Stiftung
Familienunternehmen und Politik

Herrn
Ministerialrat Dr. Daniel Meltzian
Leiter des Referats CI 1
Grundsatz; Cyber- und Informationssicherheit
Bundesministerium des Innern und für Heimat
11014 Berlin

Ausschließlich per E-Mail an: NIS2@bmi.bund.de

28. Mai 2024
BS

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

Sehr geehrter Herr Dr. Meltzian,
sehr geehrte Damen und Herren,

vielen Dank für die Übersendung des Referentenentwurfs für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG).

Zum derzeitigen Stand des Gesetzgebungsverfahrens erlauben wir uns, folgende Anmerkungen und Ergänzungsbitten aus dem Kreis großer Familienunternehmen einzubringen:

I. Meldepflichten

Die nationale Implementierung der NIS 2 durch die 27 EU-Mitgliedstaaten kann zu einer mehrfachen, in Teilen uneinheitlichen Berichterstattung durch die Industrie gegenüber den nationalen Behörden führen. Die Bundesregierung sollte dringend sicherstellen, dass Unternehmen nur in einem und nicht in allen EU-Mitgliedsstaaten berichten müssen. Dies reduziert zugleich den Aufwand auf der Seite der nationalen Behörden, die auf Basis der Entwurfsfassung im internationalen Austausch dieselben Informationen mehrfach erhalten und verarbeiten jeweils müssen. Alternativ vorstellbar wäre bei länderübergreifenden Vorfällen von multinationalen Konzernen eine Meldung an die Agentur der Europäischen Union für Cybersicherheit (ENISA).

II. Registrierungspflichten

Im Rahmen der Umsetzung der NIS-2-Richtlinie wird von erwartet, dass sich besonders wichtige und wichtige Einrichtungen spätestens nach drei Monate registrieren (§ 33, § 34 NIS2UmsuCG-E). Dem Vernehmen nach ist ein offizielles Internetportal für die Registrierung geplant. Eine für die Rechtspraxis ganz entscheidende Maßnahme ist die automatisierte Bereitstellung relevanter Informationen seitens staatlicher Stellen für die betroffenen Unternehmen. Hier könnte die Bundesregierung dem Beispiel anderer europäischer Länder folgen und die betroffenen Unternehmen zur Registrierung auffordern.

Um den Verwaltungsaufwand für betroffene Unternehmen mit Niederlassungen in anderen EU-Mitgliedsstaaten zu minimieren, sollten diese nur einmalig eine Bescheinigung ihrer jeweiligen nationalen Behörde vorlegen müssen, welche die europaweite Unternehmensstruktur und die einzelnen Ländergesellschaften beinhaltet, die von den zuständigen Behörden akzeptiert und an die betroffenen Behörden anderer europäischer Länder weitergeleitet wird.

Die verkürzte Frist bei Änderungen auf zwei Wochen gegenüber der Frist in der NIS-2 von drei Monaten stellt eine deutliche Erschwerung für deutsche Unternehmen dar und sollte zurückgenommen werden.

III. Managerhaftung

Es bleibt unklar, ob diese persönliche Haftung versicherbar ist und welche Schritte seitens der Aufsichtsräte, der Behörden und der Staatsanwaltschaft eingeleitet werden, wenn die Binnenhaftung nicht oder nur in Teilen eingefordert wird (Verstoß gegen § 38 Abs. 2 NIS2UmsuCG-E). Im Sinne der Rechtssicherheit ist es erforderlich, diese Fragen direkt im Regelungstext zu beantworten und nicht der künftigen Rechtsprechung zu überantworten.

IV. Umsetzung der Risikomanagementmaßnahmen

In der deutschen Gesetzgebung fehlt es bislang an einer detaillierten Erwartungshaltung gegenüber Unternehmen und Behörden, wie die in NIS2 Artikel 21 erwähnten Risikomanagementmaßnahmen in Bezug auf Kritikalität, Sektor, Unternehmensgröße und weiteren Faktoren konkret anzuwenden sind.

Die Berechnung des Aufwands für die deutsche Wirtschaft könnte ein grober Anhalt für den Umsetzungsaufwand sein, stellt jedoch keine verlässliche Informationsquelle dar. So

wird etwa angenommen, dass KRITIS-Unternehmen keinen weiteren Aufwand zur Umsetzung der NIS2 hätten. Betroffene Unternehmen teilen diese Einschätzung keinesfalls.

Auch die Annahme, auf 17 Prozent der Unternehmen würde keine zusätzlicher Umsetzungsbedarf zukommen, ist anzuzweifeln. Der Aufwand der Umsetzung der NIS-Richtlinie kann realistischerweise nicht mit dem Aufwand zur Umsetzung der NIS2-Richtlinie gleichgesetzt werden. Einzig die Annahme, dass 70 Prozent bei großen wichtigen Einrichtungen im Vergleich zu einer wesentlichen Einrichtung und 35 Prozent bei einer mittleren wichtigen Einrichtung im Vergleich zu einer wesentlichen Einrichtung einzuhalten ist, stellt einen groben Anhaltspunkt der Erwartungshaltung des Gesetzgebers dar.

Eine vom BSI erstellte Umsetzungshilfe mitsamt konkreter Erwartungshaltung gegenüber den betroffenen Einrichtungen zum Umfang der umzusetzenden Maßnahmen ist dringend erforderlich, um den Unternehmen die Möglichkeit zu geben, den Vorgaben fristgerecht nachzukommen. Eine fundiertere Berechnung der Umsetzungskosten für die betroffenen Unternehmen sowie eine Handreichung des BSI zu den erwarteten Maßnahmen würden betroffene Unternehmen in der Umsetzung erheblich unterstützen.

V. Sektoren

Bereits heute ist es für Unternehmen schwierig, mithilfe von Anhang I und II der NIS2 festzustellen, ob sie in den Anwendungsbereich fallen. Unsicherheiten ergeben sich insbesondere bei Unternehmen, die mehreren Sektoren zuzurechnen sind. In einigen Sektoren herrscht große Verunsicherung bei den Unternehmen. So könnte etwa der Terminus „Digitale Infrastruktur" alle deutschen Muttergesellschaften betreffen, die ihre Rechenzentrumsdienstleistungen ihren europäischen Tochtergesellschaften anbieten. Diese wären dann „Wesentliche Einrichtungen". Entsprechende flächendeckend vorhandenen Unklarheiten müssen im Rahmen des Gesetzgebungsverfahrens ausgeräumt werden.

Vom Sektor „Verwaltung von Informationstechnologie und Telekommunikation" etwa könnten theoretisch alle Einrichtungen betroffen sein, welche SOC-Dienstleistungen für europäische Unternehmen im Konzernverbund anbieten. Dies könnte beispielsweise dazu führen, dass das indische Tochterunternehmen aufgrund seiner SOC-Dienstleistungen NIS2-relevant wird.

Eine Klarstellung in diesen beiden Sektoren würde den deutschen Unternehmen helfen sich auf die Umsetzung als wesentliche oder wichtige Einrichtung vorzubereiten.

VI. Informationssicherheitsbeauftragter

Auf Bundesebene wird ein „CISO Bund" eingeführt. Im Rahmen der NIS2 Umsetzung bietet sich die einmalige Gelegenheit, einen verantwortlichen CISO für jede betroffene Einrichtung einzufordern, der – analog zum Datenschutzbeauftragten bei den Datenschutzbehörden – bei der Registrierung zu benennen ist.

Dabei kann der Gesetzgeber auf die bewährten Anforderungen an die operationelle Resilienz des Finanzsektors zurückgreifen und die BAIT 4.4 – 4.6 nachbilden: „Die Geschäftsleitung hat die Funktion des Informationssicherheitsbeauftragten einzurichten. Diese Funktion umfasst die Verantwortung für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber Dritten. Sie stellt sicher, dass die in der IT-Strategie, der Informationssicherheitsleitlinie und den Informationssicherheitsrichtlinien des Instituts festgelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch gegenüber Dritten transparent gemacht und deren Einhaltung regelmäßig sowie anlassbezogen überprüft und überwacht werden."

Dabei sollte der Vorgabe der Finanzinstitute gefolgt werden, dass die Funktion des Informationssicherheitsbeauftragten von den Bereichen getrennt werden, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind. Damit wird ausgeschlossen, dass der Informationssicherheitsbeauftragte dem IT-Leiter unterstellt ist. Dies beugt Interessenkonflikten entscheidend vor und unterstreicht die deutlich umfangreichere Aufgabe des Informationssicherheitsbeauftragten, die bekanntlich weit über die Belange der IT-Sicherheit hinausgehen.

Für die Berücksichtigung dieser Aspekte im weiteren Verfahren danke ich Ihnen.

Mit freundlichen Grüßen

Bernhard Stehfest
Leiter Wirtschaftspolitik

Stiftung Familienunternehmen und Politik
Haus des Familienunternehmens
Pariser Platz 6a
D-10117 Berlin

Tel: +49 (0)30 226 052 911
Fax: +49 (0)30 226 052 929
E-Mail: stehfest@familienunternehmen-politik.de
www.familienunternehmen-politik.de