

Berlin, 03.07.2024

Stellungnahme und Kommentierung

zum

Referentenentwurf des Bundesministeriums des Innern und für Heimat 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)

Kontakt:

RA Karsten U. Bartels, LL.M.

HK2 RAe

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Stellvertretender Vorstandsvorsitzender

Leiter TeleTrust-AG "IT-Sicherheitsrecht"

bartels@hk2.eu

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrust den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrust bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrust ist Träger der "TeleTrust European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrust Information Security Professional" (T.I.S.P.) und "TeleTrust Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Chausseestraße 17

10115 Berlin

Tel.: +49 30 4005 4310

<https://www.teletrust.de>

I. Allgemeine Vorbemerkung

Der Bundesverband IT-Sicherheit verweist auf seine bisherigen Stellungnahmen zum Referentenentwurf vom 07.05.2024 und dem Diskussionspapier vom 27.09.2023 und ergänzt diese wie folgt:

II. Anmerkungen zu ausgewählten Regelungen des BSIG-E

1. Auslegung des Sektors "Verarbeitendes Gewerbe/Herstellung von Waren", § 28 Abs. 2 BSIG-E

In § 28 Abs. 2 Nr. 3 BSIG-E wird hinsichtlich der anzubietenden Waren und Dienstleistungen auf die Anlagen 1 und 2 verwiesen. Der Sektor erfasst die in den Abteilungen 26 bis 30 NACE genannten wertschöpfenden Tätigkeiten, die im Wesentlichen auf die Herstellung von bestimmten Produkten gerichtet sind. Ob hiervon auch folgende Konstellation erfasst sein soll, geht aus dem Entwurf nicht klar hervor:

Ein Unternehmen stellt ein in den Abteilungen 26 bis 30 NACE aufgeführtes Produkt her, vertreibt dieses jedoch nicht als eigenständiges Produkt, sondern setzt dieses als Werk- bzw. Hilfsmittel oder (Teil-)Komponente ein, um damit das eigentliche Endprodukt herzustellen, das wiederum nicht den Abteilungen 26 bis 30 NACE unterfällt.

Wir gehen davon aus, dass Fälle dieser Art nicht als "entgeltliches Anbieten von Waren oder Dienstleistungen" im Sinne von § 28 Abs. 2 Nr. 3 BSIG-E erfasst sind, weil es für ein Anbieten ausschließlich darauf ankommt, dass das Endprodukt in die Abteilung 26 bis 30 NACE fällt. Anders zu beurteilen wäre dies nur dann, wenn das einer der Abteilungen 26 bis 30 NACE unterfallende Produkt im Rahmen von "Serviceleistungen" etwa eigenständig als Ersatzteil vertrieben werden würde.

Wir empfehlen insoweit eine Klarstellung, zumindest in der Gesetzesbegründung.

2. Berechnung von Beschäftigtenzahlen, Jahresumsatz, Jahresbilanzsumme, § 28 Abs. 3 BSIG-E

Gemäß der Gesetzesbegründung zu § 28 Abs. 3 BSIG-E sind bei der Berechnung von Beschäftigtenzahlen, Jahresumsatz und Jahresbilanzsumme "nur diejenigen Teile der Einrichtung einzubeziehen, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind".

Problematisch ist dies insbesondere in den unter Ziff. 1. genannten Fällen. Denn sollten die unter Ziff. 1 genannten Fälle doch unter den Sektor "Verarbeitendes Gewerbe/Herstellung von Waren" fallen, stellt sich das Folgeproblem, dass für die Berechnung des Jahresumsatzes und der Jahresbilanzsumme nach der Gesetzesbegründung zu § 28 Abs. 3 BSIG-E "nur diejenigen Teile der Einrichtung einzubeziehen [sind], die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind". Wird jedoch das den Abteilungen 26 bis 30 NACE unterfallende Produkt nicht selbst, sondern nur als Teil bzw. Komponente eines anderen Produkts vertrieben, enthält der Gesetzesentwurf keine Angaben dazu, wie in derartigen Fällen der Jahresumsatz bzw. die Jahresbilanzsumme ermittelt werden sollen.

Derartige Berechnungsprobleme können sich auch in anderen Konstellationen stellen.

Insgesamt empfehlen wir die Ausführungen in der Begründung zu § 28 Abs. 3 BSIG-E (S. 149) hinsichtlich der Berechnung von Beschäftigtenzahlen, Jahresumsatz und Jahresbilanzsumme klarzustellen und in den Gesetzestext selbst zu übernehmen. Die Ausführung, dass und wie die Kennzahlen anteilig für die in den relevanten Einrichtungskategorien tätigen Personen zu betrachten sind, ist eine nicht zu unterschätzende Klarstellung für die Wirtschaft und verhindert unverhältnismäßige Eingriffe in die Berufs-

freiheit. In diesem Zuge ist auch noch klarzustellen, dass auch bei einer Zurechnung gemäß der Kommissionsempfehlung 2003/361/EG nur solche Kennzahlen im Konzernverbund zuzurechnen sind, die ebenso für die Einrichtungskategorien relevant sind.

3. Keine Nennung des Teilbereichs ÖPNV im Sektor Transport und Verkehr, Anlage 1

Die aktuelle KRITIS-VO erfasst bestimmte Einrichtungen im Teilbereich ÖPNV im Sektor Transport und Verkehr als Betreiber kritischer Infrastrukturen. Erfasst sind Betreiber von Schienennetzen und Stellwerken sowie Leitzentralen im ÖPSV (siehe Anhang 7 der KRITIS-VO). Demgegenüber erfasst der Sektor Transport und Verkehr in Anlage 1 des BSIG-E aktuell keine Einrichtungen im Teilbereich ÖPNV.

Geht man davon aus, dass solche Einrichtungen in dem Teilbereich ÖPNV auch in Zukunft als Betreiber kritischer Anlagen gemäß der neuen Rechtsverordnung gemäß § 58 Abs. 4 BSIG-E eingestuft werden, führt dies dazu, dass Einrichtungen im Teilbereich ÖPNV so lange nicht vom BSIG-E erfasst werden, wie sie unterhalb der maßgebenden KRITIS-Schwellenwerte liegen. Erst wenn sie die KRITIS-Schwellenwerte erreichen und damit als Betreiber kritischer Anlagen eingestuft werden, werden sie dadurch automatisch auch als besonders wichtige Einrichtung eingestuft (vgl. § 28 Abs. 1 Nr. 1 BSIG-E).

Der Kritikalität des Teilbereichs ÖPNV wegen empfehlen wir, diesen ebenfalls in die Anlage 1 aufzunehmen, so dass bei Erreichen der Unternehmenskennzahlen in § 28 Abs. 1 Nr. 4 bzw. Abs. 2 Nr. 3 BSIG-E) die entsprechenden Einrichtungen als wichtige bzw. besonders wichtige Einrichtung unabhängig von der Einstufung als Betreiber kritischer Anlagen erfasst werden.

4. Klarstellung des Verhältnisses zwischen BSIG und SGB V, §§ 30 ff. BSIG-E

Im BSIG-E ist derzeit keine Regelung zum Rangverhältnis zwischen den Vorgaben in den §§ 30 ff. BSIG-E und den §§ 391 ff. SGB V (insbesondere in der Fassung des DigiG) enthalten. Es ist daher unklar, ob die Bestimmungen in §§ 391 ff. SGB V abschließend oder neben den §§ 30 ff. BSIG-E gelten sollen. Aktuell wird man im Zweifel wohl davon ausgehen müssen, dass die betroffenen Krankenhäuser und gesetzlichen Krankenkassen sowohl die Vorgaben in §§ 391 ff. SGB V als auch in §§ 30 ff. BSIG-E kumulativ einhalten müssen. In dem Fall ist aber zu beachten, dass die Regelungen in den §§ 30 ff. BSIG-E inhaltlich mit den Bestimmungen in den §§ 391 ff. SGB V vielfach übereinstimmen (z. B. ist die Pflicht zur Umsetzung von TOM und die Durchführung von Schulungen in § 391 Abs. 1, 2 SGB V auch in § 30 Abs. 1 und 2 BSIG-E vorgesehen). Es sollte daher entweder im BSIG-E oder im SGB V eine klarstellende Regelung zum Rangverhältnis aufgenommen werden, beispielsweise, dass die Bestimmungen in den §§ 30 ff. BSIG-E von den Bestimmungen in §§ 391, 392 SGB V unberührt bleiben.

5. Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen, § 31 BSIG-E

Die Anforderungen an IT-Sicherheitsmaßnahmen an Betreiber kritischer Anlagen stellen aufgrund der Relevanz einen wichtigen Regelungskern des BSIG-E dar. Dennoch bestimmt der § 31 Abs. 1 BSIG-E auch in der geänderten Fassung keinerlei eigene materiellen Anforderungen. Die Anknüpfung allein an den gesteigerten Aufwand im Verhältnis zur Maßnahmenauswahl gem. § 30 BSIG-E ist nicht bestimmt genug. Dies trifft um so mehr zu, je ernster die Gesetzesadressaten § 30 Abs. 2 S. 1 BSIG-E hinsichtlich der Anforderungen an den Stand der Technik nehmen. Denn wenn die Maßnahmen nach § 30 Abs. 2 S. 1 BSIG-E dem Stand der Technik entsprechen, können diese nicht verbessert werden. Der Stand der Technik selbst bezeichnet bereits die am Markt verfügbaren Bestleistungen von Maßnahmen zur Umsetzung der gesetzlich festgelegten Schutzziele.

TeleTrust empfiehlt dringend eine materielle Klarstellung der Norm.

6. "Umsetzungspflicht" für Geschäftsleitungen, § 38 Abs. 1 BSIG-E

§ 38 Abs. 1 BSIG-E sieht nun explizit vor, dass die Geschäftsleitung Risikomanagementmaßnahmen "umsetzen" muss. Nach dem Wortlaut würde eine solche Umsetzungspflicht im Zweifel bedeuten, dass die Geschäftsleitung die Risikomanagementmaßnahmen unmittelbar selbst implementieren muss. Die Aufgabe und Funktion der Geschäftsleitung umfassen naturgemäß die strategische Planung, Leitung und Kontrolle der Unternehmensaktivitäten. In der Praxis wird die Umsetzung der Risikomanagementmaßnahmen daher maßgeblich von den fachlich-technisch Verantwortlichen (z. B. ISB) vorangetrieben.

Die NIS-2-Richtlinie selbst enthält auch keine solche Umsetzungspflicht, sondern ausschließlich eine Pflicht zur "Billigung" und "Überwachung" der Umsetzung. Eine eigene Umsetzungspflicht der Geschäftsleitung besteht im Übrigen auch nicht in den gemäß § 30 Abs. 2 BSIG-E zu berücksichtigenden "europäischen und internationalen Normen", wie etwa der ISO 27001, so dass eine Berücksichtigung ebendieser Normen auf organisatorischer Ebene gerade nicht vollständig erfolgen könnte.

Praktisch ist davon auszugehen, dass die Qualität der Risikomanagementmaßnahmen im Unternehmen sinkt, und nicht steigt, wenn die Geschäftsleitung in der jetzigen Entwurfsfassung der Norm verpflichtet wird.

Es sollte daher in § 38 Abs. 1 BSIG-E gemäß den Vorgaben der NIS2-Richtlinie geregelt werden, dass die Geschäftsleitungen verpflichtet sind, die Umsetzung der nach § 30 zu ergreifenden Risikomanagementmaßnahmen zu billigen und zu überwachen.

7. Überarbeitung der Haftungsregelung, § 38 Abs. 2 BSIG-E

Gemäß § 38 Abs. 2 S. 2 BSIG-E haften Geschäftsleitungen nach "diesem Gesetz" (d. h. dem BSIG-E), wenn die maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelungen nach § 38 Abs. 2 S. 1 BSIG-E enthalten. Das BSIG-E enthält allerdings keine expliziten Haftungsregelungen für Geschäftsleitungen. Die Regelung in § 38 Abs. 2 S. 2 BSIG-E läuft somit ins Leere. Bleiben die aktuellen Regelungen in § 38 Abs. 2 BSIG-E weiter bestehen, sollte aus Gründen der Rechtssicherheit noch eine entsprechende Haftungsregelung aufgenommen werden.