technischen und organisatorischen Umsetzung kommt der ISO 27001-Zertifizierung auf Basis des BSI IT-Grundschutzes zu. Diese decken die in der NIS-2-Richtlinie geforderten Maßnahmen teilweise ab (Artikel 21.2 NIS-2-RL). Einrichtungen und Unternehmen, die bereits mit dem BSI IT-Grundschutz und/oder ISO 27001 zertifiziert sind, sollten nur noch NIS-2-Compliance-Nachweise für die Bereiche erbringen müssen, die durch die ISO 27001-Zertifizierung ggf. nicht abgedeckt sind (siehe Art. 1 § 43 NIS2UmsuCG zum Informationssicherheitsmanagement generell für Einrichtungen, Art. 1 § 44 NIS2UmsuCG zu Vorgaben des Bundesamtes für bundesstaatliche Einrichtungen). Bereits angestellte und bestehende Aufwände sollten also explizit anerkannt werden. Die Nachweisverfahren für die Zertifikate sind möglichst stringent zu vereinheitlichen.[36] Dies wäre ein erhebliche Vereinfachung aus Compliance-Sicht (siehe hierzu Forderung (1) Verantwortlichkeiten und Zuständigkeiten bzgl. Forderung von Rechts- und Planungssicherheit).

Das BMI argumentiert, dass die von verschiedenen Akteuren regelmäßig geforderte Umstellung des Prüfzyklus von betroffenen Einrichtungen von zwei auf drei Jahren aufgrund der erforderlichen Gleichbehandlung von Unternehmen nicht umsetzbar sei, da es insbesondere im Hinblick auf KRITIS mit einer weniger engmaschigen Aufsicht einherginge. Wie im jüngsten Bericht zur Evaluierung des IT-Sicherheitsgesetzes 2.0 des BMI (Stand Mai 2023) erwähnt, sollte jedoch die Vereinbarkeit von Zwischenaudits mit den gesetzlich erforderlichen KRITIS-Nachweisen auf Grundlage des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geprüft werden.[37]

Die für Unternehmen entstehenden Kosten aus der Umsetzung müssen möglichst gering gehalten werden. Zugleich sind effiziente und effektive Maßnahmen zur Verbesserung der Cybersicherheit und zur Reduktion der Cybervorfälle umzusetzen, die in der Konsequenz dann zu einer Reduzierung der aus Cybervorfällen resultierenden monetären und immateriellen Folgekosten beitragen.[38] Auch hier gilt es eine Bereitstellung von angemessenen finanziellen und personellen Ressourcen auf staatlicher Seite sicherzustellen (siehe Forderung (10)).

**Erläuterungen zum regulatorischen/gesetzgeberischen Fahrplan**

Die NIS-2-Richtlinie ist **am 16. Januar 2023 in Kraft getreten**. Die **Beteiligungsprozesse** der Verbände und Länder sollen demnächst offiziell eröffnet werden. Die derzeit noch unklaren Punkte zur Umsetzung in Deutschland sollen planmäßig dann **bis Mitte 2023 vor der parlamentarischen Sommerpause** (8. Juli 2023) geklärt und ein **Kabinettsbeschluss der Bundesregierung** getroffen sein. Der Regierungsentwurf ist hierauf folgend der EU-Kommission zur Notifizierung vorzulegen (für diesen Prozess sind drei Monate eingeplant). Der **Abschluss des parlamentarischen Prozesses** ist **bis Ende Herbst** (30. November 2023) vorgesehen. Nach der geplanten **Verkündung im März 2024** stünden den betroffenen Einrichtungen dann noch **sechs Monate für die Umsetzung** der im Umsetzungsgesetz enthaltenen Verpflichtungen zur Verfügung. Das Gesetz soll dann **am 1. Oktober 2024 Inkrafttreten** (Art. 15 NIS2UmsuCG). Nach Ablauf der EU-weit gesetzten Umsetzungsfrist (17. Oktober 2024) ist **keine daran anschließende Implementierungsphase** für Behörden oder Unternehmen vorgesehen (siehe auch Forderung (2) Umsetzungsfristen). Die EU-Mitgliedstaaten müssen die als wichtig und besonders wichtig (bzw. wesentlich) identifizierten Einrichtungen („important and essential entities“, siehe auch „size cap rule“) in ihrem Hoheitsgebiet **bis zum 17. April 2025 an die EU-Kommission melden**.[39]

---

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rats vom 14.12.2022 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 (veröffentlicht am: 27.12.2022).

[2] Im Folgenden bezugnehmend auf den Referentenentwurf (RefE) des Bundesministeriums des Innern und für Heimat BMI (2023a): Referentenentwurf zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), Bearbeitungsstand: 03.04.2023.
Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ist ein Änderungsgesetz, das die Artikel des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (kurz BSI-Gesetz bzw. BSIG) deutlich umstrukturiert, ändert und ergänzt. Parallel wird das KRITIS-Dachgesetz Resilienz bei kritischen Betreibern regulieren.
OpenKRITIS (2023): Das NIS2 Umsetzungsgesetz
Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), Ausfertigungsdatum: 14.08.2009

[3] In dieses Dokument sind inhaltlich folgende Publikationen eingeflossen:
Wirtschaftsrat (2022): Position Paper on the revised Directive on Security of Network and Information Systems (NIS-2.0), (14.02.2022).
BDI (2023): Implementierung der NIS-2-Richtlinie in nationales Recht (20.02.2023).
BITKOM (2023): Nationale Umsetzung der NIS-2- Richtlinie (17.03.2023).

Stiftung Neue Verantwortung (2023a): Stellungnahme von Julia Schuetze für die öffentliche Anhörung des Ausschusses für Digitales zum Thema "Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ am 25.01.2023 (19.01.2023).
VKU/ BDEW (2023): Stellungnahme zum Eckpunktepapier KRITIS-Dachgesetz (14.02.2023).
Verband der Automobilindustrie (2023): Implementierung der NIS-2-Richtlinie in nationales Recht (27.03.2023)

[4] Dies zielt insbesondere auf die zu kurzen und daher mangelhaften Beteiligungsmöglichkeiten beim Zustandekommen des im Jahr 2021 in Kraft getretenen IT-SiG 2.0 ab. Hier kam es von Seiten der Verbände und Unternehmensvertreter zu massiver Kritik: Die offizielle Konsultationsfrist für Wirtschaftsvertreter betrug lediglich 27 Stunden.

[5] Die Bremische Cybersicherheitsstrategie 2023 geht davon aus, „dass neben einer bundesweiten zentralen Anlaufstelle auch in den Ländern zuständige Behörden eingerichtet werden müssen.“
Freie Hansestadt Bremen (2023): Bremische Cybersicherheitsstrategie 2023, Stand: April 2023

[6] AG KRITIS (2023): Stellungnahme der Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS), S. 3 (18.01.2023)

[7] Vgl. mit Stiftung Neue Verantwortung (2023b): Deutschlands staatliche Cybersicherheitsarchitektur, 10. Auflage (10.05.2023), siehe auch Wirtschaftsrat (2023): Positionspapier des Wirtschaftsrates zur Cybersicherheit und Digitale Souveränität nach der „Zeitenwende (09.02.2023).

[8] Bundesregierung (2023): Nationale Sicherheitsstrategie, S. 59. veröffentlicht am: 14.06.2023

[9] Der Europäische Rat hatte sich in den Trilog-Verhandlungen im Jahr 2022 für eine Umsetzungsfrist von 24 Monate eingesetzt, während die Europäische Kommission und das Europäische Parlament 18 Monate gefordert hatten. Mit den letztlich geltenden 21 Monaten hatte man sich auf einen Kompromiss geeinigt.

[10] Timo Kob (2023): „Kaum zu bewältigen“: Neue EU-Richtlinie für Cybersicherheit setzt Unternehmen unter Zeitdruck, Handelsblatt vom 16.01.2023.

[11] Bundesamt für Justiz (2016): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV), Ausfertigungsdatum: 22.04.2016.

[12] BDI (2023): S. 3.

[13] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rats vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates

[14] Diese und weitere in diesem Dokument enthaltene Informationen zur nationalen Umsetzung der NIS-2-Richtlinie beruhen auf Aussagen von Andreas Könen, Abteilungsleiter CI Cyber- und Informationssicherheit im BMI, in Sitzungen der Bundesarbeitsgruppe Cybersicherheit sowie auf Informationen von weiteren Vertreterinnen und Vertretern des BMI und des BSI.

[15] Wirtschaftskammer Österreich (WKO): Online-Ratgeber

[16] BSI (2021): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), Ausfertigungsdatum: 17.05.2021.

[17] Wirtschaftsrat (2022): S. 6 f.

[18] BDI (2023): S. 4 f.

[19] Gem. der Eckpunkte des BMI für das KRITIS-Dachgesetz sollen „*kritische Infrastrukturen systematisch und umfassend*“ identifiziert und qualitative Kriterien als „*zentraler Regelungsgehalt*“ des berücksichtigen werden. „*Unter Einhaltung der europarechtlichen Anforderungen durch die CER- und NIS2-Richtlinie, besteht also die Chance eine dogmatisch befriedigende Antwort darauf zu finden, was an kritischen Infrastrukturen genau kritisch ist*.“
Vogel, Valentin; Ziegler, Nicolas (2023): Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie, in: International Cybersecurity Law Review, Volume 4 (2023).

[20] Entsprechende Übungen zum Umgang mit Cyberbedrohungen sind als organisatorische Vorsorgemaßnahme zur Simulation potenzieller Auswirkungen eines gezielten Cyberangriffs (z. B. durch Ransomware), zur Ermöglichung der Erprobung des hypothetischen Umgangs mit einem solchen Fall sowie zum Testen der eigenen Reaktionsfähigkeit zur Identifizierung möglicher Ineffizienzen und organisatorischer Schwachstellen konzipiert.
BSI (2023): Übungen, siehe auch Stiftung Neue Verantwortung (2023a): S. 6 ff.

[21] BMI (2022): Cybersicherheitsagenda, Stand: 12.07.2022. S. 12.

[22] Siehe hierzu Hinweis auf eine mögliche Verzehnfachung des Höchstmaßes der Geldbuße gem. § 30 OWiG in:
Bundesministerium der Justiz (1968): Gesetz über Ordnungswidrigkeiten (OWiG), Ausfertigungsdatum: 24.05.1968

[23] Konkret belaufen sich in der NIS-2-Richtlinie die Höchstbeträge auf mindestens 7 Mill. EUR oder 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes im Falle einer wichtigen Einrichtung und analog dazu 10 Mill. EUR oder 2 % im Falle einer wesentlichen bzw. besonders wichtigen Einrichtung (Art. 34 (4) u. (5) NIS-2-RL).

[24] GleissLutz (2023): Entwurf eines Umsetzungsgesetzes für NIS2 – Umfassende Erweiterung von Cybersicherheitspflichten und direkte Haftung der Geschäftsleitung, S. 3 (31.05.2023)

[25] Basar, Eren; Schreiber, Kristina (2023): Cybersecurity ist C-Level-Aufgabe, Deutscher AnwaltSpiegel, Ausgabe 11, 24. Mai 2023. S. 6-9.

[26] Anmerkung: Der Digital Operational Resilience Act (DORA) für Einrichtungen im Finanzsektor ist lex specialis und geht daher den Vorgaben des NIS-2-Richtlinie vor.

[27] Kipker, Dennis-Kenji (2023): Cybersecurity-Recht im Umbruch, Tagesspiegel Background 27.04.2023.

[28] ENISA (2020): European Cybersecurity Certification Scheme for Cloud Services, December 2020.

[29] BDI (2023): S. 6 f.
Bundesverband Gesundheits-IT (2023): EUCS-Label der ENISA: bvitg kritisiert mangelnde Transparenz (05.06.2023)
Gesamtverband der Versicherer (GDV) (2023): Dürfen Versicherer in der EU weiterhin US-Clouds nutzen? 04.05.2023
BITKOM (2020): Die Bedeutung des Zusammenspiels von EUCS / NIS / DORA für den Finanzmarkt (29.11.2022)

[30] Wirtschaftsrat (2022): S. 9.

[31] Diese Möglichkeit sollte also auch Unternehmen umfassen, die an sich keine sicherheitsbetreuten Unternehmen im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG) sind.

[32] Bundesministerium der Justiz (2017): Bundesdatenschutzgesetz (BDSG), Ausfertigungsdatum: 30.06.2017.

[33] Dies zielt u.a. auf entgegenstehende Regeln im Datenschutz nach § 26 (1) BDSG als auch der Rechtsprechung der Arbeitsgerichte ab. Unternehmen dürfen ohne konkrete Rechtsgrundlage einer entsprechenden Erlaubnis keine personenbezogenen Daten zu diesem Zweck verarbeiten und weitergeben.

[34] Gem. Stiftung Neue Verantwortung (2023a): S. 11 f.

[35] Da die entsprechenden Träger von Bildungseinrichtungen auf lokaler und regionaler Ebene zumeist auf Städte- und Länderebene angesiedelt sind, würden diese zum aktuellen Stand nicht unter die NIS-2-Umsetzung fallen.

[36] Tagesspiegel Background (2023): Wie wirksam sind die IT-Sicherheitsgesetze? 01.06.2023

[37] BMI (2023b): Bericht zur Evaluierung des IT-Sicherheitsgesetzes 2.0, Ausfertigungsdatum: 02.05.2023, zu § 8a, S. 12 f.

[38] Bezüglich des Erfüllungsaufwands für die Wirtschaft geht das BMI derzeit von einmaligen Personalkosten in Höhe von 1,37 Mrd. Euro und jährlichen laufenden Kosten in Höhe von 1,65 Mrd. Euro aus. BMI (2023a): S. 2 ff.
Laut der Folgenabschätzung der EU-Kommission („Impact assessment“), müssen Unternehmen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, in den ersten Jahren nach der Einführung mit einer Erhöhung ihrer derzeitigen IT-Sicherheitsausgaben um bis zu 22 % jährlich im Vergleich zum Stand vor der Einführung rechnen. Unternehmen, die bereits in den Anwendungsbereich der bisherigen NIS-1-Richtlinie fallen und die Maßnahmen umgesetzt haben, müssen mit einer Erhöhung von etwa 12 % rechnen. Es wird jedoch davon ausgegangen, dass die neuen Sicherheitsausgaben durch einen erheblichen Rückgang der Kosten für Cybersicherheitsvorfälle ausgeglichen werden.
European Commission (2020): Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union, (16.12.2020).

[39] Anmerkung: Zwischen den wichtigen und besonders wichtigen bzw. wesentlichen Einrichtungen besteht kein Unterschied hinsichtlich der Risikomanagementanforderungen und Meldepflichten, jedoch beim Aufsichts- und Sanktionsregime.