Stiftung
Familienunternehmen und Politik

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

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

4. Juli 2025
BS

Stellungnahme

zum Referentenentwurf des Bundesministeriums des Innern 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)

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

vielen Dank für die Übersendung des überarbeiteten 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) in der Fassung vom 23. Juli 2025.

Aus dem Kreis großer Familienunternehmen möchten wir die folgenden Rückmeldungen zum bisherigen Entwurfsstand einbringen. Ihrer Bitte entsprechend stellen wir eine Zusammenfassung unserer Forderungen umseitig voran:

A. Zusammenfassung der Forderungen

1. **Klarstellung zu konzern- und gruppeninternen IT-Diensten vornehmen**
2. **Spezialisierte Arbeitsteilung ermöglichen: § 38 Abs. 1 BSIG-E ersatzlos streichen oder sprachlich auf die Verantwortung der Geschäftsleitung für IT-Sicherheitsmaßnahmen beschränken.**
    a. Die gesellschaftsrechtliche Legalitätspflicht bietet einen besprochenen Anknüpfungspunkt, um Geschäftsleiter auf IT-Sicherheitsmaßnahmen zu verpflichten.
    b. Eine positive Pflicht von Geschäftsleitern, IT-Sicherheitsmaßnahmen selbst umzusetzen, würde die Rolle des Geschäftsleiters mit der Rolle einer Fachkraft vermischen. Dies betrieblich umzusetzen, ist weder möglich noch zweckmäßig.
    c. Ein Geschäftsführer, der die Umsetzung eigener Maßnahmen selbst überwachen müsste, würde von internationalen Revisionsstandards abkehren. Das BSIG-E darf Sicherheitssysteme nicht negativ verändern.
3. **Normenklarheit: Turnus der Schulungen von Geschäftsleitern im Gesetz regeln.**
4. **Sicherheit als Organisationsziel durch einen unabhängigen Sicherheitsbeauftragten gewährleisten.**
    a. Die BAIT bieten eine Vorlage für eine sinnvolle Rolle, an welche Sicherheitsmaßnahmen delegiert werden können.
    b. Ein starker Sicherheitsbeauftragter macht problematische behördliche Eingriffe in die Betriebsorganisation weitgehend entbehrlich.
5. **Kreative Lösungsfindung statt behördlicher Normung von Unternehmen – keine allgemeine Weisungsbefugnis des BSI im Bereich des betrieblichen Risikomanagements.**
6. **Keine „Wall of Shame": Nach einer Meldung eines Sicherheitsvorfalls darf ein Unternehmen keinen behördlichen Pranger fürchten müssen.**
7. **Keine unnötige Bürokratielast in der Krise: Eine Meldung für alles als Maßgabe!**
    a. Die Belastung von Unternehmen durch die Meldepflichten wird im Entwurf um mindestens den Faktor 7 unterschätzt.
    b. Integrierte Sicherheit bedeutet, Aufgaben nicht abzuwälzen, sondern Unternehmen in der Krise staatliche Unterstützung zukommen zu lassen.
    c. Jedenfalls muss der Staat aber bürokratische Lasten, die er selbst geschaffen hat, in der Krise aussetzen oder abfedern.

Einleitend merken wir kritisch an, dass der öffentliche Sektor zum weit überwiegenden Teil nicht von den Maßgaben des vorliegenden Entwurfs erfasst ist. Damit sendet der Entwurfsverfasser unfreiwillig ein fatales Signal – an die insoweit regulierte Privatwirtschaft sowie an andere Industrienationen, denen gegenüber wir den Anspruch der „Cybernation Deutschland" erheben. Für eine erfolgreiche Wirtschaft brauchen wir auf allen staatlichen Ebenen eine funktionieren Verwaltung. Diesem Anspruch muss sich der öffentliche Sektor spätestens im Lichte der durch NIS-2 geschaffenen Standards stellen. Hier geht vom Vorhaben der Bundesregierung ein negatives Signal aus, der Wirtschaft einseitig Belastungen aufzubürden, die man beispielsweise den Kommunen nicht zumuten möchte.

B. Im Einzelnen

I. Präzise Klarstellung zu konzern- und gruppeninternen IT-Diensten erforderlich

Bei der Zuordnung zu den Einrichtungsarten der Anlagen 1 und 2 ist eine Klarstellung mit Blick auf solche IT-Dienste erforderlich, die innerhalb einer Gruppe bzw. eines Konzerns erbracht werden. Nach dem bisherigen Wortlaut der Definitionen in § 2 BSIG-E und der entsprechenden Gesetzesbegründung könnte beispielsweise eine IT-Tochtergesellschaft als „Anbieter von Rechenzentrumsdiensten", „Managed Services Provider", „Managed Security Services Provider" und ggf. als „Anbieter von Cloud-Computing-Diensten" gelten, nur weil sie zentralen IT-Dienste im eigenen Konzern erbringt.

Dies hätte zunächst zur Folge, dass viele Unternehmen, die bisher (lediglich) als „wichtige Einrichtung" einzuordnen waren, kurzum zu „besonders wichtigen Einrichtungen" im digitalen Sektor werden. Noch problematischer wird es für Unternehmen aus Sektoren, die über NIS-2 gar nicht erfasst werden: Diese würden plötzlich den „besonders wichtigen Einrichtungen" zugeordnet. Die damit verbundene Ausdehnung des Anwendungsbereichs würde eine Vervielfachung der vom Gesetz erfassten Unternehmen bedeuten. Damit würde zugleich die detaillierte Klassifizierung der Anhänge 1 und 2 nach Sektoren, Branchen und Einrichtungsarten ad absurdum geführt. Das Umsetzungsgesetz würde dem klar umrissenen Regelungskreis der NIS-2-Richtlinie nicht mehr gerecht werden. Hinzu kommt: Denkbare Ausweichbewegungen in der Unternehmenspraxis, wie die Auslagerung der IT-Dienste an Externe, würden dem legislativen Ziel einer generellen Steigerung der Cyber-Resilienz der europäischen Wirtschaft erkennbar zuwiderlaufen. Das kann nicht gewollt sein.

Um diesen Zielkonflikt aufzulösen, sind dringend präzise Klarstellungen in der Begründung zu § 2 Ziff. 25, 26 und 35 BSIG-E zu jenen IT-Diensten erforderlich, die in einer Konzern- oder Gruppenstruktur aufgehangen sind. Insbesondere in der Begründung zu Ziff. 26 sollte klargestellt werden, dass es für die Klassifizierung als MSP maßgeblich ist, ob es sich bei den jeweiligen Kunden des betreffenden Unternehmens ihrerseits um NIS-2-relevante Unternehmen handelt oder nicht – egal ob im Konzernverbund oder als externe Kunden. Nur auf diese Weise wird der nationale Gesetzgeber dem Adressatenkreis gerecht, den die NIS-2 anhand ihrer Definitionen und Klassifizierungen vorgibt.

II. Pflichten der Geschäftsführung – Kohärenz sicherstellen, Bewährtes erhalten

Die Regelungsvorschläge zu den Pflichten der Geschäftsführer im Umgang mit IT-Sicherheitsrisiken werden in Deutschlands großen Familienunternehmen weiterhin mit größter Sorge gesehen, weil der aktuelle Regelungsentwurf Unternehmen zwingt, von internationalen Standards abzukehren.

1. Streichung des Verzichtsverbots zu begrüßen

Dahingehend begrüßen die Familienunternehmen, dass der Referentenentwurf von einem Verzichtsverbot auf entsprechende Organhaftungsansprüche Abstand genommen hat. Ein solches Verbot hätte unzweckmäßige Interessengegensätze innerhalb der Unternehmen begründet, welche nun vermieden werden. Familienunternehmer sind stolz darauf, auch mit Geschäftsführern und Arbeitnehmern vertrauensvoll zusammenzuarbeiten und erleichtert, dass diese Beziehung durch das BSIG-E nicht belastet werden soll.

2. Klare Regeln des Gesellschaftsrechts nicht durch Sonderrecht aufbrechen

Aus Sicht der Familienunternehmen ist die nun im Entwurf vorgelegte Regelung in einem anderen Punkt systemwidrig und schafft dadurch unnötige Auslegungsschwierigkeiten. Es ist nicht erforderlich, die Pflichten von Geschäftsleitern im Umgang mit dem BSIG-E spezialgesetzlich zu regeln. Das allgemeine Gesellschaftsrecht verpflichtet Geschäftsleiter bereits in Form der „äußeren Legalitätspflicht" auf die Einhaltung der Vorgaben des BSIG-E. Es ist ferner besprochenes Recht, dass Geschäftsleitern die Gesamtverantwortung für die Einhaltung rechtlicher Pflichten im Unternehmen obliegt und ihnen auch bei einer Delegation von Aufgaben an nachgeordnete Mitarbeiter eine Restverantwortung in Form einer Legalitätskontrollpflicht verbleibt. Dieser bewährte und in der Praxis erprobte Regelungskanon des Gesellschaftsrechts ist Grundlage anspruchsvoller und effizienter Compliance- und Risikomanagementsysteme, die in Familienunternehmen erfolgreich praktiziert werden. Eine spezialgesetzliche Regelung im BSIG-E würde solche Systeme in einem spezifischen Teilbereich infrage stellen und ihre Ausgestaltung mit schwierigen rechtlichen Auslegungsfragen belasten. Dies ist weder erforderlich noch zweckmäßig. Der Entwurf sollte von einer spezialgesetzlichen Ausgestaltung der Pflichten von Geschäftsleitern Abstand nehmen und stattdessen an Bewährtem anknüpfen. Dass das allgemeine Gesellschaftsrecht ausreicht, um die unionsrechtlichen Anforderungen zu erfüllen, zeigt im Übrigen die Neufassung des § 38 Abs. 2 BSIG-E ausdrücklich. Hier gilt der Grundsatz: Wenn es nicht erforderlich ist, ein Gesetz zu erlassen, dann ist es erforderlich, kein Gesetz zu erlassen.

3. Expertise erhalten: Rollen von Geschäftsleitern und Spezialisten nicht vermischen

Noch dazu ist die Regelung schlechthin nicht praktikabel. Die Anforderung an Geschäftsleiter, IT-Sicherheitsmaßnahmen „umzusetzen", entfernt sich von dem gesellschaftsrechtlichen Prinzip, anstelle einer Handlungspflicht von Geschäftsleitern eine Gesamtverantwortung vorzusehen. Geschäftsleiter sind keine IT-Systemadministratoren und sollten – zumindest im eigenen Verantwortungsbereich – auch keine sein. Geschäftsleiter positiv zur Umsetzung aller IT-Sicherheitsmaßnahmen zu verpflichten, verpflichtet diese in der Sache zu etwas Unmöglichem: Selbst kleinere Familienunternehmen unterhalten ganze

Teams für die Umsetzung von IT-Sicherheitsmaßnahmen. Geschäftsleiter können diese Teams nicht ersetzen. Dies hätte auch keinen Mehrwert. So sinnvoll es ist, Geschäftsführer für Cybersicherheit zu sensibilisieren, so wenig zweckmäßig ist eine positive Handlungspflicht in diesem Bereich. Hierfür gibt es bereits Spezialisten.

4. Internationale Standards nicht gefährden

Zuletzt begegnet der aktuelle Regelungsentwurf Bedenken, weil er mit internationalen Best Practices nicht vereinbar ist. Familienunternehmen, welche aktuell bereits hocheffiziente Sicherheitsmanagementsysteme betreiben, befürchten diese zum Negativen verändern zu müssen, wenn der Entwurf Gesetz würde. Effiziente Sicherheitsorganisationen der Unternehmen orientieren sich in aller Regel an der internationalen Best Practice des sogenannten Drei-Linien-Modells (three lines of defense). In der Praxis deutscher Familienunternehmen ist es längst Standard: Die erste (Verteidigungs-)Linie bilden die Fachabteilungen eines Unternehmens. Sie tragen die Umsatzverantwortung und entscheiden über das Risikomanagement in ihren Bereichen. Diese erste Linie wird bei risikorelevanten Entscheidungen von der zweiten Linie unterstützt, welche fachkundige Expertise verfügbar macht und Risiken überwacht. Diese beiden Linien arbeiten eng zusammen und sorgen dafür, dass Risikomanagemententscheidungen mit den geschäftlichen Interessen von Unternehmen abgestimmt sind. Wesentlich ist deshalb die dritte Linie: Diese beschreibt die Revision der Risikomanagementmaßnahmen und ist von den geschäftlichen Abteilungen unabhängig. Sie wird umschrieben als „Auge und Ohr" der Geschäftsleitung im eigenen Unternehmen. Dabei ist ihre Unabhängigkeit von den unternehmerischen Fachabteilungen Grundlage ihrer Neutralität und Effizienz: Der Überwacher darf nicht seine eigenen Entscheidungen überprüfen. Ansonsten liefe eine Überwachung leer und brächte keinen Mehrwert. Exakt dies verlangt der Entwurf allerdings von Geschäftsleitern: Sie sollen IT-Sicherheitsmaßnahmen einerseits positiv „umsetzen", gleichsam aber – ihre eigene (!) – Umsetzung überwachen. Dies ist mit fachlichen Standards für Risikomanagementsysteme schlechthin unvereinbar und sollte überdacht werden.

5. Rechtssicherheit wahren: Widerspruch zum Unionsrecht vermeiden

Zuletzt möchten wir darauf hinweisen, dass die Regelung des § 38 Abs. 1 BSIG-E mit den Anforderungen des Entwurfs des Durchführungsrechtsaktes zur NIS-2 RL in Widerspruch steht: Gemäß Ziffer 1.2.3 des Anhangs zum Durchführungsrechtsakt (Ares(2024)4640447) ist eine Delegation sogar unionsrechtlich erforderlich:

> *„At least one person shall report directly to the management bodies on matters of network and information system security."*

Wenn § 38 Abs. 1 BSIG-E überhaupt erhalten bleiben sollte, wäre es aus Sicht der Familienunternehmen erforderlich, ihn wie folgt zu formulieren:

> *„(…) die Umsetzung der (…) Risikomanagementmaßnahmen sowie deren Überwachung zu verantworten."*

6. Normenklarheit: Turnus der Schulungen ins Gesetz statt in die Begründung

Familienunternehmen ist ferner an einheitlichen Standards gelegen, deren Nachweis gegenüber einer Aufsichtsbehörde möglichst unkompliziert ist und keinen unnötigen bürokratischen Aufwand auslöst. Auch in dieser Hinsicht bietet der aktuelle Entwurf Gelegenheit zur Klarstellung: Der Referentenentwurf sieht vor, dass sich Geschäftsleiter „regelmäßigen Schulungen" zur IT-Sicherheit unterziehen sollen. Dies basiert auf Art. 20 Abs. 2 der NIS-2-Richtlinie. Dahingehend existieren verschiedene Auslegungen, wie ein solches Schulungssystem auszugestalten ist. Der Referentenentwurf weist lediglich in der Begründung zu § 38 Abs. 3 BSIG-E aus, dass mindestens aller drei Jahre Schulungen stattfinden sollen. Weil der erforderliche Turnus dieser Schulungen unionsrechtlich nicht vorgezeichnet ist, sollte der Bundesgesetzgeber seinen Umsetzungsspielraum nutzen, um für die betroffenen Unternehmen Verbindlichkeit zu schaffen: Der Turnus von drei Jahren ist überzeugend, aber er gehört in das Gesetz, nicht lediglich in die Gesetzesbegründung.

III. Alternativvorschlag: Der Sicherheitsbeauftragte

Um Unternehmenssicherheit als Organisationsziel zu gewährleisten, bietet sich eine Alternative, welche auch die Vereinbarkeit mit internationalen Normen und Standards sicherstellt: Die Einführung eines Sicherheitsbeauftragten in Unternehmen nach dem Vorbild des CISO-Bund.

Im Rahmen der Umsetzung der NIS-2-Richtlinie bietet sich die einmalige Gelegenheit, einen verantwortlichen CSO für jede betroffene Einrichtung einzufordern, der – analog zum Datenschutzbeauftragten bei den Datenschutzbehörden – bei der Registrierung zu benennen ist. Hiermit würde der nationale Gesetzgeber einen guten Gedanken aus dem Durchführungsrechtsakt zur NIS-2-Richtlinie aufgreifen.

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.*" Da ebenfalls die Umsetzung der CER-Richtlinie bevorsteht, könnte der dort vorgesehen Informationssicherheitsbeauftragte durch den Sicherheitsbeauftragten ersetzt werden, wodurch auch seine Befassung mit der physischen Unternehmenssicherheit sichergestellt wäre.

Dabei sollte der Vorgabe der Finanzinstitute gefolgt werden, dass die Funktion des Sicherheitsbeauftragten unabhängig ist. Damit wird ausgeschlossen, dass der Sicherheitsbeauftragte, so wie es in der IT noch zu häufig geschieht, einem Fachbereichsleiter unterstellt wird. Dies beugt Interessenkonflikten entscheidend vor und verankert die Gewährleistung internationaler Organisationsstandards im Gesetz.

IV. Meldepflichten – Sicherheitspartnerschaft statt Abwälzen von Aufgaben

Die Meldepflichten in Umsetzung des BSIG-E werden die Familienunternehmen administrativ stark belasten, was vom Bundesgesetzgeber bei der Ausgestaltung der Regelungen zu berücksichtigen ist. Hier gilt: Die administrative Belastung der Unternehmen aufgrund der Meldepflichten muss auf ein Mindestmaß reduziert werden. Unternehmen müssen Anreize für eine Meldung haben, anstatt im Falle einer Meldung mit rechtlichen Risiken belastet zu werden.

1. Die bürokratische Belastung ist um den Faktor 7 zu niedrig geschätzt

Eine Verprobung der Maßstäbe aus dem Durchführungsrechtsakt der Union zur NIS-2-Richtlinie zeigt: Die betroffenen Unternehmen werden deutlich weitergehend Meldungen vornehmen müssen, als ursprünglich gedacht. Die Schätzungen der Verwaltung sind dahingehend deutlich zu niedrig. Ein mittelgroßes Familienunternehmen allein kommt aufgrund der Definition der Europäischen Union zu zwei abgewehrten, aber meldepflichtigen Vorfällen an einem durchschnittlichen Werktag. Die Fallzahl von 2.400 zusätzlichen Meldungen aufgrund des Gesetzesvollzugs wird nicht zu halten sein. Sie widerspricht ferner den Verlautbarungen des BSI. Das Bundesamt zitiert seine Präsidentin in einer Meldung vom 14.03.2024 selbst mit den Worten „Die Gefährdungslage ist so hoch wie nie", sodass sich nicht die Frage stelle, ob ein Cyberangriff auf ein Unternehmen erfolgreich sei, sondern nur noch, wann dies geschehe. In diesem Kontext anzunehmen, dass lediglich ca. 10 Prozent der zusätzlich regulierten Unternehmen pro Jahr einen meldepflichtigen Vorfall erleiden werden, widerspricht der Realität. Auch der Branchenverband Bitkom gibt an, dass ca. 80 Prozent der befragten Unternehmen im letzten Jahr entweder nachweislich oder vermutlich von einem Cyberangriff betroffen waren. Schon diese Zahlen legen nahe, dass nicht mit 2.950 Meldungen zu rechnen ist, sondern mit ca. 20.000. Allein aufgrund der öffentlich verfügbaren Zahlen unterschätzt der Referentenentwurf die Herausforderungen, vor denen Unternehmen stehen, um den Faktor 7!

Die tatsächlichen Zahlen in Familienunternehmen zeigen jedoch: Auch dies dürfte noch eine konservative Schätzung sein. Ein durchschnittlich großes Familienunternehmen hätte für den zurückliegenden Zeitraum ca. 700 Vorfälle verzeichnet, welches es zwar abwehren konnte, jedoch nach künftiger Rechtslage würde melden müssen. Auch der Aufwand für diese Meldungen übersteigt die Schätzung im Referentenentwurf deutlich. Das aktuelle BSIG sieht eine Meldung vor, der Entwurf jedoch drei: Eine Erstmeldung, eine aktualisierte Folgemeldung nach 72 Stunden und eine „ausführliche" (sic!) Abschlussmeldung. Die Folgemeldung und die ausführliche Abschlussmeldung sollen insgesamt einen Aufwand von 2,25 Personenstunden verursachen. Die betriebliche Praxis geht jedoch von mindestens 20 Personenstunden aus, von denen ein Großteil auf die „ausführliche" Abschlussmeldung entfällt.

Aus Sicht der Familienunternehmen ist deshalb klar: Die Resilienz der deutschen Wirtschaft gegenüber IT-Sicherheitsrisiken muss gewährleistet sein. Allerdings müssen die daraus resultierenden Belastungen offen besprochen werden. Der aktuelle Entwurf zeigt, dass der aus dem Gesetz resultierende Bürokratieaufbau nicht ausreichend bewusst ist.

2. Schutz statt Überlastung: eine Meldung für alles

Die Meldepflichten drohen in ihrer aktuellen Fassung zu einer bürokratischen Hürde für Unternehmen zu werden, die sie an einem vulnerablen Punkt belastet. Dies widerspricht der Nationalen Sicherheitsstrategie, welche integrierte Sicherheit als Ziel vorgibt. Leitbild des Verhältnisses zwischen Unternehmen und BSI sollte nach Ansicht der Familienunternehmen eine Sicherheitspartnerschaft sein. In einer solchen sollte jeder nach seinen Möglichkeiten einen Beitrag leisten. Das Abwälzen von Aufgaben auf Unternehmen, welche der Staat übernehmen könnte, wäre mit diesem Leitbild unvereinbar.

Aus Sicht der Familienunternehmen ist deshalb bereits bedauerlich, dass auf europäischer Ebene überhaupt einer Pflicht der Unternehmen zugestimmt wurde, Sicherheitsvorfälle zu melden und dazu auch noch für die Sicherheitsbehörden auszuwerten. Die Analyse der Bedrohungslage ist eine originär hoheitliche und staatliche Aufgabe, welche nur dort auf Unternehmen übertragen werden sollte, wo dies zwingend erforderlich ist.

Zumindest ist es aber nun am nationalen Gesetzgeber, den Eingriff in die Betriebsabläufe von Unternehmen durch diese Meldepflicht so gering wie möglich zu halten. Hiermit entspricht er nicht nur einem dringenden Erfordernis der Unternehmen, sondern erfüllt ebenfalls die Maßgaben des europäischen Gesetzgebers: Dieser gab ausdrücklich ein, dass die Meldepflicht nicht dazu führen darf, dass ein angegriffenes Unternehmen Ressourcen von der Krisenbewältigung abzieht und auf die Erfüllung bürokratischer Pflichten umlenkt (ErwG 102 NIS-2 RL). Daraus folgen zwei Forderungen:

Das Bundesamt sollte betroffene Unternehmen erstens proaktiv unterstützen. Insoweit ist der klarstellende Verweis im neu eingefügten § 32 Abs. 6 BSIG-E zu begrüßen, dass das Bundesamt der meldenden Einrichtungen nach § 32 Abs. 1 S. 2 BSIG-E Unterstützungsangebote bei der Behebung des Sicherheitsvorfalls machen kann. Wenn z. B. ein Datenverarbeitungssystem ausgefallen ist, sollte das Bundesamt die im hoheitlichen Interesse liegende Meldepflicht auch als solche begreifen und das betroffene Unternehmen bei der Meldung und Aufbereitung der relevanten Informationen durch eigene Ressourcen unterstützen. Das rollende Forensik-Labor des LKA NRW weist in diesem Rahmen den Weg. Der Bund sollte in seinen Fähigkeiten und Bemühungen nicht dahinter zurückstehen.

Zweitens sollte das Prinzip „eine Meldung für alles" etabliert werden. Unternehmen, welche von einer Cyberattacke betroffen sind, werden in aller Regel aus den eigenen Systemen ausgeschlossen. In dieser Situation darf der Gesetzgeber Unternehmen nicht an bürokratischen Meldepflichten festhalten, die er durch die staatlichen Strukturen selbst geschaffen hat und die in der Krise umso schwerer zu erfüllen sind. Vielmehr muss er sich als verlässlicher Sicherheitspartner zeigen. Wenigstens sollte es deshalb dem Bundesamt obliegen, die relevanten Meldungen gegenüber allen erforderlichen Stellen abzugeben, damit das betroffene Unternehmen die Krisenreaktion priorisieren kann.

Dieser Grundsatz muss nach Ansicht der Familienunternehmen nicht nur für die Umsetzung der NIS-2 Richtlinie in nationales Recht gelten, sondern zu einem Grundsatz aller Gesetze zur betrieblichen IT-Sicherheit werden.

3. Angst vor Reputationsschäden bei Zusammenarbeit mit Behörde vermeiden

Kritisch sehen Familienunternehmen im Bereich der Meldepflichten zuletzt die Regelung des § 36 Abs. 2 BSIG-E. Diese Regelung wird teilweise dahingehend verstanden, dass sie Grundlage einer „Wall of Shame" für Unternehmen wird, die von Sicherheitsvorfällen betroffen sind – ähnlich der Plattform, welche die BaFin betreibt. Dies darf aus Sicht der Familienunternehmen nicht geschehen. Es muss klar vor Augen stehen, dass Unternehmen, die von einem Sicherheitsvorfall betroffen sind, nahezu immer eines sind: Opfer eines Angriffs durch organisierte Kriminelle oder staatliche oder zumindest staatsnahe Stellen. Würde für diesen Fall eine „Wall of Shame" geschaffen, würde die Weisheit „Wer den Schaden hat, braucht für den Spott nicht zu sorgen" in Gesetzesform gegossen. Es liegt ferner auf der Hand, dass dies den fatalen Anreiz setzen würde, Sicherheitsvorfälle im Zweifel nicht zu melden. An dieser Stelle sind Unternehmen zurecht sehr sensibel: Aus dem Imageverlust infolge eines Cyberangriffs resultiert mit einem Anteil an den Gesamtschäden in Höhe von ca. 17 Prozent der größte themenbezogene Schadensposten, – welcher zudem schnell wächst. Die Meldepflicht muss auf diese Interessen- und Sachlage abgestimmt werden und Anreize für eine Meldung von Sicherheitsvorfällen setzen, statt Anreize gegen eine solche Meldung. Dafür sollte die Regelung klargestellt werden: Der Umfang der Information der Öffentlichkeit sollte definiert und auf die Inhalte, welche für die Verhinderung oder Bewältigung eines Sicherheitsvorfalls unbedingt erforderlich sind, beschränkt werden.

V. Fremdkörper im Risikomanagement: Anordnungsbefugnis des Bundesamts

Seitens der Familienunternehmen stößt ferner die Befugnis des Bundesamts nach §§ 61 Abs. 6, 62 BSIG-E, Sicherheitsmaßnahmen zu verfügen, auf Bedenken. Denn diese Norm ist entgrenzt. Hier droht eine Situation, in welcher sich das Bundesamt als „besserer Kaufmann" geriert – was nicht Sinn der Sache ist.

Es ist Standard und Ausweis eines jeden guten Sicherheitsmanagementsystems, dass es – durch den PDCA-Kreislauf – dynamisiert und individuell ist. Dies entspricht auch den Maßgaben des Bundesamts selbst. Im Kern betrifft ein ISMS allerdings Prognoseentscheidungen: Ein Risiko kann sich verwirklichen oder eben nicht. Dies ist erst im Nachhinein bekannt. In Teilbereichen eines ISMS gibt es schlicht keine eindeutige Handlungsempfehlung. Eine Norm, welche nach ihrem Wortlaut dem Bundesamt erlaubt, auch in solchen Situationen unternehmerisch-kreative Lösungsfindung einzuschränken, ist abzulehnen.

Stattdessen sollte die Norm auf das konzentriert werden, was sinnvoll ist: Grundlegenden Sicherheitslücken vorzubeugen. Hierzu ist eine Einschränkung erforderlich. Entweder sollte das Bundesamt nur solche Maßnahmen anordnen können, welche grundlegenden Mängeln der Sicherheitsorganisation begegnen oder solche Maßnahmen, welche Sicherheitslücken, die auch Dritte betreffen oder gefährden, schließen. Das Bundesamt sollte jedoch nicht grundlegend weisungsbefugt gegenüber Unternehmen im Bereich des Managements von IT-Sicherheitsrisiken sein.

VI. Untersagung der Geschäftsleitung sollte Ultima ratio bleiben

Aus ähnlichen Gründen sehen die Familienunternehmen die Möglichkeit der Aufsichtsbehörden, Geschäftsleitern die Tätigkeit zu untersagen, kritisch. Hier ist relevant, dass eine solche Untersagung nach dem Wortlaut des Gesetzes auch dann infrage kommt, wenn ein Unternehmen den Vorschlägen eines Auditors, welche sich das Bundesamt nach § 61 Abs. 3 BSIG-E zu eigen macht, fachlich entgegentritt. Aus Sicht der Unternehmen ist eine solche Untersagung der Geschäftsleitung nicht erforderlich, wenn ein unabhängiger Sicherheitsbeauftragter intern vorhanden ist, der notfalls mit Entscheidungsbefugnis ausgestattet werden könnte. Aus Sicht der Familienunternehmen ist wesentlich, die vertrauensvolle betriebsinterne Zusammenarbeit möglichst weitgehend zu schützen. Die Untersagung der Geschäftsleitung sollte unbedingt auf Fälle grundlegender und nachhaltiger Sicherheits- oder Organisationsmängel beschränkt sein.

VII. Registrierungs- und Unterrichtungspflichten

1. Rechtsunsicherheit nicht auf Private abwälzen

Im Rahmen der Umsetzung der NIS-2-Richtlinie wird von Unternehmen erwartet, dass sich besonders wichtige und wichtige Einrichtungen spätestens nach drei Monate registrieren (§ 33, § 34 BSIG-E). Dem Vernehmen nach ist ein offizielles Internetportal für die Registrierung geplant. Eine für die Rechtspraxis entscheidende Maßnahme ist die automatisierte Bereitstellung relevanter Informationen seitens staatlicher Stellen für die betroffenen Unternehmen. Hier sollte die Bundesregierung den Bemühungen von Nachbarländern der Bundesrepublik nicht nachstehen: Die Französische Republik nutzt die NIS-2-Umsetzung, um die Regulierung der Cybersicherheit in Frankreich insgesamt zu prüfen, zu homogenisieren und zu vereinfachen. Hierzu wird ein besonderes Augenmerk auf die behördenübergreifende Zusammenarbeit gelegt. Da aus den zersplitterten Zuständigkeiten von Behörden in Deutschland erhebliche Bürokratiebelastung resultiert, sollte auch die Bundesrepublik diesen Ansatz wählen. Hierzu zählt insbesondere, dass Unternehmen nicht mit einer Prüfung belastet werden sollten, wenn die erforderlichen Daten an anderer Stelle bereits staatlich erhoben wurden oder vorhanden sind. Das Königreich der Niederlande stellt Unternehmen ferner einen digitalen „Self Check" zur Verfügung, mittels welchem überprüft werden kann, ob ein Unternehmen – zumindest aus Sicht der Verwaltung – der Regulierung unterliegt oder nicht. Außerdem kann der eigene Umsetzungsstand in Bezug auf die regulativ erforderlichen Maßnahmen eingeschätzt werden. Auch solche niedrigschwelligen Angebote sollte die Bundesrepublik nutzen, um die administrative Belastung der Vielzahl der betroffenen Unternehmen abzumildern.

Um den Verwaltungsaufwand für betroffene Unternehmen mit Niederlassungen in anderen EU-Mitgliedsstaaten zu minimieren, sollten diese außerdem 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.

2. Gesetzesbegründung zu Unterrichtungsfrist dem Wortlaut anpassen

In der Begründung zu § 34 Abs. 2 BSIG-E ist noch eine redaktionelle Änderung erforderlich. Während im Wortlaut der Norm davon die Rede ist, dass die Einrichtungen das Bundesamt „*unverzüglich über diese Änderung, jedoch spätestens innerhalb von drei Monaten ab dem Tag, an dem die Änderung eingetreten ist*" unterrichten müssen, ist in der Begründung noch immer folgender Wortlaut aufgeführt: „*unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt der Änderung dem Bundesamt zu übermitteln sind*". Die Begründung sollte nun dem Normtext entsprechend angepasst werden.

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