Institut der Wirtschaftsprüfer
in Deutschland e. V.

Wirtschaftsprüferhaus
Tersteegenstraße 14
40474 Düsseldorf
Postfach 32 05 80
40420 Düsseldorf

TELEFONZENTRALE:
+49 (0) 211 / 45 61 - 0
FAX GESCHÄFTSLEITUNG:
+49 (0) 211 / 4 54 10 97
INTERNET:
www.idw.de
E-MAIL:
info@idw.de
BANKVERBINDUNG:
Deutsche Bank AG Düsseldorf
IBAN: DE53 3007 0010 0748 0213 00
BIC: DEUTDEDDXXX
USt-ID Nummer: DE119353203

Bundesministerium des Innern und für Heimat

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

Düsseldorf, 24.05.2024
624/550

IDW Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) 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 geehrte Damen und Herren,

mit diesem Schreiben nehmen wir zum Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) 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) Stellung.

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW), gegründet 1932, repräsentiert rd. 13.000 Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften, damit etwa 80 % aller deutschen Wirtschaftsprüfer. Die Mitgliedschaft ist freiwillig. Das IDW wahrt die Interessen seiner Mitglieder, unterstützt deren Berufsausübung durch fachlichen Rat und berufsständische Standards, fördert die Aus- und Fortbildung der Wirtschaftsprüfer und ihres Nachwuchses und leistet umfassenden Mitgliederservice. Themen der Rechnungslegung und Prüfung, des Steuer- und Berufsrechts sowie der betriebswirtschaftlichen Beratung sind Gegenstand der Tätigkeit des IDW.

Wir begrüßen ausdrücklich, dass mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG die unionsrechtlichen Vorgaben der

NIS-2-Richtlinie insbesondere im Rahmen einer Novellierung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) umgesetzt werden und mit der beabsichtigten Neufassung des BSI-Gesetzes eine übersichtlichere Struktur in Folge einer neuen Gliederung bestehender Vorschriften geschaffen wird.

Unsere Mitglieder, d.h. Wirtschaftsprüfer*innen und Wirtschaftsprüfungsgesellschaften, führen Prüfungen bei den Betreibern Kritischer Infrastrukturen nach § 8a Abs. 3 BSIG unter Anwendung des *IDW Prüfungshinweises: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Abs. 1 und § 8a Abs. 1a BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2 n.F.) (11.2023)* durch. Ebenso beraten sie Betreiber Kritischer Infrastrukturen bei der Einrichtung und Aufrechterhaltung von angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Die bei diesen Prüfungen und Beratungen gewonnenen Erkenntnisse unserer Mitglieder sind in die in dieser Stellungnahme dargestellten Anmerkungen eingeflossen.

Dies vorausgeschickt, nehmen wir zum Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) 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) im Einzelnen wie folgt Stellung:

Zu § 28 Abs. 5 BSIG – Finanz- und Versicherungswesen

In § 28 Abs. 5 BSIG wird ein Großteil des Finanz- und Versicherungswesens über einen entsprechenden Verweis auf die Verordnung (EU) 2022/2554 (DORA) von den §§ 30, 31, 32, 35, 36, 38 und 39 BSIG ausgenommen.

Der Referentenentwurf verwendet jedoch weiterhin den Begriff des Betreibers kritischer Anlagen. Eine kritische Anlage bestimmt sich nach § 2 Abs. 1 Nr. 21 i.V.m. § 28 Abs. 7 BSIG. Hier wird das Finanz- und Versicherungswesen explizit genannt.

Auch in Anlage 1 „Sektoren besonders wichtiger und wichtiger Einrichtungen“ werden einzelne Einrichtungsarten (Kreditinstitute, Handelsplätze und

Gegenparteien), welche wiederum alle unter den Anwendungsbereich von DORA fallen, explizit genannt.

Möglicherweise fallen also diverse Unternehmen des Finanz- und Versicherungswesens als Betreiber einer kritischen Anlage über die Rechtsverordnung nach § 58 BSIG doch in den Anwendungsbereich und die Ausnahme von den §§ 30, 31, 32, 35, 36, 38 und 39 BSIG gilt für diese nicht.

Wir regen daher an, die in § 28 Abs. 5 BSIG aufgenommene Regelung für den Finanz- und Versicherungssektor weiter zu präzisieren, um Sicherheit für den Sektor sowie insbesondere für Betreiber einer kritischen Anlage (nach der aktuell gültigen Fassung des BSIG) zu schaffen.

Zu § 28 Abs. 5 BSIG – IKT-Drittdienstleister

§ 28 Abs. 5 BSIG verweist explizit auf Artikel 2 Abs. 2 der Verordnung (EU) 2022/2554 (DORA). IKT-Drittdienstleister gemäß DORA sind von der Ausnahme bzgl. der §§ 30, 31, 32, 35, 36, 38 und 39 BSIG somit nicht erfasst.

Einzelne Unternehmen, welche als IKT-Drittdienstleister im Finanz- und Versicherungswesen tätig sind, sind möglicherweise durch das BSIG als auch – über ihre Kunden – durch DORA reguliert.

Die Folgen für IKT-Drittdienstleister, welche (nach aktuell gültiger Fassung des BSIG) Betreiber einer kritischen Anlage im Sektor Finanz- und Versicherungswesen (ggf. aber nicht zwangsläufig auch im Sektor Informationstechnik und Telekommunikation) sind, bleiben unklar.

Wir regen daher an, die in § 28 Abs. 5 BSIG aufgenommene Regelung für den Finanz- und Versicherungssektor im Hinblick auf den Umgang mit IKT-Drittdienstleistern weiter zu präzisieren, um Sicherheit für IKT-Drittdienstleister im Finanz- und Versicherungssektor zu schaffen.

Zu § 39 Abs. 1 BSIG – Nachweispflichtige Einrichtungen

§ 39 Abs. 1 BSIG sieht einen Nachweis der Erfüllung der Anforderungen nach § 30 Abs. 1 BSIG nur für Betreiber kritischer Anlagen vor.

Um eine wirksame flächendeckende Steigerung des Sicherheitsniveaus in der deutschen Wirtschaft zu erreichen, halten wir eine Begrenzung der Nachweispflichten auf den Kreis der Betreiber kritischer Anlagen für nicht ausreichend. Vor dem Hintergrund der gesteigerten Cyberbedrohungslage sollte auch eine nachhaltige Steigerung der Resilienz der besonders wichtigen Einrichtungen

erfolgen. Ein wesentlicher qualitätsbestimmender Faktor hierfür ist eine bestehende Nachweispflicht über die Einhaltung der vorgeschriebenen technischen und organisatorischen Maßnahmen.

Die gemäß § 39 Abs. 1 Satz 2 BSIG vorgesehene Nachweiserbringung durch Sicherheitsaudits, Prüfungen oder Zertifizierungen stellt hierbei eine externe Qualitätssicherung dar, da eine zusätzliche Beurteilung der getroffenen Maßnahmen durch einen unternehmensunabhängigen Dritten erfolgt. Bei dieser Beurteilung ergeben sich häufig Erkenntnisse, die zu einer Verbesserung in der Umsetzung der Maßnahmen in den Unternehmen beitragen.

Darüber hinaus zeigen unsere Erfahrungen, dass Unternehmen häufig nicht über ausreichende Kapazitäten, notwendige Strukturen bzw. ausreichende fachliche Expertise verfügen, um durch regelmäßige interne Audits Schwachstellen zu identifizieren und zu beseitigen. Dies zeigen insbesondere die Erfahrungen unserer Mitglieder bei der Durchführung von Erstprüfungen Kritischer Infrastrukturen.

Wir regen daher an, die in § 39 Abs. 1 BSIG vorgesehene Nachweispflicht der Erfüllung der Anforderungen nach § 30 Abs. 1 BSIG auf besonders wichtige Einrichtungen auszuweiten.

Zu § 39 Abs. 1 BSIG – Nachweiszeitraum

§ 39 Abs. 1 Satz 1 BSIG verpflichtet Betreiber kritischer Anlagen ferner dazu, den Nachweis gegenüber dem Bundesamt „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“ zu erbringen.

Die IT-Sicherheitslage in Deutschland hat sich, auch in Folge des russischen Angriffskriegs auf die Ukraine, insgesamt zugespitzt. Bedrohungen aus dem Bereich Cybercrime treten nicht mehr nur vereinzelt auf, sondern sind zunehmend Teil des unternehmerischen Alltags geworden. Vor diesem Hintergrund halten wir die Abkehr von dem nach aktuell gültiger Rechtslage bestehenden zweijährigen Zeitraum für die Nachweiserbringung für nicht zielführend, um die Cybersicherheit in Deutschland zu stärken. Eine Verlängerung des Zeitraums auf mindestens drei Jahre birgt die Gefahr, dass bestehende Cyberrisiken in den Unternehmen aufgrund unzureichender Maßnahmen durch externe Prüfungen zu spät erkannt bzw. behoben werden. Eine Verlängerung des Nachweiszeitraums

von zwei auf mindestens drei Jahre steht aus unserer Sicht der Schnelllebigkeit bei der Entwicklung von Cyberrisiken entgegen.

Wir regen daher an, den Nachweiszeitraum entsprechend der aktuellen Rechtslage für Betreiber kritischer Anlagen bei zwei Jahren zu belassen.

Da eine auftretende Gefährdungslage bei den besonders wichtigen Einrichtungen ggf. mit anderen Auswirkungen auf die deutsche Wirtschaft verbunden sein kann als bei Betreibern kritischer Anlagen, kann bei den besonders wichtigen Einrichtungen auch ein abweichender Nachweiszeitraum als adäquat angesehen werden.

Zu § 39 Abs. 3 BSIG – Übergangszeitraum

§ 39 Abs. 3 BSIG legt den Zeitpunkt der Nachweiserbringung für Betreiber kritischer Anlagen, die zum Zeitpunkt des Inkrafttretens des NIS2UmsuCG Betreiber Kritischer Infrastrukturen nach aktueller Rechtslage waren, auf frühestens drei Jahre nach Erbringung des letzten Nachweises fest.

Wir regen an, auch bei der Festlegung des Übergangszeitraums zu berücksichtigen, dass für Betreiber Kritischer Infrastrukturen, die aktuell der Nachweispflicht unterliegen, eine Einhaltung des von uns vorgeschlagenen zweijährigen Zeitraums der Nachweiserbringung durchgehend sichergestellt ist.

Wir hoffen Ihnen mit diesen Hinweisen behilflich sein zu können und stehen für Rückfragen gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Moser

Pöhlmann, WP StB
Technical Director Digitalization & Advisory