Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 D

Boehringer Ingelheim

Stellungnahme

Für die Anhörung des Deutschen Bundestages zum Entwurf der Bundesregierung eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG-E), BT-Drucksache 20/13184

Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 4. November 2024 um 11:00 Uhr

Sehr geehrte Damen und Herren Abgeordnete,

wir bedanken uns für die Einladung zu der oben genannten Anhörung im Rahmen des Gesetzgebungsverfahrens zur Umsetzung der europäischen NIS-2-Richtlinie durch die Bundesrepublik Deutschland.

Zu dem Gesetzentwurf der Bundesregierung nehmen wir wie folgt Stellung:

Als Hersteller von Arzneimitteln und Medizinprodukten und Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel betreiben, fallen zumindest alle großen Pharmaunternehmen in Deutschland als „wichtige“ bzw. „besonders wichtige Einrichtungen“ in den Anwendungsbereich der NIS-2-Richtlinie beziehungsweise des geplanten deutschen Umsetzungsgesetzes.

Viele Unternehmen investieren bereits jetzt in erheblichem Umfang in Maßnahmen zur Gewährleistung eines hohen Cybersicherheitsniveaus, nicht zuletzt, um ihre Lieferketten stabil zu halten und um zu verhindern, dass wertvolles Know-how und Geschäftsgeheimnisse ins Ausland abfließen. Daher begrüßen wir die Absicht der Kommission, das Cybersicherheitsniveau in der Europäischen Union flächendeckend zu erhöhen und stärker zu harmonisieren, indem beispielsweise zu implementierende Risikomanagement-Maßnahmen verbindlich vorgeschrieben und gesetzlich konkretisiert werden.

Bevor wir uns zu einzelnen Bestimmungen äußern, möchten wir grundsätzlich dafür plädieren, bei der Umsetzung die Mindestanforderungen der NIS-2-Richtlinie nicht zu überschreiten. Hintergrund ist, dass europaweit bzw. global agierende Unternehmensgruppen oft mit einer einheitlichen, zentral gesteuerten IT-Landschaft arbeiten, in der Maßnahmen zum Risikomanagement, zur IT-Sicherheit sowie zu Meldeprozessen nicht länderbezogen, sondern in operativ sinnvoller Weise europaweit einheitlich implementiert sind. Ein solch zentraler Ansatz führt zur Erhöhung der IT-Sicherheit und ist gleichzeitig deutlich effizienter als eine dezentrale IT-Landschaft und -Organisation. Dieser Ansatz wird gefährdet, wenn Mitgliedstaaten über die NIS-2-Richtline hinausgehende Pflichten vorsehen. Daher plädieren wir dafür, komplexitätssteigernde überschießende Regelungen zu streichen und damit unnötige Bürokratie und

Aufwände auf Unternehmensseite zu vermeiden. Wir sind überzeugt, dass auf diesem Weg die Zielsetzungen der Gewährleistung eines hohen Cybersicherheitsniveaus in der EU und der Förderung der Attraktivität des Wirtschaftsstandorts Deutschland am effizientesten erreicht werden können.

Im Einzelnen möchten wir für eine Anpassung oder Streichung folgender Regelungen des vorliegenden Entwurfs plädieren:

1. **Sonderregelungen für Betreiber kritischer Anlagen – nicht erforderlich**

   Die Sonderregelungen für Betreiber kritischer Anlagen sind systemfremd, signifikant komplexitätssteigernd und im Ergebnis nicht erforderlich. Wir regen daher an, die entsprechenden Regelungen aus dem NIS2UmsuCG-E zu streichen.

   Mit dem NIS2UmsCG-E wird ein Systemwechsel gegenüber der Regulierung kritischer Infrastrukturen nach dem bestehenden BSIG vollzogen: Bezugspunkt sind nicht mehr (kritische) Infrastrukturen und deren Schutz, sondern Unternehmen/Institutionen und deren Dienste. Die Übernahme und Integration der bisherigen Kategorie der (Betreiber von) kritischen Infrastrukturen (bzw. jetzt "kritischen Anlagen") in das neue einrichtungsbezogene System des BSIG-E führt zu einem systematischen Bruch, der zu Interpretationsschwierigkeiten in vielerlei Hinsicht führt, z. B. in Bezug auf die Frage, ob die verschärften Anforderungen für Betreiber kritischer Anlagen für die gesamte Einrichtung oder nur für den Betrieb der kritischen Anlage Geltung beanspruchen.

   Darüber hinaus erhöht die unionsrechtlich nicht geforderte Kategorie der Betreiber kritischer Anlagen die Komplexität für Unternehmen in Bezug auf die Anwendbarkeitsprüfung und Umsetzung der Anforderungen erheblich. So wird eine belastbare Anwendbarkeitsprüfung unter dem derzeit geplanten BSIG-E erst dann möglich sein, wenn auch die finale Fassung der Verordnung nach § 56 Abs. 4 BSIG-E feststeht.

   Und auch danach erfordert das geplante Festhalten an sektorspezifischen Schwellenwerten über ein unternehmensseitiges Monitoring der allgemeinen Schwellenwerte der KMU-Empfehlung hinaus auch ein permanentes Monitoring von Versorgungskennzahlen. Im Falle einer Überschreitung der definierten Versorgungskennzahlen soll dann, den Vorgaben nach § 31 Abs. 1 BSIG-E entsprechend, ad hoc ein verschärfter Verhältnismäßigkeitsmaßstab für die zu implementierenden Risikomanagementmaßnahmen gelten. Dieses "Alles-oder-Nichts"-Prinzip, das im pharmazeutischen Bereich im Fall einer zusätzlich produzierten Packung Arzneimittel zu einem verschärften Risikomanagementmaßstab führen kann, ist aus Verhältnismäßigkeitsgesichtspunkten und Praktikabilitätserwägungen nicht zielführend.

   Darüber hinaus ist die Sonderregelung des § 31 Abs. 1 BSIG-E nicht erforderlich, da eine erhöhte gesellschaftliche oder wirtschaftliche Bedeutung einer bestimmten Dienstleistung bereits im Zuge der allgemeinen für besonders wichtige und wichtige Einrichtungen geltenden Risikomanagementanforderungen zu berücksichtigen ist und bereits auf Grundlage des § 30 Abs. 1 BSIG-E zu einer Anhebung des geforderten Schutzniveaus führt.

Die vorstehenden Ausführungen gelten entsprechend für die Verpflichtung zum Einsatz von Angriffserkennungssystemen in § 31 Abs. 2 BSIG-E. Soweit von dieser Regelung besonders wichtige oder wichtige Einrichtungen betroffen sind, die in den Anwendungsbereich der Durchführungsverordnung (EU) 2024/2690 fallen (wie zum Beispiel Anbieter von Cloud Computing-Diensten), begegnet die Vorschrift zudem unionsrechtlichen Bedenken: Sie widerspricht der in Erwägungsgrund 84 der NIS-2-Richtlinie verankerten unionsrechtlichen Intention eines hohen Maßes an Harmonisierung in den erfassten digitalen Sektoren, da sich die Anforderungen aus § 31 Abs. 2 BSIG-E i.V.m. § 2 Nr. 41 BSIG-E nicht mit den in Nummer 3.2.1 des Anhangs der vorstehend genannten Durchführungsverordnung konkretisierten Anforderungen an Überwachung und Protokollierung decken.

Ebenfalls nicht erforderlich, jedoch ein signifikantes Maß an Bürokratie generierend, ist die in § 39 BSIG-E verankerte periodische Nachweispflicht für Betreiber kritischer Anlagen. Wir halten insofern die gegenüber besonders wichtigen Einrichtungen bestehenden Aufsichtsbefugnisse des BSI, die eine anlasslose Anordnung der Durchführung von Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen (siehe § 61 Abs. 1 BSIG-E) oder der Vorlage von Nachweisen über die Einhaltung der Risikomanagementpflichten (siehe § 61 Abs. 3 BSIG-E) erlauben, für ausreichend.

Sofern weiterhin an den Sonderregelungen für Betreiber kritischer Anlagen festgehalten werden sollte, sollte in § 56 Abs. 4 BSIG-E jedenfalls eine Anhörungspflicht aufgenommen werden, um sicherzustellen, dass die relevanten Interessengruppen Stellung nehmen können, bevor in der entsprechenden Verordnung die als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehende Versorgungsgrade definiert werden. Eine derartige Bestimmung, die die *„Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände“* vorsieht, ist de lege lata auch in § 10 Abs. 1 BSIG enthalten.

2. Nationale Spezifizierungen von Risikomanagementmaßnahmen sollten sich auf internationale Standards und Normen beziehen

Die in § 30 Abs. 5 BSIG geregelte Verordnungsermächtigung des Bundesministeriums des Inneren und Heimat ("BMI") sollte auf eine Präzisierung der nach § 30 Abs. 1 und 2 BSIG geforderten Risikomanagementmaßnahmen beschränkt und um ein Anhörungserfordernis sowie um die Pflicht des BMI, sich bei der Ausarbeitung der Verordnung so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen zu orientieren, ergänzt werden.

§ 30 Abs. 5 BSIG-E erlaubt es dem BMI – jenseits abschließender unionsrechtlicher Durchführungsrechtsakte der Europäischen Kommission nach Art. 21 Abs. 5 der NIS-2-Richtlinie – eine Präzisierung und Erweiterung der von § 30 Abs. 2 BSIG-E geforderten Risikomanagementmaßnahmen vorzunehmen.

Wir plädieren im Sinne einer möglichst umfassenden unionsweiten Harmonisierung der Cybersicherheitsvorgaben dafür, die Verordnungsermächtigung auf die Befugnis zur Präzisierung der

Vorgaben des § 30 Abs. 2 BSIG zu beschränken und keine Erweiterung der Managementmaßnahmen auf dem Verordnungsweg zu eröffnen.

Jedenfalls sollte das BMI in § 30 Abs. 5 BSIG-E verpflichtet werden, sich bei der Ausarbeitung der Verordnung so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen zu orientieren. Die Europäische Kommission unterliegt im Rahmen ihrer delegierten Rechtsetzung ebenfalls einer entsprechenden Vorgabe (siehe Art. 21 Abs. 5 UAbs. 3 NIS-2-Richtlinie).

Zudem sollte die Verordnungsermächtigung des § 30 Abs. 5 BSIG-E um eine Anhörungspflicht ergänzt werden. Wir halten auch hier die Beteiligung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände für angezeigt, um eine praxistaugliche und an der Unternehmensrealität orientierte Spezifizierung der Risikomanagementmaßnahmen zu gewährleisten.

3. Governance- und Schulungspflichten durch Geschäftsleitungen in § 38 BSIG-E sollten nachgeschärft werden

§ 38 BSIG-E ist in der gegenwärtigen Entwurfsfassung missverständlich und sollte wie in der NIS-2-Richtlinie gefasst werden, um die bestehenden Rechtsunsicherheiten zu beseitigen.

Dem Wortlaut von § 38 Abs. 1 BSIG-E zufolge sind "*Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen […] verpflichtet, die von diesen Einrichtungen […] zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen*". Wir halten diese Formulierung in zweierlei Hinsicht für missverständlich.

Zum einen suggeriert der Wortlaut "*umzusetzen*", dass eine Umsetzung der Maßnahmen durch die Leitungsebene selbst erfolgen müsse. Abweichend hiervon wird in der Gesetzesbegründung ausgeführt, dass Geschäftsleitungen die konkret zu greifenden Maßnahmen "*als für geeignet zu billigen*" haben und auch dann letztverantwortlich für die Geeignetheit und Umsetzung erforderlicher Maßnahmen bleiben, wenn Hilfspersonen eingeschaltet, also zum Beispiel Aufgaben an einen Informationssicherheitsbeauftragten delegiert werden. Da eine Umsetzung durch die Leitungsebene in persona nicht der Intention des § 38 Abs. 1 BSIG-E entsprechen kann, regen wir an, die Formulierung "*umzusetzen*" mit der Formulierung "*als für geeignet zu billigen*" oder – entsprechend der Formulierung in Artikel 20 Abs. 1 NIS-2-Richtlinie – mit dem Wortlaut "*zu billigen*" zu ersetzen.

Zum anderen führt die Verwendung des Begriffs "*Geschäftsleitungen*" in § 38 BSIG-E in Verbindung mit der Legaldefinition des Begriffs der "*Geschäftsleitung*" in § 2 Nr. 13 BSIG-E zu vermeidbaren Unschärfen der Vorgaben in § 38 BSIG-E. Vor dem Hintergrund, dass § 2 Nr. 13 BSIG-E den Begriff der Geschäftsleitung als "*eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist,*" definiert und § 38 BSIG-E stets auf den Plural "*Geschäftsleitungen*" rekurriert, scheint § 38 BSIG-E dem Wortlaut zufolge stets alle Mitglieder der Leitungsebene zu adressieren und allen Mitgliedern die entsprechenden Überwachungs- und

Schulungspflichten sowie die mit der Überwachungspflicht korrelierende Binnenhaftung nach § 38 Abs. 2 BSIG-E aufzuerlegen.

Da dies im Widerspruch zu gesellschaftsrechtlichen Vorgaben und der gelebten Leitungspraxis steht, sollte insofern klargestellt werden, dass § 38 BSIG-E einer geschäftsleitungsinternen Allokation der Zuständigkeit für das Thema Cybersicherheit im Rahmen einer Ressortaufteilung nicht entgegensteht und in einem solchen Fall ausschließlich der mit dieser Aufgabe betraute Geschäftsführer der jeweiligen besonders wichtigen oder wichtigen Einrichtung den Überwachungs- und Schulungspflichten des § 38 Abs. 1 und 3 BSIG-E sowie der Binnenhaftung nach § 38 Abs. 2 BSIG-E unterliegt.

Wir regen insofern an, anstelle des Plurals "*Geschäftsleitungen*" in § 38 BSIG-E den Singular "*Geschäftsleitung*" zu verwenden und die Legaldefinition in § 2 Nr. 13 BSIG-E wie folgt anzupassen:

> *„Geschäftsleitung“ eine natürliche Person **oder mehrere natürliche Personen**, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist **oder sind**;*

Adressat der Verpflichtungen aus § 38 BSIG-E wäre damit das Organ der Geschäftsleitung als solches und nicht die einzelnen Personen dieses Organs. Einer Zuständigkeitsallokation innerhalb der Geschäftsleitung stünde die Regelung in der Folge nicht mehr entgegen.

4. Verweis auf § 30 Abs. 2 Satz 3 OWiG im Falle der Verletzung der Nachweispflicht nach § 39 Abs. 1 Satz 1 BSIG-E unverhältnismäßig

In den Bußgeldregelungen wird in § 65 Abs. 5 Satz 2 BSIG-E für bestimmte Verstöße gegen die Vorschriften des BSIG-E auf die Regelung des § 30 Abs. 2 Satz 3 OWiG verwiesen. Diesen Verweis, der zu einer Verzehnfachung des jeweils angedrohten Höchstmaßes des Bußgeldes führt, halten wir für Verstöße gegen die in § 39 Abs. 1 Satz 1 BSIG geregelte Nachweispflicht für nicht verhältnismäßig.

Wir regen daher an, den Verweis auf Satz 1 Nr. 3 in § 65 Abs. 5 Satz 2 BSIG-E zu streichen.

5. Dokumentationserfordernis in § 30 Abs. 1 Satz 3 BSIG-E sollte gestrichen werden

Die in § 30 Abs. 1 Satz 3 BSIG-E geregelte Verpflichtung, die Einhaltung der Verpflichtung nach § 30 Abs. 1 Satz 1 BSIG-E zu dokumentieren, sollte gestrichen werden.

Die Dokumentationspflicht in § 30 Abs. 1 Satz 3 BSIG-E ist in ihrem Umfang zu unbestimmt und schafft unnötige Bürokratie. Sie ist darüber hinaus nicht erforderlich, da besonders wichtige Einrichtungen gemäß § 61 Abs. 3 BSIG-E auch ohne eine solche Dokumentationspflicht verpflichtet sind, auf Anforderung des Bundesamts für Sicherheit in der Informationstechnik einen Nachweis über die Erfüllung der geforderten Risikomanagementmaßnahmen zu erbringen.

6. Öffentlichkeitsbeteiligung auch hinsichtlich der Verordnungsermächtigungen in § 56 Abs. 3 und 5 BSIG-E

Analog zu unseren Forderungen zu den Verordnungsermächtigungen in § 30 Abs. 5 BSIG-E und § 56 Abs. 4 BSIG-E regen wir auch bezüglich der Ermächtigungsgrundlagen in § 56 Abs. 3 und 5 BSIG-E an, eine Verpflichtung zur Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände aufzunehmen.

Eine Beteiligung dieser Kreise ist aus unserer Sicht auch in diesen Bereichen unerlässlich, um wissenschaftliche Expertise und Praxiserfahrungen in dem erforderlichen Umfang in die Ausarbeitung der entsprechenden Verordnungen einfließen zu lassen und eine praxistaugliche und gleichzeitig ein hohes Schutzniveau gewährleistende Ausgestaltung der entsprechenden Vorgaben sicherzustellen.

7. Konkretisierung der Regelungen zur Berechnung der relevanten Einrichtungskennzahlen

In der Regelung zur Berechnung der relevanten Einrichtungskennzahlen (§ 28 Abs. 3 BSIG-E) sollte klargestellt werden, ob die geschäftstätigkeitsbezogene Betrachtung, wie sie in § 28 Abs. 3 Satz 1 Nr. 1 BSIG-E vorgeschrieben wird, auch für die Zurechnung von Kennzahlen verbundener Unternehmen und Partnerunternehmen gilt.

§ 28 Abs. 3 Satz 1 Nr. 1 BSIG-E schreibt vor, dass "*bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme […] auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen*" ist.

In der Gesetzesbegründung wird hierzu ausgeführt, dass "*bei der Bestimmung der maßgeblichen Mitarbeiterzahlen und des Umsatzes […] nur diejenigen Teile der Einrichtung einzubeziehen [sind], die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind [und dass] Querschnittsaufgaben wie beispielsweise Personal, Buchhaltung etc. […] hierbei anteilig zu berücksichtigen [sind].*" Hierdurch soll "*sichergestellt [werden], dass Einrichtungen, die insgesamt die Größenschwelle für Mitarbeiteranzahl, Jahresumsatz oder Jahresbilanzsumme überschreiten, deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden*".

Angesichts der auf einzelne juristische Personen bezogenen Legaldefinition von Einrichtungen in § 28 Abs. 1 Nr. 4 und Abs. 2 Nr. 3 BSIG-E verstehen wir die Regelung in § 28 Abs. 3 Satz 1 Nr. 1 BSIG dahingehend, dass diese für die isolierte Betrachtung einer juristischen Person gelten soll.

Offen bleibt indes, ob die auf die erfasste Geschäftstätigkeit beschränkte Betrachtung auch für die unter § 28 Abs. 3 Satz 1 Nr. 2 BSIG-E i.V.m. der KMU-Empfehlung vorzunehmende Zurechnung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme gelten soll. Hierfür spricht, dass sich die vorstehend zitierte Argumentation aus der Gesetzesbegründung auch auf die Zurechnung von Daten verbundener Unternehmen übertragen lässt.

Die insofern bestehende Regelungslücke, die die aufgrund der Verweisungssystematik der Anhänge 1 und 2 ohnehin bestehenden Rechtsunsicherheiten im Rahmen der Anwendbarkeitsprüfung erheblich verstärkt, sollte durch eine Klarstellung geschlossen werden.

***