Zentralverband
des Deutschen Handwerks

ZDH

Stellungnahme

zum Referentenentwurf des Bundesministeriums des Innern (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)

Berlin, 04.07.2025

Zentralverband des Deutschen Handwerks
Bereich Wirtschaftspolitik
+49 30 20619-265
geier@zdh.de

Bereich Wirtschaftspolitik
+49 30 20619-260
terton@zdh.de

Lobbyregister: R002265
EU Transparency Register: 5189667783-94

DAS HANDWERK

Der Zentralverband des Deutschen Handwerks e.V. (ZDH) ist die Dachorganisation für Handwerkskammern und Zentralfachverbände des Handwerks sowie wirtschaftliche und wissenschaftliche Einrichtungen des Handwerks in Deutschland. Wir vertreten die Interessen von rund 1 Million Handwerksbetrieben mit rund 5,6 Millionen Beschäftigten und 340.000 Auszubildenden.

Wir bedanken uns für die Gelegenheit, zum Referentenentwurf des Bundesministeriums des Innern (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) vom 24. Juni 2025 Stellung nehmen zu können, wovon wir nachfolgend Gebrauch machen.

Aufgrund der kurzen Frist zur Stellungnahme weisen wir bereits jetzt darauf hin, dass wir uns vorbehalten, weitere Anmerkungen im Laufe des Verfahrens einzubringen.

1. Allgemeine Anmerkungen

Die Bedeutung von Cybersicherheit ist unbestritten. Insofern werden die geplanten Regelungen im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) grundsätzlich nicht in Frage gestellt.

Dabei muss es aber immer auch eine Abwägung zwischen potentiellem Risiko und potentiellem Schaden auf der einen Seite sowie den Kosten und dem weiter steigenden Bürokratieaufwand für die Betriebe auf der anderen Seite geben. Die **Praxistauglichkeit und insbesondere die mittelstandsgerechte Umsetzbarkeit** der vorgesehenen Maßnahmen müssen daher **bei der Umsetzung des Gesetzes an erster Stelle** stehen.

Gerade wegen der sich aus dem NIS2UmsuCG ergebenden Anforderungen an die Betriebe und Unternehmen, insbesondere bzgl. der geforderten Cybersicherheitsrisikomanagementmaßnahmen und drohender Konsequenzen bei Nichteinhaltung der Pflichten, muss **Klarheit darüber herrschen, ob ein Unternehmen tatsächlich in den Anwendungsbereich des Gesetzes** fällt.

Daher ist für uns die Frage nach der **Betroffenheit der Handwerksbetriebe seitens des Gesetzes** von zentraler Bedeutung: Eine **scharfe Abgrenzung der Betroffenheit** ist dringend notwendig. Die Betriebe benötigen Rechtssicherheit dahingehend, ob sie betroffen sind oder nicht.

Instrumente, wie etwa das speziell an KMU gerichtete Online-Tool FitNIS2-Navigator (unter der URL https://fitnis2.de/ abrufbar), sind zwar gut gedacht, aus ihrer Unverbindlichkeit ergeben sich aber eher Unschärfen, die mehr zu Verwirrung und Unsicherheit beitragen als diese lösen. Sie können daher rechtssichere Auslegungen nicht ersetzen.

Das BMI und das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind daher aufgefordert, mittelstandsfreundliche Auslegungshilfen und FAQ-Listen bereitzustellen sowie nachvollziehbare und ermessensleitende Auskünfte zu geben.

Dabei muss das BMI dem BSI den klaren politischen Auftrag erteilen, damit hier auch verbindliche Auskünfte erteilt werden können – und tatsächlich dann auch werden.

2. Zu den Regelungen des Referentenentwurfs im Einzelnen

Artikel 1 Teil 3 Kapitel 1 Anwendungsbereich

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

Die besonders wichtigen Einrichtungen und die wichtigen Einrichtungen inkl. der Größenangaben werden zwar direkt im Gesetzestext spezifiziert, und die Auflistung betroffener Einrichtungsarten erfolgt in den Anlagen 1 und 2. Dennoch halten wir dieses nicht für ausreichend: Die Betriebe benötigen erst einmal Klarheit über ihre Betroffenheit, wozu folgende, zweifelsfreie Klärung der Betroffenheit gehört: Welche Gewerke, welche Betriebsgrößen sind betroffen, welcher Umfang an Maßnahmen ist zu ergreifen? Die genannten Anlagen sind dafür aus unserer Sicht nicht ausreichend.

Hierzu und **für die konkrete Umsetzung sind rechtssichere und praxistaugliche Umsetzungshilfen zur Verfügung zu stellen**. Mit der starken Ausweitung des Umsetzungsbereichs muss eine verstärkte Kommunikations- und Vermittlungsarbeit einhergehen, insbesondere gegenüber den mittelständisch geprägten Betrieben.

Zudem ist unbedingt **zu vermeiden** – und dieses auch sicherzustellen – dass Cybersicherheitspflichten von besonders wichtigen und wichtigen Einrichtungen **vollumfänglich auf die Betriebe in der Lieferkette weitergereicht werden** können und damit eine Betroffenheit dieser Regelungen im Sinne eines „trickle down“ entsteht.

Hier erwarten wir vom BMI eine verbindliche Aussage und Klarstellung – gerne in einer „offiziellen“ Auslegungshilfe. Ein (positives) Beispiel aus Baden-Württemberg möge illustrieren, wie dieses geschehen könnte:

- In Baden-Württemberg wurde am 16. April 2025 die Cybersicherheitsverordnung (CSVO) BW verabschiedet, die die Cybersicherheitsstandards für Landesbehörden etc. nach NIS-2 regelt. Während Handwerksbetriebe grundständig nicht in ihren Anwendungsbereich fallen, besagt § 9 (4) ebd. *„Vertragliche Dienstleister, die als Auftragnehmer für öffentliche Stellen Leistungen erbringen, sind bei der Auftragserteilung auf die Einhaltung dieser Verordnung im notwendigen Umfang zu verpflichten. Dies ist über einzelvertragliche Regelungen oder Rahmenverträge sicherzustellen und vom Auftraggeber angemessen zu kontrollieren.“*
- Hierzu gab es auf Nachfrage vom dortigen Innenministerium folgende Erklärung: *„Es ist nicht beabsichtigt, dass bietende Unternehmen grundsätzlich auf die Einhaltung der CSVO verpflichtet werden. Dies soll in „notwendigem Umfang“ nur dann geschehen, wenn sie Dienstleistungen erbringen, die ein Sicherheitsrisiko darstellen könnten (z. B. IT-Verfahren, Wartung IT-Geräte, …). Handwerkstätigkeiten wie bspw. Malerarbeiten, Gärtnerarbeiten wären demnach nicht betroffen.“*
- Auf diese Weise konnte die Sorge der Betriebe bzgl. einer „Betroffenheit durch die Hintertür“ belegbar entkräftet werden. Dieses ist auch ein gutes Beispiel für eine gelungene und partnerschaftliche Zusammenarbeit zwischen Staat und Wirtschaft, für die wir hier sehr dankbar sind.

Dass gemäß §28 Abs. 3 bei der Zuordnung zu einer der Einrichtungsarten nach Anlage 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind, begrüßen wir.

Welche **materiellen und konkreten Fragen hinsichtlich der Betroffenheit** die Betriebe haben und die dringend einer Lösung bedürfen, wird **mit Blick auf Nr. 4 Gesundheit in Anlage 1** deutlich und soll **anhand der Gesundheitshandwerke und der Textilreiniger verdeutlicht** werden:

Gesundheitshandwerke

Fragen der Betriebe:

- Wie werden Gesundheitsdienstleister auf europäischer Ebene definiert?
- Wie werden Gesundheitsdienstleister auf nationaler Ebene definiert?
- Gibt es definitorische Unterschiede?
- Wird es eine Positivliste der Betroffenen geben?
- Bezieht sich die Anzahl der Beschäftigen sowie des Umsatzvolumens auf einen einzelnen (Filial-)Betrieb oder unter Umständen auf das gesamte Unternehmen?

Hintergrund:

- Die Gesundheitshandwerke bieten Gesundheitsdienstleistungen an. Sie zählen zu den Gesundheitsberufen, sind aber keine Gesundheitsfachberufe. Sie sind gesetzliche Mitglieder in den Handwerkskammern. Somit unterliegen sie der handwerklichen Selbstverwaltung.
- Im Umkreis von 50 km gibt es bundesweit zahlreiche Fachgeschäfte. Eine auch nur ansatzweise monopolistische Struktur ist ausgeschlossen. Das Gesundheitshandwerk ist klein- und mittelständig geprägt.
- Auch während der Corona-Pandemie durften die Fachgeschäfte geöffnet bleiben, zählten aber ausdrücklich nicht zur kritischen Infrastruktur.
- Sollte ein Unternehmen mit mehr als 50 Beschäftigten einer Cyberattacke unterliegen, kann sich der Kunde jederzeit an ein anderes Fachgeschäft seiner Wahl wenden.

Beispiel der Hörakustiker:

- Alle Hörsystem sind zwar individuell auf den Hörschaden des Kunden angepasst, die Anpassdaten können aber jederzeit ausgelesen werden. Selbst wenn das nicht möglich sein sollte, kann der Hörschaden mit einem qualifizierten Hörtest ermittelt und die Hörsysteme neu angepasst werden. Wenn die Anamnese und der qualifizierte Hörtest einmal im Fachgeschäft erfolgt sind, kann notfalls die weitere Feinanpassung auch per Fernanpassung über das Internet erfolgen. Notwenige Reparaturleistungen können auch postalisch erfolgen, in dem der Kunde seine Hörsystem an das Fachgeschäft schickt oder dort abgibt.

- Diese Punkte lassen sich in ähnlicher Form auch auf die anderen Gewerke der Gesundheitshandwerke übertragen.

Schlussfolgerung und Petitum:

- Sollte ein Unternehmen mit mehr als 50 Mitarbeitern eine Cyberattacke unterliegen, werden die anderen Fachgeschäfte die Versorgung sofort übernehmen können.
- Ein Wechsel des Leistungserbringers (hier: Hörakustiker) erfolgt regelhaft, da die Versorgungsleistung individuell ist und der Kunde dem Leistungserbringer sein Vertrauen „schenken" muss.
- Nach wie vor sind die beabsichtigten Regelungen und möglichen Auswirkungen auf zumindest Teile von Betrieben der Orthopädietechnik/Sanitätshäusern/Home-Care-Betrieben nicht eindeutig.
- Nach bisheriger Lesart gibt es eine Einteilung nach Betreibern kritischer Anlagen (KRITIS), besonders wichtiger und wichtiger Einrichtungen. Zu den kritischen Anlagen zählen von der Sache her gem. Anlage 5 (Anlagenkategorien und Schwellenwerte im Sektor Gesundheit) BSI-KritisV auch orthopädietechnische Betriebe. Allerdings erreichen oder überschreiten sie nicht den angegebenen Schwellenwert von 90,68 Mio. EUR Jahresumsatz. Für diese Betriebe ist daher festzuhalten, dass sie keine KRITIS-Betreiber sind. **Hier wird jedoch eine rechtssichere und verbindliche Bestätigung benötigt**.
- Mit Blick auf die besonders wichtigen und wichtigen Einrichtungen ist eine Beurteilung hingegen sehr unscharf. NIS2 verweist auf den Artikel 22 der Richtlinie (EU) 2022/123). Dieser enthält jedoch keine klare Begriffsbestimmung, sondern beschreibt das Zustandekommen einer Liste von betroffenen Medizinprodukten nach der jeweiligen Notlage, festzustellen durch eine Lenkungsgruppe. **Damit bleibt unklar, ob orthopädietechnische Betriebe als Hersteller von Medizinprodukten betroffen sein könnten.**
- Ganz allgemein wird von Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU gesprochen. Darunter würden die gesundheitshandwerke fallen, sowohl als besonders wichtige als auch wichtige Einrichtung (Größenklassen Mitarbeiter/Umsatz).
- **Diese Unklarheiten müssen zwingend ausgeräumt werden!**

Textilreiniger

Textile Dienstleister sind u.a. mit OP-Kleidung und OP-Tüchern im Bereich der Medizinprodukte tätig. Sie sind zudem mit Berufskleidung und Flachwäsche (Bettwäsche, Handtücher) Dienstleister auch anderer in den Anlage 1 und 2 genannten Einrichtungen (bspw. für Gesundheitsdienstleister, die Pharmaindustrie, Energieversorger).

I. Unmittelbare Betroffenheit

Die unmittelbare Betroffenheit als besonders wichtige Einrichtung bzw. wichtige Einrichtung (s. § 28 BSIG-E) richtet sich nach der Auflistung der Einrichtung in einer der in Anlage 1 bzw. Anlage 2 genannten Sektoren und dem Erreichen eines bestimmten Schwellenwertes.

1. Medizinprodukt

a. **Eine Betroffenheit könnte sich ergeben aus Anlage 1 Nr. 4.1.5:**

- *Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden.*
- *Art. 22 VO (EU) 2022/123: (1) Unmittelbar nach Feststellung einer Notlage im Bereich der öffentlichen Gesundheit konsultiert die Lenkungsgruppe für Engpässe bei Medizinprodukten die in Artikel 21 Abs. 5 genannten Arbeitsgruppe. Unmittelbar nach der Konsultation nimmt die Lenkungsgruppe für Engpässe bei Medizinprodukten eine Liste der Kategorien kritischer Medizinprodukte an, die sie während einer Notlage im Bereich der öffentlichen Gesundheit für kritisch hält (im Folgenden „Liste kritischer Produkte für Notlagen im Bereich der öffentlichen Gesundheit“).*

Fragen der Betriebe:

- Gibt es eine entsprechende Liste kritischer Medizinprodukte?
- Welche Internetseite ist in Art. 22 Abs. 3 VO (EU) 2022/123 gemeint?

➢ Ohne eine entsprechende Liste lässt sich nicht rechtssicher feststellen, ob eine Betroffenheit vorliegt. Sollte die Liste kritischer Produkte erst nach Feststellung einer Notlage aufgestellt werden, ist unklar, wie erst im Anschluss die Anforderungen aus dem BSIG-E erfüllt werden sollen.

b. Eine Betroffenheit könnte sich ergeben aus Anlage 2 Nr. 5.1.1:

- *Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates herstellen, mit Ausnahme von Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden.*
- *Art. 2 Nr. 1 VO (EU) 2017/745: „Medizinprodukt“ bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software, ein Implantat, ein Reagenz, ein Material oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen*

bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll:

- *Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten,*
- *Diagnose, Überwachung, Behandlung, Linderung von oder Kompensierung von Verletzungen oder Behinderungen,*
- *Untersuchung, Ersatz oder Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs oder Zustands,*
- *Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper — auch aus Organ-, Blut- und Gewebespenden — stammenden Proben und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann.*

Fragen der Betriebe:

- Fallen OP-Textilien unter Medizinprodukte nach Art. 2 Nr. 1 VO (EU) 2017/745?
- Wer prüft / bestimmt / berät bei der Zuordnung zu den in Anlage 1 und 2 genannten Sektoren?

➢ Die ständige Verweisung auf weitere Verordnungen und Richtlinien macht es schwierig, den Anwendungsbereich abschließend zu beurteilen. **Hier sind klare Auslegungshilfen notwendig**!

2. Hersteller i.S. BSIG-E

- Unter die in Anlage 1 und 2 genannten Sektoren fallen Unternehmen, die die entsprechenden Produkte „herstellen".
- OP-Textilien werden von textilen Dienstleistern nicht selbst produziert, sondern von Textilherstellern eingekauft. Allerdings erfüllen diese Textilien zu diesem Zeitpunkt noch nicht die Anforderungen, um bestimmungsgemäß eingesetzt zu werden. Dafür bedarf es erst der zusätzlichen Aufbereitung (u.a. Desinfizieren, Ausrüsten, Sterilisieren, Verpacken) durch den Textildienstleister.

Frage der Betriebe:

- Reicht diese Aufbereitung der Textilien aus, um den Textildienstleister als Hersteller eines Medizinproduktes zu qualifizieren?

3. Schwellenwerte (§ 28 Abs. 1 Nr. 4, Abs. 2 Nr. 3 BSIG-E)

- Neben einer Zuordnung zu den in den Anlagen 1 und 2 genannten Einrichtungen bedarf es für eine unmittelbare Betroffenheit einer gewissen Unternehmensgröße, die sich aus Jahresumsatz, Jahresbilanz und Mitarbeiterzahl bestimmt.
- Gem. § 28 Abs. 3 Nr. 1 BSIG-E ist 1. dabei auf „*die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen*".

Fragen der Betriebe:

- Es kommt damit nur auf die Umsätze / Mitarbeiter an, die in dem entsprechenden Bereich erzielt werden bzw. beschäftigt sind? Konkret gefragt: Andere Geschäftsbereiche eines Textildienstleisters (bspw. Flachwäsche, Berufsbekleidung) bleiben unberücksichtigt?
- Da Bezugspunkt in § 28 u.a. die juristische Person ist, ist damit auf das Unternehmen abzustellen? Arbeiten Unternehmen bspw. in Konzernstrukturen zusammen, bleibt dies dementsprechend unberücksichtigt?

II. Mittelbare Betroffenheit

- Textile Dienstleister sind mit ihren Produkten (OP-Textilien, Flachwäsche, Berufsbekleidung) Zulieferer für besonders wichtige und wichtige Einrichtungen gem. § 28 BSIG-E. Dabei sind sie regelmäßig insoweit mit der EDV des Anbieters verknüpft, dass Informationen über die Produkte, auf die sich die Dienstleistung bezieht, erfasst und ausgetauscht werden.
- Besonders wichtige Einrichtungen und wichtige Einrichtungen sind zumindest gem. § 30 Abs. 2 Nr. 4 BSIG-E verpflichtet, auch die Lieferkette mit in den Blick zu nehmen:
    - *„Die Maßnahmen müssen zumindest Folgendes umfassen: … 4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern, …“*

Fragen der Betriebe:

- Inwieweit können textile Dienstleister von ihren Auftraggebern, die die Pflichten nach § 30 BSIG-E erfüllen müssen, ebenfalls in die Pflicht genommen werden, gleiche oder vergleichbare Anforderungen zu erfüllen?
- Inwieweit können besonders wichtige und wichtige Einrichtungen ihre Dienstleister bspw. im Rahmen entsprechender Anforderungen in der Ausschreibung

Artikel 1 Teil 3 Kapitel 2 Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen – hier: Verhältnismäßigkeit der zu ergreifenden Maßnahmen

Der Ansatz, die **Verhältnismäßigkeit der Maßnahmen** im Verhältnis zum Risiko zu bestimmen, ist grundsätzlich in unserem Sinne. Allerdings dürfte es gerade betroffenen Betrieben, die lediglich knapp über 50 Mitarbeiter haben, oder Betrieben, die unter 50 Mitarbeitern beschäftigen, aber einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen, aufgrund der Ungenauigkeit der Kriterien schwerfallen einzuschätzen, wann sie die Vorgaben der Verhältnismäßigkeit der Maßnahmen erfüllen. Da gerade diese betroffenen Handwerksbetriebe keine Stabsbereiche aufweisen, die sich vertieft mit juristischen Fragestellungen beschäftigen können, ist für diese Betriebe aufgrund der Ungenauigkeit der Kriterien kaum abschätzbar, welche

Maßnahmen verhältnismäßig sind. Aufgrund dieser Unsicherheit und der Befürchtung, gegen die Vorgaben des § 30 zu verstoßen, ist damit zu rechnen, dass diese Handwerksbetriebe über die Verhältnismäßigkeit hinausgehende Maßnahmen ergreifen, welche die Betriebe finanziell schwerer belasten als eigentlich notwendig und durch die Regelungen intendiert.

Daher wäre eine **Auslegungshilfe zur Verhältnismäßigkeit der Maßnahmen im Verhältnis zum Risiko**, zumindest aber eine Klarstellung der unteren Grenzen der verhältnismäßigen Maßnahmen **in FAQ oder ähnlichen Hinweisen nicht nur wünschenswert, sondern unseres Erachtens auch geboten**.

Unmittelbar verpflichtete Unternehmen haben ferner gemäß § 30 Abs. 1 und 2 Maßnahmen zu treffen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Hierzu zählen auch vertragliche Vereinbarungen mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen, Patchmanagement sowie der Berücksichtigung von Empfehlungen des BSI in Bezug auf deren Produkten und Dienstleistungen. Ebenfalls kann dies beinhalten, Zulieferer und Dienstleister zur Beachtung von grundsätzlichen Prinzipien wie „Security by Design“ oder „Security by Default“ anzuhalten. Dies erscheint logisch, damit sich unmittelbar betroffene Unternehmen keine vermeintlichen Risiken über Dritte aussetzen.

Für die betroffenen Handwerksbetriebe bedeutet dies aber, dass diese ebenfalls gewisse Standards gewährleisten müssen, um nicht vom Markt ausgeschlossen zu werden. Etwaige Nachweise tragen auch hier zur Steigerung der Bürokratielast der Betriebe bei. Es ist fraglich, ob kleinere Betriebe hier mithalten können. Daher ist es **notwendig, hier unnötige Lasten zu vermeiden und eine Umsetzung im Sinne der Betriebe vorzunehmen**.

§ 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die Pflichten nach § 38 Abs. 1 könnten die Geschäftsleitungen von kleineren, betroffenen Handwerksbetrieben, die knapp über 50 Mitarbeiter haben, oder Betrieben, die unter 50 Mitarbeitern beschäftigen, aber einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen, einem unverhältnismäßigen Risiko aussetzen.

Gerade Handwerksbetriebe werden in der Regel von Handwerkern geführt, deren Kernkompetenz gewerkespezifisches und betriebswirtschaftliches Wissen umfasst. In der Regel gehört hierzu aber weniger fachlich-vertiefte Expertise im Bereich der IKT, wenn diese nicht für die Ausübung des speziellen Handwerks notwendig ist. Die Geschäftsleitungshaftung in § 38 Abs. 1, Abs. 2 setzt gemäß der Begründung die Billigung der Maßnahmen als geeignet sowie die kontinuierliche Überwachung der Umsetzung der Maßnahmen voraus. Ohne tiefere Kenntnis im Bereich der Cybersicherheit, welche weder in der handwerklichen Aus- oder Weiterbildung noch in der beruflichen Praxis notwendigerweise erlangt wird, ist eine Einschätzung, ob die Maßnahmen geeignet sind, kaum möglich. Solches Know-how wird in der Regel durch Einschaltung einer Hilfsperson

erlangt. Gemäß der Begründung zu § 38 Abs. 1 verbleibt die Letztverantwortlichkeit jedoch beim Leitungsorgan.

Fraglich ist daher, was diese Letztverantwortlichkeit umfasst. Wenn es sich bei der Letztverantwortlichkeit lediglich um ein Auswahlverschulden handelt, ist das Risiko der Haftung für die Geschäftsleitung kalkulierbar und verhältnismäßig. Sofern die Geschäftsleitung trotz des Einschaltens eines geeigneten Experten für die Geeignetheit der Maßnahmen, was aufgrund der Komplexität dieser Maßnahmen kaum möglich ist, haftet, würde diese einem unverhältnismäßigen Risiko ausgesetzt.

Daher bitten wir um **Klarstellung, wie der Begriff der Letztverantwortlichkeit auszulegen** ist.

./.

Ansprechpartner
Pius Geier
Bereich Wirtschaftspolitik
+49 30 20619-265
geier@zdh.de · www.zdh.de

Dr. Constantin Terton
Bereich Wirtschaftspolitik
+49 30 20619-260
terton@zdh.de · www.zdh.de

Herausgeber:
Zentralverband des Deutschen Handwerks e.V.
Haus des Deutschen Handwerks
Mohrenstraße 20/21 · 10117 Berlin
Postfach 110472 · 10834 Berlin

Lobbyregister: R002265
EU Transparency Register: 5189667783-94

Der Zentralverband des Deutschen Handwerks e. V. (ZDH) vertritt die Interessen von rund 1 Million Handwerksbetrieben in Deutschland mit rund 5,6 Millionen Beschäftigten. Als Spitzenorganisation der Wirtschaft mit Sitz in Berlin bündelt der ZDH die Arbeit von Handwerkskammern, Fachverbänden des Handwerks auf Bundesebene sowie bedeutenden wirtschaftlichen und sonstigen Einrichtungen des Handwerks in Deutschland. Mehr unter www.zdh.de