Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern und für Heimat
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinieund zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
(NIS-2-Umsetzungs- und Cybersicherheitsstärkunggsesetz – NIS2UmsuCG)
(Stand: 24.06.2024, 16:13 Uhr)

Einleitung

Die fachärztlichen Mitgliedslabore des ALM e.V. unterstützen ausdrücklich die Bemühungen um eine Verbesserung von Resilienz und Cybersicherheit und ebenso die Bemühungen um eine Harmonisierung der Vorgaben auf europäischer Ebene. Es liegt im Eigeninteresse der Unternehmen, eine größtmögliche Resilienz und IT-Sicherheit etablieren zu können. Dabei sollte im Sinne des im Entwurf zum KRITIS-DachG erwähnten „All-Gefahren-Ansatzes" ein möglichst integrativer Ansatz erfolgen, der die unterschiedlichen Aspekte aus der Sicht der betroffenen Betreiber kritischer Anlagen und Dienstleistungen quasi „aus einer Hand" regelt. Im Sinne der Vermeidung von Doppelstrukturen, vermeidbarer Bürokratie und letztlich bestmöglicher Effizienz, auch mit Blick auf die für die Registrierung, Überprüfungen und Audits erforderlichen zusätzlichen personellen Ressourcen in einem sehr engen Arbeitsmarkt der hierfür benötigten Fachkräfte, sollten die Transaktionskosten niedrig und die Prozesse für alle Beteiligten und Betroffenen so wenig komplex wie möglich ausgestaltet sein.

Grundsätzlich sehen die mitgeltenden EU-Richtlinien 2022/2555 vom 14.12.2022 (NIS-2-Richtlinie) und 2022/2557 vom 14.12.2022 (CER-Richtlinie) vor, dass mit Blick auf die verschiedenen Aspekte (physische Sicherheit, IT-Sicherheit) Doppelarbeit vermieden werden soll, dass Mitgliedsstaaten aber auch mehrere nationale Behörden benennen können. Der ALM e.V. empfiehlt daher nachdrücklich, Art. 9 Absatz 1 und 2 der CER-Richtlinie in Deutschland umzusetzen und das BBK (physische Sicherheit) und das BSI (IT-Sicherheit) als die beiden nationalen Behörden zu benennen, wobei das BBK im Sinne von Art. 9 Absatz 3 die Koordinierungsstelle zu den EU-Mitgliedsstaaten übernehmen könnte.

Zur Vermeidung von inhaltlichen Abstimmungsproblemen zwischen BBK, BSI und im Falle des Gesundheitswesens mit dem hierfür zuständigen Bundesministerium für Gesundheit, sollten klarere und einfachere Zuständigkeiten festgelegt werden, da die Prozesse der Herstellung des Einvernehmens sonst länger dauern können und somit die Betreiber von kritischen Anlagen unter Umständen erst sehr spät erfahren, welche Rahmenbedingungen und Detailvorgaben für sie gelten.

Es ist sicherzustellen, dass die bereits seit mehreren Jahren gemachten positiven Erfahrungen mit der Umsetzung des BSIG und der daraus entstandenen Rechtsverordnung (KritisV) voll umfänglich übernommen werden. Die Betreiber der kritischen Anlagen und Dienstleistungen in der Anlagenkategorie Laboratoriumsdiagnostik (Labore, Laborinformationsverbund) im Sektor Gesundheit haben nunmehr mindestens zwei Prüfzyklen nach den Vorgaben des BSI durchlaufen und im Falle der fachärztlichen Laboruntersuchungen zudem einen branchenspezifischen Standard entwickelt, dessen Fortentwicklung aktuell wegen der noch unklaren Gesetzeslage stockt. Das ist jedoch nicht im Sinne der Betreiber, die ein eigenes hohes Interesse an bestmöglicher IT-Sicherheit sowie auch an bestmöglichem Schutz im Sinne von BCM für ihre Einrichtungen bzw. Anlagen haben. Gleichzeitig sollte es ähnlich eines integrativen Ansatzes möglich sein, dass ein branchenspezifischer Standard sowohl die Resilienz als auch die IT-Sicherheit adressieren kann, zumal sich in vielen und insbesondere in den wesentlichen Teilen beide Fragestellungen vollständig überlappen. Damit würde Doppelarbeit vermieden, sowohl für die Betreiber bzw. die Branchenverbände als auch für das BBK/BSI in der Prüfung und Feststellung der

Geeignetheit eines solchen Standards. Insbesondere könnte dadurch auch ein doppelter Audit-Aufwand der Betreiber nach dem KRITIS-DachG und dem BSI-Gesetz in der Fassung des NIS2UmsuCG mit sich in größeren Teilen inhaltlich identischen bzw. ähnlichen Audit-Gegenständen vermieden werden.

Die geltenden EU-Richtlinien 2022/2555 (NIS-2-Richtlinie) und 2022/2557 (CER-Richtlinie) und die beiden Umsetzungsgesetze NIS2UmsuCG sowie KRITIS-DachG verwenden unterschiedliche Definitionen und Schwellenwerte zur Festlegung, welche Einrichtungen unter den Anwendungsbereich der jeweiligen Richtlinie bzw. das jeweilige Gesetz fallen. Dabei bestehen auch Unterschiede zu bereits geltenden Gesetzen und Verordnungen wie das BSI-Gesetz und die BSI-Kritisverordnung. Der ALM e.V. empfiehlt hier dringend eine Harmonisierung und verbindliche Festlegung im NIS2UmsuCG im Einklang mit dem KRITIS-DachG. Nach den aktuellen Entwürfen würden eine Vielzahl der fachärztlichen Labore und darüber hinaus auch größere ambulante Einrichtungen in der vertragsärztlichen Versorgung unter den Geltungsbereich beider Gesetze fallen und somit einen enormen zusätzlichen neuen Prüfungsbedarf für das BBK sowie das BSI auslösen, dem aktuell erkennbar keine entsprechenden personellen und finanziellen Ressourcen für die Bewältigung dieser Aufgabe gegenüberstehen, insbesondere vor dem Hintergrund des derzeitigen enormen zusätzlichen Fachkräftebedarfs in der Gesamtwirtschaft und ebenso im Gesundheitswesen.

Die fachärztlichen Labore haben wie alle Einrichtungen im Gesundheitswesen im Vergleich zu den meisten anderen Wirtschaftsunternehmen, die in den Regelungsbereich des NIS2UmsiCG fallen, keine Möglichkeiten, die mit der Umsetzung von gesetzlich vorgeschriebenen Rahmenbedingungen zur IT-Sicherheit gemäß des laufenden Gesetzgebungsverfahrens des NIS2UmsuCG verbundenen erheblichen einmaligen und wiederkehrenden Investitions- und laufenden Betriebskosten über eine Anhebung der Preise zu refinanzieren. Da im Gesundheitswesen der Gesetzgeber unmittelbar (Gebührenordnung für Ärzte) und mittelbar (Ausgestaltung der Finanzierung der Gesetzlichen Krankenversicherung und damit der ambulanten und stationären Behandlung) die Einnahmen der fachärztlichen Labore bestimmt, ist es erforderlich, den erhöhten einmaligen, wiederkehrenden und laufenden Finanzbedarf hier entsprechend abzubilden.

Soweit durch Umsetzung des vorangehenden Vorschlags keine vollständige Refinanzierung des Umsetzungsaufwandes beider Gesetze für die fachärztlichen Labore sichergestellt wird, sieht der ALM e.V. die Auflage eines ausreichend dotierten und möglichst bürokratiearm ausgestalteten Förderprogramms zur Finanzierung des Umsetzungsaufwandes für in den Anwendungsbereich eines oder beider Gesetze fallender Unternehmen für erforderlich an (oder die Ausweitung eines bereits bestehenden Förderprogramms z.B. betreffend Krankenhäuser, auf alle betroffenen Einrichtungen des Gesundheitswesen, insbesondere auch auf ambulant tätigen Einrichtungen des Gesundheitswesens, die einem oder beiden Gesetzen unterliegen).

Im Kontext der Finanzierung ist auch der besondere zusätzliche Nutzen der kritischen Anlagen/Dienstleistungen zugunsten des Gemeinwohls zu sehen. Denn mit der Erfüllung der gesetzlichen Vorgaben des KRITIS-DachG und auch des NIS2UmsuCG erhöhen die Betreiber nicht nur die eigene Resilienz und IT-Sicherheit, sondern tragen maßgeblich zur Sicherstellung der gesamtgesellschaftlichen IT-Sicherheit und Resilienz bei.

Stellungnahme zu einzelnen Aspekten:

Zu § 2 Abs. 1 Nr. 21 i.V.m. § 28 und § 58 Abs. 4 NIS2UmsuCG

Stellungnahme*:*

In § 2 Abs. 1 Nr. 21 erfolgt die Definition „Kritische Anlage“ mit der inhaltlichen Konkretisierung in § 28 und der weiteren Ausgestaltung durch die in § 58 Abs. 4 vorgesehene Ermächtigung zum Erlass einer Rechtsverordnung. Diese Regelungen korrespondieren direkt mit der systematisch gleich gestalteten Definition „Kritische Anlage“ im KRITIS-DachG (dort in § 2 Nr. 3 sowie § 4 und der Ermächtigung zum Erlass von Rechtsverordnungen durch § 15).

In § 58 Abs. 4 NIS2UmsuCG wird darauf verwiesen, dass der als kritisch anzusehende Schwellwert des Versorgungsgrades definiert, welche Anlagen als kritische Anlage im Sinne des Gesetzes gelten. Dieser Schwellenwert ist für jede als kritisch anzusehende Dienstleistung zu bestimmen und durch branchenspezifische Schwellenwerte festzulegen

Die Zugehörigkeit einer Anlage zur Kategorie „kritische Anlage“ erfolgt auf der Grundlage der NIS-2-Richtlinie (EU) 2022/2555 in Artikel 2, so dass einerseits alle über die CER-Richtlinie der EU (2022/2557) als kritische Anlage bereits erfassten Anlagen gesehen werden und andererseits die Zuordnung nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten soll. Diese Definition findet sich in § 2 (Begriffsbestimmungen) des NIS2UmsuCG wieder, so dass sich unterschiedliche und nicht ergänzende Kriterien für eine Zuordnung eines Unternehmens zur Gruppe der „kritischen Anlagen“ ergeben. Das sollte in jedem Fall vermieden werden und durch eine Harmonisierung der Zuordnungskriterien, ggf. auch auf europäischer Ebene erfolgen.

Formulierungsvorschlag zu § 58 (Ermächtigung zum Erlass von Rechtsverordnungen)

(4) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter Festlegung der in § 28 Absatz 7 genannten Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, *in Anlehnung an die Anhänge 1 – 8 der BSI-KritisV* welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Der als bedeutend anzusehende Versorgungsgrad ist anhand branchenspezifischer Schwellenwerte für jede als kritisch anzusehende Dienstleistung zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.

Zu § 3:

Stellungnahme*:*

In § 3 Abs. 1 wird festgelegt, dass dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die alleinige Zuständigkeit für die Überwachung der IT-Sicherheitsmaßnahmen gemäß NIS2-UmsuCG übertragen wird, wohingegen die äquivalente Zuständigkeit für Resilienz gemäß § 3 KRITIS-DachG dem

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als einzige nationale Behörde nach Artikel 9 Absätze 1 und 2 der CER-Richtlinie obliegt. Im Kontext der Unternehmensabsicherung gegen physische und informationstechnische Gefahren erscheint eine Trennung von IT-Sicherheit und Resilienz nicht sinnvoll. Daraus ergibt sich die Notwendigkeit klarer Zuständigkeitsstrukturen.

Aus der Perspektive der fachärztlichen Labore, von denen ohnehin schon ein großer Teil über das BSI-Gesetz und die BSI-Kritisverordnung als Betreiber kritischer Dienstleistungen eingestuft ist, wäre eine solche doppelte Zuordnung dringend zu vermeiden.

Formulierungsvorschlag zu § 3 (Aufgaben des Bundesamtes)

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:

Zusatz zu Nr. 1 – 28: Unterstützung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) bei der Überwachung und Prüfung der Umsetzung von Resilienzmaßnahmen im Sinne von § 10 KRITIS-DachG, die im Zusammenhang mit Informationssicherheitsmaßnahmen stehen.

Zu § 30:

Stellungnahme:

Der ALM e.V. begrüßt es ausdrücklich, dass die Betreiber Kritischer Anlagen und ihre Branchenverbände branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach BSI-Gesetz vorschlagen können. Diese Regelung korrespondiert mit dem KRITIS-Dachgesetz (hier § 6), in dem ebenfalls den branchenspezifischen Verbänden die Entwicklung von Standards ermöglicht wird.

In der Anhörung wurde auf den Vorschlag, des ALM e.V., eine Regelung zu schaffen, die die Zusammenfassung beider Standards in einem branchenspezifischen Standard zur Erfüllung beider Anforderungen aus dem NIS2UmsuCG und dem KRITIS-DachG ermöglicht, seitens des BMI sehr positiv aufgenommen und von weiteren Verbänden unterstützt.

Leider findet sich in dem angepassten Referentenentwurf hierzu keine Entsprechung. Wir bitten um eine entsprechende Klarstellung, mindestens in der Begründung zum § 30 Absatz 8.

Zu § 33:

Stellungnahme:

Betreiber kritischer Anlagen sind nach § 33 Abs. 1 NIS2-UmsuCG dazu verpflichtet, sich zu einem Stichtag bei einer gemeinsam vom BBK und dem BSI eingerichteten Registrierungsmöglichkeit zu registrieren. Diese Vorschrift ist im Zusammenhang mit der im KRITIS-DachG und dort in § 6 vorgesehenen Registrierungspflicht für Betreiber kritischer Anlagen zu sehen. Da beide Registrierungsverfahren zum großen Teil deckungsgleich sind und inhaltlich nicht bzw. nicht maßgeblich voneinander abweichen, wäre im Sinne einer Entbürokratisierung und einer Minimierung des Verwaltungsaufwandes eine zentrale Registrierung kritischer Anlagen anzustreben.

Weiterhin sind nach § 33 Abs. 2 und Abs. 5 betroffene Institutionen verpflichtet, u.a. öffentliche IP-Adressen der Anlagen anzugeben bzw. Änderungen zu melden. Die geforderten Informationen können zur Benachrichtigung wichtig sein und der Sinn wird erkannt. Je nach Sektor und Branche erscheint die

getroffene Regelung aber unter Berücksichtigung von komplexen Konzernstrukturen als zu starr, um mehrere, zu verschiedenen Einrichtungstypen gehörenden Standorte praktikabel abbilden zu können.

Formulierungsvorschlag zu § 33 Abs. 1 (Registrierungspflicht)

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, spätestens drei Monate, nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit folgenden Angaben zu übermitteln […].

Eine doppelte Registrierung besonders wichtiger Einrichtungen und wichtiger Einrichtungen in Verbindung mit § 6 KRITIS-DachG ist dabei ausgeschlossen, sofern der Betreiber einer Anlage sowohl die Voraussetzungen gemäß § 28 als auch gemäß § 7 KRITIS-DachG erfüllt. In diesem Fall ist eine zentrale Meldung der Anlage ausreichend.

(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die kritische Dienstleistung, *sofern möglich* die öffentlichen IP-Adressbereiche der von ihnen betriebenen Anlagen sowie die für die von ihnen betriebenen kritischen Anlagen ermittelte Anlagenkategorie und ermittelte Versorgungskennzahlen gemäß der Rechtsverordnung nach § 58 Absatz 4 sowie den Standort der Anlagen und eine Kontaktstelle. Die Betreiber stellen sicher, dass sie über ihre in Satz 1 genannte Kontaktstelle jederzeit erreichbar sind.

Zu § 39:

Stellungnahme*:*

In § 39 Abs. 1 NIS2-UmsuCG wird die organisatorisch wie prozessual geregelte Erfüllung der Nachweispflicht der Umsetzung der Maßnahmen zur IT-Sicherheit gemäß § 30 Abs. 2 und § 31 NIS2-UmsuCG durch die Betreiber Kritischer Anlagen dem BSI gegenüber geregelt. Dabei können BBK und BSI jeweils Vorgaben für die zur Erfüllung der Nachweispflicht möglichen Audits und Prüfungen hinsichtlich der Art und Weise der Durchführung, der auszustellenden Nachweise sowie der fachlichen und organisatorischen Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.

Für die Betreiber kritischer Anlagen entsteht hier ein nicht mehr einschätzbares Risiko und damit ein nicht mehr vertretbarer organisatorischer und letztlich auch finanzieller Aufwand aufgrund potenziell unterschiedlicher Bewertungen identischer Inhalte durch das BBK bzw. das BSI. Zudem kann es zu doppelten Audits bzw. Prüfungen und damit auch doppelten Dokumentationen kommen, wenn die Anforderungen des BBK und des BSI in den Detailvorgaben unterschiedlich sind.

Formulierungsvorschlag zu § 39 (Nachweispflichten für Betreiber kritischer Anlagen)

(1) Betreiber kritischer Anlagen haben die Erfüllung der Anforderungen nach § 30 Absatz 1 und § 31 zu einem vom Bundesamt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt frühestens drei Jahre nachdem sie erstmals oder erneut als ein Betreiber einer kritischen Anlage gelten und anschließend alle drei Jahre dem Bundesamt auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. *Unterliegt ein Betreiber einer kritischen Anlage zusätzlich der Nachweispflicht gemäß § 11 Abs.*

1 KRITIS-DachG erfolgt die Nachweisführung zur Erfüllung der Anforderungen der IT-Sicherheitsmaßnahmen nach § 30 Absatz 1 und § 31 und der Resilienzmaßnahmen nach § 10 KRITIS-DachG in einer einheitlichen durch das Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe abgestimmten Art und Weise.

Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen.

Zu § 40:

Stellungnahme:

Der ALM e.V. begrüßt ausdrücklich die Einrichtung einer gemeinsamen Meldestelle des BBK im Einvernehmen mit dem BSI, an das der Betreiber einer kritischen Anlage Vorfälle in der vorgeschriebenen Art und Weise melden kann, und dass diese Meldestelle in beiden Gesetzesentwürfen korrespondierend ausgestaltet sind (§ 12 Abs.1 KRITIS-DachG und § 40 Abs. 1 NIS2-UmsuCG).

Allerdings halten es die fachärztlichen Labore für sachdienlich, die Meldeanlässe sowie die Meldefrequenzen des Kritis-DachG und des BSI-Gesetzes in der Fassung des NIS2UmsuCG ebenfalls zu harmonisieren.

Formulierungsvorschlag zu § 40 (Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen)

(3) Nr. 1 Zur Wahrnehmung seiner Aufgabe als zentrale Meldestelle hat das Bundesamt die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Schwachstellen, zu Schadprogrammen und zu Angriffen. *Relevante Meldung durch die Betreiber kritischer Anlagen erfolgen dabei analog zu § 12 KRITIS-DachG.*

Zu § 41:

Stellungnahme:

Die derzeit vorgesehene 2-monatige Frist für kritische Komponenten erscheint gerade im IT-Infrastrukturbereich nicht für alle Komponenten als umsetzbar. Am Beispiel des Tauschs eines Firewall-Clusters kann dies verdeutlicht werden: ein derartiges Vorhaben ist komplex und kann sich über Monate erstrecken. Insbesondere wenn dann nicht mehr freigegebene Teilkomponenten (beispielsweise Chips von Huwaii im Server) auftauchen, bedeutet dies im Worstcase den Tausch des ganzen Clusters. Unabhängig von der betriebswirtschaftlichen Komponente erscheint uns alleine der Angebots- und Bestellprozess nicht unter 6 Monaten abbildbar.

Formulierungsvorschlag zu § 41 (Untersagung des Einsatzes kritischer Komponenten)

(4) Das Bundesministerium des Innern und für Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Einvernehmen mit den in § 58 Absatz 4

aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend. *Im Falle der Untersagung des weiteren Einsatzes einer kritischen Komponente bzw. einer Anordnung wird zwischen dem Bundesamt und dem Betreiber der kritischen Anlage eine angemessene Frist als Einzelfallentscheidung zur Erneuerung der betroffenen kritischen Komponente abgestimmt.*