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, 19.10.2023

624/550

IDW Stellungnahme zum Diskussionspapier des Bundesministeriums des Innern und für Heimat „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“

Sehr geehrte Damen und Herren,

mit diesem Schreiben nehmen wir zum Diskussionspapier des Bundesministeriums des Innern und für Heimat „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ 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 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2)* 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 Diskussionspapier des Bundesministeriums des Innern und für Heimat „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ im Einzelnen wie folgt Stellung:

Zu § 28 Abs. 1 BSIG – Ausnahmeregelung

§ 28 Abs. 1 Satz 2 BSIG sieht die Ausnahme bestimmter Finanzunternehmen von den besonders wichtigen Einrichtungen und den wichtigen Einrichtungen vor. Die hier zitierten § 1a Abs. 2 Kreditwesengesetz und § 293 Abs. 5 Versicherungsaufsichtsgesetz existieren jedoch nicht. Somit bleibt unklar, welche Unternehmen unter die Ausnahmeregelung des § 28 Abs. 1 Satz 2 BSIG-E fallen.

Anlage 1 führt als Sektor mit hoher Kritikalität das Finanz- und Versicherungswesen auf. Dort sind als Teilsektoren das Bankwesen und Finanzmarktinfrastrukturen, nicht jedoch das Versicherungswesen genannt. Auch hier bleibt somit unklar, welche Einrichtungen unter die Definition des § 28 Abs. 1 BSIG fallen bzw. davon ausgenommen sind.

Wir regen an, die Definition der betroffenen Unternehmen klarzustellen.

Zu § 39 Abs. 1 BSIG-E – 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 vorgesehenen Nachweispflichten 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 „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 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 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. 1 BSIG – Übergangszeitraum

§ 39 Abs. 1 Satz 1 BSIG verpflichtet Betreiber kritischer Anlagen, „…die Erfüllung der Anforderungen nach § 30 Absatz 1 und § 31 zu einem … festgelegten Zeitpunkt frühestens drei Jahre nach Inkrafttreten dieses Gesetzes … nachzuweisen“.

Wir sehen die Gefahr, dass es in bestimmten Konstellationen bei Betreibern Kritischer Infrastrukturen, die nach aktuell gültiger Rechtslage einer zweijährigen Prüfung unterliegen, durch diese Regelung zu einem Zeitraum von mehr als drei Jahren kommen kann, in dem keine Nachweiserbringung erfolgt.

Wir schlagen daher vor, den Übergangszeitraum nicht in § 39 BSIG, sondern ergänzend zu regeln und hierbei zu berücksichtigen, dass auch 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