Nomos **PRAXIS**

Nink

Das neue IT-Sicherheitsrecht

Das BSI-Gesetz nach Umsetzung der NIS-2-Richtlinie

Nomos

Nomos**PRAXIS**

Dr. Judith Nink, Köln

Das neue IT-Sicherheitsrecht

Das BSI-Gesetz nach Umsetzung der NIS-2-Richtlinie

Nomos

Zitiervorschlag: Nink Das neue IT-SicherheitsR § … Rn. …

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7560-0995-4 (Print)
ISBN 978-3-7489-4651-9 (ePDF)

1. Auflage 2026

Vorwort

Die vom Verlag im Sommer 2024 gestellte Herausforderung schien machbar: Ein Handbuch für die Praxis zum deutschen NIS-2-Umsetzungsgesetz konzipieren und bis zur Veröffentlichung des Gesetzes fertigstellen. Ein neuer Regierungsentwurf war gerade veröffentlicht worden. Trotz zahlreicher Kritik der Experten am Entwurf erschien er aber als ausreichende Grundlage für die Basisarbeit. Gemeinsam mit einem Co-Autoren begann die Arbeit.

Tatsächlich stellte mich das Projekt aber vor zahlreiche nicht vorhersehbare Herausforderungen:

Während die Manuskripte Form annahmen, zerbrach im November 2024 die Ampel. Aufgrund der verpassten Umsetzungsfrist im Oktober 2024 erschien aber eine Verabschiedung dennoch machbar. Es bestand Einigkeit, dass eine Erhöhung des Cybersicherheitsniveaus dringend nötig sei.

Wenig später stieg mein Co-Autor aus dem Projekt aus und es ging alleine weiter. Im Januar 2025 war dann klar: Die aktuelle Regierung wird das NIS-2-Umsetzungsgesetz nicht mehr verabschieden. Die mit Hochdruck fertiggestellten Manuskripte wanderten in die Schublade.

Mit Veröffentlichung der neuen Regierungsentwürfe im Juni/Juli 2025 durften sie diese wieder verlassen. Bis zur Verabschiedung im Bundestag am 13.11.2025 blieb der Inhalt aber im Detail unklar. Erst einen Tag vorher reichte die Regierung einen Änderungsantrag ein, der zahlreiche Anpassungen in den Manuskripten notwendig machte.

Mit Hochdruck und Teamwork haben die Nomos-Verlagsgesellschaft und ich es aber dennoch geschafft, binnen zwei Wochen die Manuskripte zu finalisieren, Druckfahnen zu erstellen und zu korrigieren.

Der Fokus des Handbuchs ist nicht auf Vollständigkeit gerichtet, sondern darauf, Anwendern in Unternehmen und in der Beratung eine Orientierung und Hilfe zu geben, um die neuen Anforderungen für mehr Cybersicherheit zu meistern.

An dieser Stelle möchte ich Dr. Marco Ganzhorn in besonderem Maße danken. Ohne ihn und sein stets unermüdliches und unterstützendes Lektorat gäbe es dieses Handbuch nicht. Eine bessere Zusammenarbeit kann man sich als Autorin nicht wünschen. Ein großer Dank gebührt auch meinem Mann, der sich geduldig meine Gedanken anhörte, als Sparring-Partner agieren musste und vor allem auf viele gemeinsame Wochenenden und Abende verzichtet hat.

Köln, im Dezember 2025 *Dr. Judith Nink*

Inhaltsverzeichnis

Vorwort 5

Literaturverzeichnis 11

Abkürzungsverzeichnis 15

§ 1 Einführung 19

A. Allgemeines 19
B. Historie 20
C. Kontext und Querbezüge 21
I. Ziele der EU-Cybersicherheitsstrategie 21
II. Umsetzung in Deutschland 25
D. Begrifflichkeiten 27
I. Überblick 27
II. Einzelne Begrifflichkeiten 28
E. Globale Kooperation 39
I. Kooperationsgruppe 39
II. Computer-Notfallteams (CSIRTs) 40
III. EU-CyCLONe 40

§ 2 Anwendungsbereich 41

A. Allgemeines 41
B. Räumlicher Anwendungsbereich 42
C. Sachlicher und persönlicher Anwendungsbereich 43
I. Einrichtungsart 44
II. Besonders wichtige Einrichtungen 46
III. Wichtige Einrichtungen 49
IV. Berechnung der Schwellenwerte 50
V. Ausnahmen 54
VI. Bundesverwaltung 56
D. Anlage 1 und 2 BSIG: Betroffene Einrichtungen 58
I. Einrichtungsarten mit Verweisen: Beispiele 58
II. Einrichtungsarten mit NACE-Codes 59
III. Sonstige Einrichtungsarten: Beispiele 63

§ 3 Mindestanforderungen IT-Sicherheit 66

A. Allgemeines 66
B. Maßstab 67
I. Verhältnismäßige und geeignete Maßnahmen 67
II. Anforderungen 69
III. Mindestmaßnahmen 70
IV. Dokumentationspflicht 77
V. Cybersicherheitszertifizierung 78
VI. Keine zusätzlichen Pflichten aus Meldungen 80
C. Betreiber kritischer Anlagen 80
I. Erhöhte Sicherheitsanforderungen 80
II. Systeme zur Angriffserkennung 81
D. Branchenspezifische Sicherheitsstandards 82
I. Erarbeitung und Erlass von B3S 82
II. Wirkung und Verbindlichkeit 83
III. Bereits existierende B3S 84
E. Bundesverwaltungen 85
I. Aufgaben des BSI 86
II. Abweichungen 86
III. Ausnahmen 86
IV. Wirkung 87
V. Verpflichtung von Beauftragten 87
VI. Unterrichtungspflicht 88
F. Bestellung eines Vertreters 88

§ 4 Sonstige Pflichten 89

A. Allgemeines 89
B. Meldepflichten, § 32 BSIG 89
I. Meldestelle, Verfahren 92
II. Fristen 92
III. Ausnahmen 96
IV. Pflichten des BSI 96
C. Registrierungspflichten 97
I. Allgemeine Registrierungspflicht, § 33 BSIG 97
II. Besondere Registrierungspflicht, § 34 BSIG 98
III. Änderungsmitteilungen 99
IV. Ausnahmen 99

§ 5 Aufsicht 100
A. Allgemeines 100
I. Das BSI und das BSIG 100
II. Allgemeine Aufgaben und Befugnisse des BSI 101
B. Aufsichtsbehörde 104
I. Zuständigkeit des BSI 104
II. Ausnahmen 104
C. Aufsichts- und Durchsetzungsmaßnahmen 106
I. Maßnahmen 107
II. Zwangsgelder 110
III. Maßnahmen gegen Institutionen der Sozialen Sicherung 111
D. CISO Bund 111
E. Durchführung des Ordnungswidrigkeitenverfahrens 112
F. IT-Sicherheitskennzeichen 112
I. Allgemeines 112
II. Prüfungsverfahren 113
III. Anspruch auf Freigabe 114
IV. Erlöschen der Freigabe 115
V. Überprüfung durch das BSI 116

§ 6 Haftung 117
A. Allgemeines 117
B. Pflichten 117
I. Umsetzungs- und Überwachungspflicht 118
II. Fortbildungspflicht 120
C. Haftung 121
I. Allgemeine gesellschaftsrechtliche Haftungsgrundsätze 122
II. Voraussetzung der Haftung nach § 38 Abs. 2 BSIG 123
III. Directors & Officers (D&O)-Versicherung 123

§ 7 Sanktionen 124
A. Allgemeines 124
B. Überblick Bußgeldregime 125
I. Stufen der Geldbußen 125
II. Überblick Geldbußen 127
III. Anhebung der Höchstsummen 135
C. Berechnung von Geldbußen 135
I. Gesetz über Ordnungswidrigkeiten 136
II. Zuständigkeit für die Verhängung von Geldbußen 137
III. Verbot der Doppelbebußung 137

Stichwortverzeichnis 139

§ 1 Einführung

A. Allgemeines 1
B. Historie 3
C. Kontext und Querbezüge 5
I. Ziele der EU-Cybersicherheitsstrategie 7
II. Umsetzung in Deutschland 13
1. Konsequenzen einer europarechtswidrigen Umsetzung 14
2. Änderungen in Spezialgesetzen ... 16
D. Begrifflichkeiten 17
I. Überblick 18
II. Einzelne Begrifflichkeiten 21
1. Beinahevorfall (Nr. 1) 22
a) Verfügbarkeit 26
b) Integrität 27
c) Vertraulichkeit 28
2. (Erhebliche) Cyberbedrohung (Nr. 6, 10) 29
3. (Erheblicher) Sicherheitsvorfall (Nr. 11, Nr. 40) 32
4. Geschäftsleitung (Nr. 13) 36
5. IKT-Dienst (Nr. 14) 38
6. IKT-Produkt (Nr. 15) 41
7. IKT-Prozess (Nr. 16) 42
8. Managed Service Provider (Nr. 26) 43
9. Managed Security Service Provider (Nr. 25) 45
10. Cyberhygiene (§ 5 Abs. 3 S. 3 Nr. 7 EnWG) 46
11. Betreiber kritischer Anlagen (§ 28 Abs. 8 S. 1 BSIG) 48
E. Globale Kooperation 51
I. Kooperationsgruppe 52
II. Computer-Notfallteams (CSIRTs) ... 54
III. EU-CyCLONe 55

A. Allgemeines

Mit dem NIS-2-Umsetzungsgesetz[1] setzt der deutsche Gesetzgeber die NIS-2-Richtlinie (RL (EU) 2022/2555) um.[2] Diese ist Teil der europäischen Cybersicherheitsstrategie, die Ende 2020 verabschiedet wurde (Cybersicherheitsstrategie der EU, → Rn. 7 ff.).[3] Der Gesetzgeber selbst stellt das NIS-2-Umsetzungsgesetz zudem in den Kontext der **Europäischen Strategie für wirtschaftliche Sicherheit**[4] sowie der Resolution der Generalversammlung der Vereinten Nationen „Transformation unserer Welt: Die Agenda 2030 der Vereinten Nationen für nachhaltige Entwicklung".[5] 1

Im Wesentlichen hat der Gesetzgeber für **Unternehmen** mit dem NIS-2-Umsetzungsgesetz die folgenden, aus der NIS-2-Richtlinie vorgegebenen Änderungen im BSIG eingeführt:[6] 2

1. Einführung der durch die NIS-2-Richtlinie vorgegebenen **Einrichtungskategorien** „besonders wichtige Einrichtungen"[7] und „wichtige Einrichtungen", § 28 BSIG, sowie „Einrichtungen der Bundesverwaltung", § 29 BSIG (→ § 2 Rn. 1 ff.). Dadurch wird der Pflichtenkatalog signifikant über die bisher regulierten Betreiber Kritischer Infrastrukturen, ua auf Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse, ausgeweitet und es kommen zahlreiche Sektoren entsprechend

1 Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BT-Drs. 21/1501, 8.9.2025, geändert durch den Änderungsantrag v. 12.11.2025 BT-Drs. 21/2782.

2 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, ABl. L 333, 80 v. 27.12.2022.

3 S. https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-strategy.

4 European economic security strategy, Brüssel 20.6.2023, JOIN/2023) 20 final.

5 Resolution der Generalversammlung der Vereinten Nationen vom 25.9.2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung", A/RES/70/1, https://www.un.org/depts/german/gv-70/band1/ar70001.pdf.

6 BT-Drs. 21/1501, 3.

7 Die NIS-2-Richtlinie spricht von „wesentlichen" Einrichtungen. Die abweichende Bezeichnung in der deutschen Umsetzung ist unschädlich, aber vor dem Hintergrund einer avisierten einheitlichen EU-Umsetzung unverständlich.

ihres Digitalisierungsgrades und ihrer Bedeutung für Wirtschaft und Gesellschaft hinzu.[8]

> **Praxishinweis: Neue Sektoren**
>
> Als neue Sektoren hinzugekommen sind die
>
> - Sektoren besonders wichtiger und wichtiger Einrichtungen: Weltraum (Anlage 1 Nr. 7 BSIG), Abwasserbeseitigung (Anlage 1 Nr. 5.2.1 BSIG) und Bundesverwaltungen (§ 29 BSIG);[9]
> - Sektoren wichtiger Einrichtungen: Post- und Kurierdienste (Anlage 2 Nr. 1.1 BSIG), Abfallbewirtschaftung (Anlage 2 Nr. 2 BSIG), Produktion, Herstellung und Handel mit chemischen Stoffen (Anlage 2 Nr. 3 BSIG), Produktion, Verarbeitung und Vertrieb von Lebensmitteln (Anlage 2 Nr. 4 BSIG), Verarbeitendes Gewerbe/Herstellung von Waren (Anlage 2 Nr. 5 BSIG), Anbieter digitaler Dienste (Anlage 2 Nr. 6 BSIG) und Forschung (Anlage 2 Nr. 7 BSIG).

2. Ein Katalog der **Mindestsicherheitsanforderungen** (sogenannte Risikomanagementmaßnahmen), deren Intensität sich an der jeweiligen Einrichtungskategorie orientiert (→ § 3 Rn. 1 ff.).
3. Änderung der bisherigen deutschen einstufigen Meldepflicht bei Sicherheitsvorfällen auf das in der NIS-2-Richtlinie vorgesehene **dreistufige Melderegime** (→ § 4 Rn. 1 ff.).
4. Ausweitung des Instrumentariums des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Hinblick auf von der NIS-2-Richtlinie vorgegebene Aufsichtsmaßnahmen sowie die Funktion des CISO Bunds (→ § 5 Rn. 1 ff.).
5. Risikomanagementpflichten für Geschäftsleitungen, § 38 BSIG (→ § 6 Rn. 1 ff.).

Das bereits in § 9c BSIG-alt existierende einheitliche, freiwillige IT-Sicherheitskennzeichen zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien hat der deutsche Gesetzgeber mit wenigen redaktionellen Änderungen in § 55 BSIG fortgeführt (→ § 5 Rn. 41 ff.).

B. Historie

3 Das Umsetzungsverfahren der NIS-2-Richtlinie verlief zäh. Der Gesetzgeber ließ die Umsetzungsfrist in Art. 41 Abs. 1 der NIS-2-Richtlinie – ebenso bei der CER-Richtlinie (RL (EU) 2022/2557) zum 17.10.2024 verstreichen, trotz der im Frühjahr/Sommer kurz hintereinander veröffentlichten diversen Referentenentwürfe.[10] Der mit Datum vom 22.7.2024 veröffentlichte Gesetzentwurf wurde erst am 2.10.2024 in eine Bundestagsdrucksache überführt.[11] Zwar gab es am 11.10.2024 eine Beratung im Bundestag und Empfehlungen von Ausschüssen,[12] anschließend passierte aber nichts mehr. Die EU-Kommission hat daher gegen Deutschland – und 22 weitere Mitgliedstaaten – ein **Vertragsverletzungsverfahren** eingeleitet, weil sie die NIS-2-Richtlinie – sowie die

8 Werry/Éles MMR 2024, 829 (830).
9 Entspricht in etwa der öffentlichen Verwaltung iSv Anhang 1 Nr. 10 NIS-2-Richtlinie.
10 Zum Verlauf: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CII/nis2umsucg.html.
11 BT-Drs. 20/13184.
12 S. https://dip.bundestag.de/vorgang/gesetz-zur-umsetzung-der-nis-2-richtlinie-und-zur-regelung-wesentlicher-grundzüge/314976?f.deskriptor=Innerstaatliche%20Umsetzung%20von%20EU-Recht&rows=25&pos=4&ctx=e.

CER-Richtlinie (RL (EU) 2022/2557) nicht vollständig umgesetzt haben. Im Frühjahr 2025 hat sich die EU-Kommission entschlossen, gegen Deutschland, Ungarn und Österreich zu klagen.[13]

Mit Datum vom 23.6.2025 veröffentlichte die neue Bundesregierung einen im Wesentlichen auf dem Gesetzentwurf BT-Drs. 20/13184 basierenden neuen Referentenentwurf.[14] Der einen Monat später folgende Regierungsentwurf mit Datum vom 25.7.2025 enthielt lediglich leichte Überarbeitungen und wurde dann im September 2025 in einen Gesetzentwurf überführt,[15] und am 14.11.2025 mit weiteren Änderungen[16] in der 2. und 3. Lesung angenommen. 4

Wesentliche **Änderungen** im Vergleich zum Regierungsentwurf aus der vorherigen Legislaturperiode sind

- die Einschränkung des Anwendungsbereichs in § 28 Abs. 3 BSIG anknüpfend an die Einrichtungsart statt der Berechnung der Schwellenwerte (→ § 2 Rn. 8),
- erweiterte Befugnisse bei der Untersagung kritischer Komponenten iSv § 2 Nr. 23 BSIG gemäß § 41 BSIG (→ § 5 Rn. 5),
- die Übertragung der Aufgabe des **Koordinators der Bundesregierung für Informationssicherheit,** sogenannter CISO Bund, an das BSI, § 48 BSIG (→ § 5 Rn. 38 f.).

C. Kontext und Querbezüge

In Art. 2 Abs. 12 NIS-2-Richtlinie hat der Gesetzgeber klargestellt, dass die NIS-2-Richtlinie die Regelungen zum Datenschutz und zum Schutz der Privatsphäre nach der **Datenschutz-Grundverordnung** (VO (EU) 2016/679) und der Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie, RL 2002/58/EG) ebenso unberührt lässt wie die Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie (RL 2011/93/EU), die Richtlinie über Angriffe auf Informationssysteme (RL 2013/40/EU) und die Richtlinie über die Resilienz kritischer Einrichtungen (RL (EU) 2022/2557). 5

Der deutsche Gesetzgeber hat in den §§ 20 ff. BSIG die bisherigen Regelungen aus §§ 3a, 6, 6a-6f BSIG-alt fortgeschrieben, wo er bereits von den Öffnungsklauseln in Art. 6 Abs. 3 DS-GVO sowie Art. 23 Abs. 1 lit. c DS-GVO Gebrauch gemacht und sowohl die **Zulässigkeit der Datenverarbeitung** durch das BSI in § 20 BSIG präzisiert als auch **Beschränkungen der Betroffenenrechte** in den §§ 21–27 BSIG geregelt hatte. 6

I. Ziele der EU-Cybersicherheitsstrategie

Mit der EU-Cybersicherheitsstrategie will die Union zum einen die Sicherheit wesentlicher Dienstleistungen, wie Krankenhäuser, Energienetze und Eisenbahnen, aber auch „die Sicherheit der ständig wachsenden Anzahl von vernetzten Objekten in unseren 7

13 Pressemitteilung vom 7.5.2025, abrufbar unter: https://germany.representation.ec.europa.eu/news/vertragsverletzungsverfahren-zwei-entscheidungen-zu-deutschland-2025-05-07_de.
14 S. auch Nink EuDIR 2025, 185 Rn. 2.
15 Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BT-Drs. 21/1501, 8.9.2025.
16 BT-Drs. 21/2782.

Häusern, Büros und Fabriken" abdecken.[17] Im Fokus der **EU-Cybersicherheitsstrategie** stehen der Aufbau „kollektiver Fähigkeiten" gemeinsam mit internationalen Partnern, mit dem Ziel der Reaktionsfähigkeit auf große Cyberangriffe und der Gewährleistung der internationalen Sicherheit und Stabilität im Cyberspace.[18]

8 Die Union hat ihre Strategie in drei Fokusbereiche eingeteilt:

1. **Resilienz**, technologische Souveränität und Führung;
2. operative Fähigkeit zur **Verhinderung, Abschreckung** und **Reaktion**;
3. **Zusammenarbeit** zur Förderung eines globalen und offenen Cyberspace.[19]

Die NIS-2-Richtlinie ist dem zweiten und dritten Fokusbereich zuzuordnen, dh insbesondere dem Bereich der **Verhinderung** von, der Abschreckung vor und der Reaktion auf Cyberangriffe. Unter anderem werden mit dem Computer Security Incident Response Team (CSIRT), Art. 10 NIS-2-Richtlinie, und der **NIS-Kooperationsgruppe**, Art. 14 NIS-2-Richtlinie (→ Rn. 52 f.), die notwendigen Stellen für die Zusammenarbeit geschaffen (→ Rn. 51 ff.).[20]

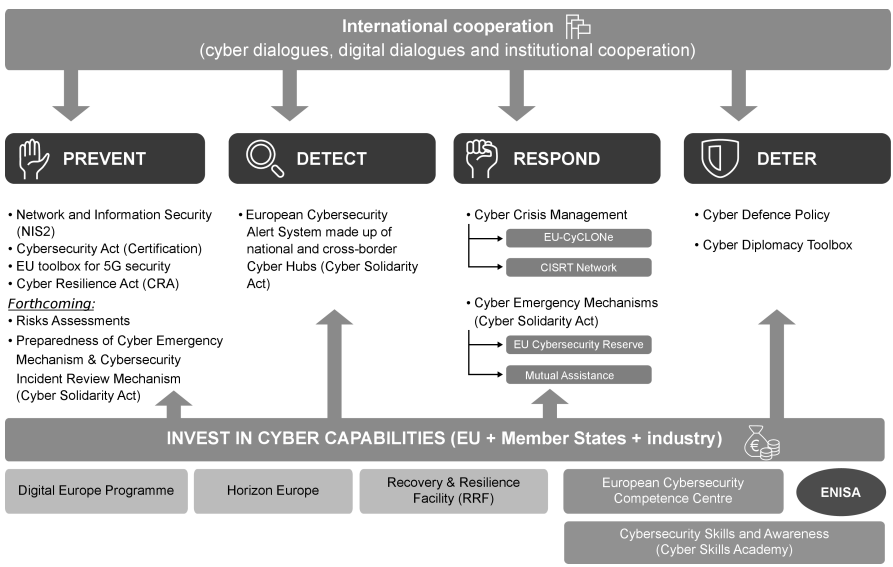

Abb.: Grafik zur Illustration, wie die unterschiedlichen Gesetzesinitiativen im Kontext der EU-Cybersicherheitsstrategie einzuordnen sind.[21]

9 Die ursprünglich (2016) auf die Sicherheit von Netz- und Informationssystemen (kurz „NIS") gerichtete Richtlinie hat in ihrer neuen Fassung einen deutlich breiteren Fokus erhalten. In der aktualisierten Fassung hat der europäische Gesetzgeber sie insbesondere

17 S. https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies.
18 S. https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies.
19 S. https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies.
20 S. https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies.
21 S. https://digital-strategy.ec.europa.eu/de/policies/cybersecurity.

auf zahlreiche Sektoren und Einrichtungen erweitert und ihren Namen konsequenterweise auf „Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union" angepasst. Lediglich die Abkürzung „NIS" ist geblieben. Im Wesentlichen will der europäische Gesetzgeber mit der NIS-2-Richtlinie Unternehmen, die als Betreiber wesentlicher Dienste in bestimmten Sektoren eingestuft wurden, inkl. **digitaler Dienste** wie Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze, verpflichten, geeignete Sicherheitsmaßnahmen zu ergreifen und die zuständigen nationalen Behörden über schwerwiegende Vorfälle zu informieren.

10 Die NIS-2-Richtlinie steht im engen Kontext mit dem als Verordnung gestalteten **Cyber Resilience Act** VO (EU) 2024/2847.[22] Mit dem Cyber Resilience Act sollen durch Cybersicherheitsvorschriften sichere Produkte mit digitalen Elementen entwickelt werden, damit Hersteller Hardware- und Softwareprodukte mit weniger Schwachstellen in den Verkehr bringen (Erwägungsgrund 2 VO (EU) 2024/2847). Der Cyber Resilience Act ist daher als eine Art Zwilling der NIS-2-Richtlinie für die digitale Cyber-Produktsicherheit zu sehen.

11 Zeitgleich mit der NIS-2-Richtlinie hat der europäische Gesetzgeber die RL (EU) 2022/2557 (CER-Richtlinie)[23] verabschiedet. Mit der CER-Richtlinie soll die Resilienz kritischer Einrichtungen gestärkt werden. Kritische Einrichtungen sind solche, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten unerlässlich sind und von den Mitgliedstaaten als kritische Einrichtung eingestuft werden.[24] Die Pflichten ähneln den Pflichten aus der NIS-2-Richtlinie. Die Umsetzungsfrist lief parallel mit der Umsetzungsfrist der NIS-2-Richtlinie am 17.10.2024, Art. 26 CER-Richtlinie, ab. Zum Zeitpunkt des Redaktionsschlusses lag lediglich ein Regierungsentwurf zum sogenannten **KRITIS-DachG** vor.[25]

12 Am 16.1.2025 sind die Regelungen des Digital Operational Resilience Act VO (EU) 2022/2554 (DORA)[26] in Kraft getreten. Mit DORA regelt die EU die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz für den **Finanzsektor**. Als sektorspezifische Regelung genießt DORA in den Bereichen Cybersicherheitsrisikomanagement, Berichtspflichten, Aufsicht und Durchsetzung als *lex specialis* Vorrang vor der NIS-2-Richtlinie, Erwägungsgrund 28 NIS-2-Richtlinie.[27] DORA soll dazu beitragen, den europäischen Finanzmarkt gegenüber Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie (IKT) zu stärken. Ein wichtiger Baustein

22 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23.10.2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L 2024/2847 v. 20.11.2024.

23 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333/164 v. 27.12.2022.

24 Art. 1 Abs. 1 lit. a CER-Richtlinie; Überblick zu den Regelungen der CER-Richtlinie Hornung/Muttach/Schaller CR 2024, 229 ff.

25 Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG), 10.9.2025.

26 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14.12.2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, v. 27.12.2022, ABl. L 333/1, 1.

27 S. auch Kipker/Dittrich MMR 2023, 481 (482).

von DORA sind die vertraglichen Verpflichtungen des IKT-Dienstleisters in der **Lieferkette**, konkret mindestens, Art. 30 Abs. 2 DORA:

- eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat (Art. 30 Abs. 2 lit. a DORA),
- die Standorte – das heißt die Regionen oder Länder –, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen (Art. 30 Abs. 2 lit. b DORA),
- Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten (Art. 30 Abs. 2 lit. c DORA),
- Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format (Art. 30 Abs. 2 lit. d DORA),
- Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen (Art. 30 Abs. 2 lit. e DORA),
- die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten (Art. 30 Abs. 2 lit. f DORA),
- die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten (Art. 30 Abs. 2 lit. g DORA),
- Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden (Art. 30 Abs. 2 lit. h DORA),
- Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz gem. Art. 13 Abs. 6 DORA (Art. 30 Abs. 2 lit. i DORA).

Zusätzliche Vereinbarungen müssen Finanzunternehmen aufgrund der besonderen Kritikalität mit IKT-Dienstleistern vereinbaren, die IKT-Dienstleistungen zur **Unterstützung kritischer oder wichtiger Funktionen** erbringen (Art. 30 Abs. 3 DORA). Dazu gehören neben Notfallplänen und Tests (Art. 30 Abs. 3 UAbs. 1 lit. c DORA) auch die Vereinbarung von Ausstiegsstrategien (Art. 30 Abs. 3 UAbs. 1 lit. e DORA).

> **Praxishinweis:**
>
> Ausstiegsstrategien sind je nach Dienstleistung nicht immer ohne Weiteres umsetzbar. Gerade auf Hyperscalern in der Cloud entwickelte Dienstleistungen lassen sich häufig nicht 1:1 austauschen. Das sollten Finanzunternehmen bereits vor der Beauftragung berücksichtigen.

II. Umsetzung in Deutschland

Überwiegend hat der deutsche Gesetzgeber die Regelungen der NIS-2-Richtlinie wörtlich übernommen. In einigen Vorschriften finden sich jedoch nicht immer nachvollziehbare, aber durch Auslegung unschädliche Zusätze (zB → § 3 Rn. 4). Kritisch ist die Eingrenzung des Anwendungsbereichs in § 28 Abs. 3 BSIG durch eine von der NIS-2-Richtlinie abweichende Einordnung zu den Einrichtungsarten in Anlage 1 und 2 BSIG (→ § 2 Rn. 8). Die Regelung dürfte **europarechtswidrig** sein (ausf. → § 2 Rn. 8). 13

Praxishinweis: Umsetzungsspielraum allgemein

Die Mitgliedstaaten verfügen bei der Umsetzung von Richtlinien über einen Ermessensspielraum. Jedoch wird dieser dadurch beschränkt, dass das Erreichen der inhaltlichen Ziele und die praktische Wirksamkeit der Richtlinie gewährleistet werden müssen.[28] Nach Art. 288 AEUV sind Richtlinien hinsichtlich der Ziele verbindlich, die Wahl der Form und der Mittel ist jedoch – in Grenzen – den Mitgliedstaaten überlassen.

Ermessensspielräume ergeben sich nur innerhalb der von der jeweiligen Richtlinie gezogenen Grenzen. Auch bei den Mitteln haben die Mitgliedstaaten nur dann eine Wahlmöglichkeit, wenn und soweit die Richtlinienbestimmung hierzu keine Festlegung trifft.[29]

Der Umsetzungsspielraum ist daher stets im Einzelfall zu prüfen. Selbst bei Richtlinien, die lediglich einen Rahmen regeln wollen, ist es möglich, dass dem umsetzenden Mitgliedstaat im Einzelfall kein nennenswerter Umsetzungsspielraum bleibt, wenn die konkrete Richtlinie über eine erhebliche normative Dichte verfügt.[30] Soweit die Mitgliedstaaten einen Umsetzungsspielraum haben, sind sie bei der Umsetzung verpflichtet, „diejenigen Formen und Mittel zu wählen, die für die Gewährleistung der praktischen Wirksamkeit (effet utile) der Richtlinien am besten geeignet sind".[31]

1. Konsequenzen einer europarechtswidrigen Umsetzung

Praktisch hat die europarechtswidrige Regelung – bis zu einer Entscheidung des EuGH – aber keine Konsequenzen, die Vorschrift bleibt bis zur Änderung durch den deutschen Gesetzgeber in Kraft.[32] Es kommt weder eine direkte Anwendung von Art. 2 Abs. 1 NIS-2-Richtlinie in Betracht noch eine richtlinienkonforme Auslegung. 14

Praxishinweis: Unmittelbare Anwendung / richtlinienkonforme Auslegung

Eine Richtlinienbestimmung kann nur dann unmittelbar angewendet werden, wenn diese dem Einzelnen ein subjektiv-öffentliches oder individuelles Recht zuschreibt oder den Einzelnen jedenfalls begünstigt.[33] Es muss sich um die Geltendmachung von Rechten des Bürgers gegen den Staat handeln.[34] Ausgeschlossen ist eine **unmit-**

28 Ausf. Nink EuDIR 2025, 185 Rn. 6 f.
29 Grabitz/Hilf/Nettesheim/Nettesheim AEUV Art. 288 Rn. 112; Nink EuDIR 2025, 185 Rn. 7.
30 Callies/Ruffert/Ruffert AEUV Art. 288 Rn. 26; Nink EuDIR 2025, 185 Rn. 8.
31 EuGH 8.4.1976 – Rs 48/75, NJW 1976, 2065 (2067).
32 Ausf. zu den Konsequenzen einer nicht richtlinienkonformen Umsetzung: Nink EuDIR 2025, 185 Rn. 14 ff. IE auch Hessel/Callewaert/Schneider RFamU 2024, 200 (201).
33 Streinz/Schroeder AEUV Art. 288 Rn. 95 f.
34 EuGH 19.1.1982 – Rs 8/81, NJW 1982, 499 (500).

telbare Wirkung stets für Regelungen, die rechtliche Verpflichtungen für Private begründen.[35]

Art. 2 Abs. 1 NIS-2-Richtlinie regelt, welche Unternehmen unter den Anwendungsbereich fallen, mit der Konsequenz, dass diese die entsprechenden Sicherheitsmaßnahmen umsetzen müssen. Aus Art. 2 Abs. 1 NIS-2-Richtlinie leiten sich folglich keine Rechte der Unternehmen gegen den Staat ab. Vielmehr treffen sie **rechtliche Verpflichtungen**, sodass eine unmittelbare Wirkung ausgeschlossen ist.

Auch eine richtlinienkonforme Auslegung kommt nicht infrage. Zwar ist der Grundsatz der **richtlinienkonformen Auslegung** in der Rechtsprechung des EuGH und der Mitgliedstaaten anerkannt. Mitgliedstaatliches Recht soll danach durch die nationalen Gerichte im Lichte des Wortlauts und Zwecks der Richtlinie ausgelegt werden.[36] Dafür muss die nationale Regelung aber auch auslegungsfähig sein. Ob eine Auslegung möglich ist, beurteilt sich nach den Kriterien des nationalen Rechts[37] und kann durch eine Auslegung des Wortlauts oder bspw. durch eine teleologische Reduktion erfolgen.[38] Aufgrund des klaren Wortlauts in § 28 Abs. 3 BSIG und der gesetzgeberischen Intention kommt aber beides hinsichtlich der aufgeweichten Bestimmung der Einrichtungsart nicht in Betracht.

15 Kommt eine Rechtsfortbildung, wie hier, nicht in Betracht, behält die gegenständliche Norm bis zu ihrer Abänderung ihre Wirksamkeit.[39] Die Korrektur der Unionsrechtswidrigkeit ist nach Auffassung des BGH allein Aufgabe der Legislative.[40] Durch die fehlerhafte Umsetzung der NIS-2-Richtlinie droht Deutschland aber ein weiteres **Vertragsverletzungsverfahren** nach Art. 258 AEUV.

2. Änderungen in Spezialgesetzen

16 Die größten Änderungen aus dem NIS-2-Umsetzungsgesetz ergeben sich für das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Aufgrund der zahlreichen Querbezüge in **Spezialgesetze** waren aber auch Änderungen in zahlreichen weiteren Gesetzen notwendig, überwiegend jedoch formaler Natur. Inhaltliche Änderungen erfolgten vor allem in folgenden Gesetzen:

- Energiewirtschaftsgesetz: Regelung der IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz (§ 5c EnWG), Dokumentations-, Melde-, Registrierungspflicht (§ 5c EnWG), Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen (§ 5e EnWG), Ergänzung des Ordnungswidrigkeitentatbestands (§ 95 Abs. 1, 2–8 EnWG).
- Telekommunikationsgesetz: Änderung Definition des IT-Sicherheitsvorfalls (§ 3 Nr. 53 TKG), Definition des Netz- und Informationssystems (§ 3 Nr. 80 TKG), Maßnahmen zum Schutz von Systemen vor Sicherheitsvorfällen (§ 165 Abs. 2a TKG: Risikomanage-

35 EuGH 26.2.1986 – Rs 152/84, NJW 1986, 2178 Rn. 48; s. konkret bzgl. der deutschen Umsetzung im BSIG Werry/Éles MMR 2024, 829 (832).
36 EuGH 10.4.1984 – Rs 14/83, NZA 1984, 157 (158).
37 Streinz/Schroeder AEUV Art. 288 Rn. 113.
38 BGH 26.11.2008 – VIII ZR 200/05, NJW 2009, 427 Rn. 21 f.
39 BGH 18.11.2020 – VIII ZR 78/20, NJW 2021, 1008 Rn. 46; Nink EuDIR 2025, 185 Rn. 17.
40 BGH 18.11.2020 – VIII ZR 78/20, NJW 2021, 1008 Rn. 44.

mentmaßnahmen), Verpflichtungen der Geschäftsleitung und deren Haftung (§ 165 Abs. 2b–d TKG) sowie Meldung eines Sicherheitsvorfalls (§ 168 TKG).

D. Begrifflichkeiten

Verwendete Begrifflichkeiten sind wie auch schon bisher überwiegend in § 2 BSIG definiert. Die Liste ist, dem Ausweiten des Regelungsbereichs geschuldet, stark – von 14 auf 46[41] Definitionen – gewachsen. Leider können Anwender die Definitionen aus § 2 BSIG nicht als alleinige Quelle heranziehen. Wie die NIS-2-Richtlinie enthält auch § 2 BSIG zahlreiche **Verweisketten** in EU-Verordnungen und -Richtlinien. Zudem versteckt der Gesetzgeber teils Definitionen in einzelnen Vorschriften (→ Rn. 46, 48). 17

I. Überblick

Gegenüber § 2 BSIG-alt gibt es in § 2 BSIG die folgenden **neuen Definitionen**: Beinahevorfall (Nr. 1, → Rn. 22 ff.), Berechtigte Zugangsnachfragen (Nr. 2), Bodeninfrastruktur (Nr. 3), Content Delivery Network (Nr. 5), Cyberbedrohung (Nr. 6, → Rn. 29 ff.), DNS-Diensteanbieter (Nr. 8), Domain-Name-Registry-Dienstleister (Nr. 9), Erhebliche Cyberbedrohung (Nr. 10, → Rn. 29 ff.), Erheblicher Sicherheitsvorfall (Nr. 11, → Rn. 32 ff.), Forschungseinrichtung (Nr. 12), Geschäftsleitung (Nr. 13, → Rn. 36 f.), IKT-Dienst (Nr. 14, → Rn. 38 ff.), IKT-Prozess (Nr. 16, → Rn. 42), Institutionen der sozialen Sicherung (Nr. 19), Internet Exchange Point (Nr. 20), Managed Security Service Provider (Nr. 25, → Rn. 45), Managed Service Provider (Nr. 26, → Rn. 43 ff.), NIS-2-Richtlinie (Nr. 27), Plattform für Dienste sozialer Netzwerke (Nr. 30), Qualifizierter Vertrauensdienst (Nr. 33), Qualifizierter Vertrauensdiensteanbieter (Nr. 34), Rechenzentrumsdienst (Nr. 35), Sicherheit in der Informationstechnik (Nr. 39), Sicherheitsvorfall (Nr. 40, → Rn. 32 ff.), Top Level Domain Name Registry (Nr. 42), Vertrauensdienst (Nr. 43), Vertrauensdiensteanbieter (Nr. 44) und Weltraumgestützte Dienste (Nr. 45). 18

Neu ist der **Betreiber einer kritischen Anlage** (§ 28 Abs. 8 S. 1 BSIG, → Rn. 48). Das BSIG-alt verwendete den Begriff der Betreiber Kritischer Infrastrukturen an diversen Stellen, ohne ihn aber zu definieren. Der Begriff der Kritischen Infrastruktur aus dem BSIG-alt ist in § 2 Nr. 22 BSIG durch Kritische Anlage ersetzt worden. 19

In teils lediglich redaktionell, teils inhaltlich geänderter Fassung regelt § 2 BSIG die bereits **bekannten Begrifflichkeiten**: Cloud-Computing-Dienst (Nr. 4, bisher Abs. 11 Nr. 3 BSIG-alt), IKT-Produkt (Nr. 15, bisher Abs. 9a BSIG-alt, → Rn. 41), Informationssicherheit (Nr. 17, bisher Abs. 2 S. 2 f. BSIG-alt), Informationstechnologie (Nr. 18, bisher Abs. 1 BSIG-alt), Kritische Anlage (Nr. 22, bisher Kritische Infrastruktur in Abs. 10 BSIG-alt), Kritische Komponenten (Nr. 23, bisher Abs. 13 BSIG-alt, die nunmehr schlicht IKT-Produkte sind, die durch eine Rechtsverordnung nach § 56 Abs. 7, 8 BSIG als solche bestimmt werden), Kritische Dienstleistungen (Nr. 24, bisher Abs. 10 Nr. 1 BSIG-alt, → Rn. 50), Online-Marktplatz (Nr. 28, bisher Abs. 11 Nr. 1 BSIG-alt) und Schwachstelle (Nr. 38, bisher Abs. 6 BSIG-alt). 20

41 41 Definitionen enthält die NIS-2-Richtlinie in Art. 6.

II. Einzelne Begrifflichkeiten

21 Die Komplexität der Anwendung der definierten Begrifflichkeiten sowie die teilweise inkonsistenten **Verweisketten** und damit die Herausforderungen bei der Bestimmung des Anwendungsbereichs zeigen die nachfolgenden Beispiele:

1. Beinahevorfall (Nr. 1)

22 Die Definition des Beinahevorfalls in § 2 Nr. 1 BSIG (Art. 6 Nr. 5 NIS-2-Richtlinie) hat der Gesetzgeber nach eigenen Angaben bewusst weit gefasst, tatsächlich aber im Wesentlichen die Definition aus Art. 6 Nr. 5 NIS-2-Richtlinie übernommen. Er knüpft dabei an das bereits im Rahmen des Begriffs der „Sicherheit in der Informationstechnik" in § 2 Abs. 2 S. 4 BSIG-alt verankerte Sicherheits-„Trias", konkret der Schutzziele der Informationssicherheit, dh der Verfügbarkeit, Integrität oder Vertraulichkeit an.[42] Ein Beinahevorfall ist danach „ein Ereignis, das die **Verfügbarkeit**, **Integrität** oder **Vertraulichkeit** gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert worden ist oder aus anderen Gründen nicht erfolgt ist".

23 Die Formulierung „beeinträchtigt haben könnte" lässt zum einen erahnen, wie weit der Gesetzgeber die Definition verstanden haben möchte, macht zum anderen aber auch deutlich, dass die Bewertung, ob ein Beinahevorfall vorlag oder nicht, stets eine **Einzelfallbetrachtung** ist und häufig zu Abgrenzungsproblemen in der Praxis führen wird:

> **Praxishinweis: Bewertung Beinahevorfall nach Auffassung des Gesetzgebers**
>
> Der Gesetzgeber selbst nennt als Beispiel für einen Beinahevorfall die professionell gestaltete Phishing-E-Mail, „die nur aufgrund entsprechender besonders intensiver Sensibilisierung der Mitarbeiter oder aufgrund einer erhöhten Aufmerksamkeit der Belegschaft als solche erkannt wurde", vorausgesetzt, diese wäre „unter sonst üblichen Bedingungen nicht erkannt worden".[43] Er zieht dabei eine Schwelle der Komplexität der Erkenn- und Verhinderbarkeit, ohne diese aber zu konkretisieren. Keine Beinahevorfälle seien jedoch „regelmäßige und alltägliche Störungen und Belästigungen wie Spam-E-Mails oder offenkundig auch für ungeschultes Personal als Phishing-E-Mail erkennbare E-Mails".[44] Die Negativbeispiele orientieren sich eher an Banalitäten. Wo diese beginnen oder aufhören, bleibt jedoch unklar.

24 Vom Wortlaut ist diese Auslegung des Gesetzgebers nicht gedeckt. Verständlich wird die Abgrenzung eher aus dem Kontext, in dem der Beinahevorfall im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik weiter geregelt ist: Informationen zu Beinahevorfällen und anderen Bedrohungen und Vorfällen nimmt das BSI als **zentrale Meldestelle** (→ § 5 Rn. 1ff.) entgegen, § 5 Abs. 2 S. 1 BSIG, und berichtet darüber der ENISA, § 58 Abs. 4 BSIG. Im Rahmen der zu errichtenden **Online-Plattform** zum Informationsaustausch (BSI-Portal) kann das BSI weiter die „beteiligten Hersteller, Lie-

42 BT-Drs. 21/1501, 125.
43 BT-Drs. 21/1501, 125.
44 BT-Drs. 21/1501, 125.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen (Beitrag), die mageren auf die Randnummer.

Abhilfemaßnahme, Pflicht **4** 18
Abschlussmeldung **4** 19
– Inhalt **4** 17
– Meldepflicht **4** 17
Abschöpfung, Jahresumsatz **7** 14
Abweichung, Mindeststandard **3** 53
Adressat, Netzwerk und IT-Sicherheitsorganisation **3** 15
Amtshilfe **5** 11
Anbieter
– Einrichtungsart **2** 13
– Entgeltlichkeit **2** 13
Anbieter öffentlicher Telekommunikationsnetze, Zuständigkeit **5** 17
Anbieter öffentlich zugänglicher Telekommunikationsdienste
– Schwellenwert **2** 12, 20
– Zuständigkeit **5** 17
Änderungsmitteilung **4** 32
Angabe, Übermittlung **4** 26
Angebot, Ware und Dienstleistung **2** 15
Angemessenheit, Bewertung **3** 8
Angriffserkennungssystem **3** 40 ff.
– Stand der Technik **3** 41
Anomaliedetektion **3** 41
Anwendungsbereich NIS-2, BSIG
– Ausnahmen **2** 31 ff.
– Einrichtungsarten, Betroffenheit **2** 42 ff.
– NACE-Codes **2** 45 ff.
– persönlicher **2** 7 ff.
– räumlicher **2** 4 ff.
– sachlicher **2** 7 ff.
– Sektoren **2** 42 ff.
Asset, Kronjuwelen **3** 17
Audit
– Durchführung **5** 30
– Gebühren **5** 31
– Kostenfreiheit **5** 31
Auffangtatbestand **6** 13
Aufsicht **5** 1 ff.; *siehe auch* Bundesamt für Sicherheit in der Informationstechnik (BSI)
– Aufgaben und Befugnisse **5** 3 ff.
– Aufsichtsbefugnis **3** 29, **5** 1 ff.
– Aufsichtsbehörde **5** 1 ff.
– Aussetzung **5** 22
Aufsichts- und Durchsetzungsmaßnahmen **5** 9, 19
Ausnahmebescheid, Befreiung **4** 33
Aussetzungsbefugnis
– Voraussetzung **5** 33
– vorübergehende Aussetzung **5** 32

Beauftragter, vertragliche Verpflichtung **3** 57
Befugnis, Anordnungsbefugnis **5** 22
Beinahevorfall **1** 18, 22
– Banalität **1** 25
– Komplexität **1** 25
Beschäftigtenschulung, E-Learning **3** 24
Besonders wichtige Einrichtung **2** 9 ff.
Betreiber
– Energieanlage **3** 21
– Telekommunikationsdienste, öffentliche Telekommunikationsnetze **2** 12, 20, **3** 47
Betreiber kritischer Anlagen **1** 48 ff., **3** 37 ff., **4** 27
– Ausnahme Meldepflicht **2** 33
– Begriff **1** 48 ff.
– Bundesverwaltung **2** 9
– erweiterte Sicherheitsmaßnahme **7** 6
– Informationspflicht **4** 15
– Pflichten **2** 1, 11
– Risikomanagement **3** 42
– Systeme zur Angriffserkennung **3** 40 ff.

– Zusatzpflicht, erhöhte Sicherheitsanforderungen **3** 3, 38 f.
– Zuständigkeit ***5*** 12
Betreiber wesentlicher Dienste, Sicherheitsmaßnahmen **1** 9
Bewertung eines Sicherheitsvorfalls **4** 15
Bezugsgröße, Stichtag Rechnungsabschluss **2** 27
Branchenarbeitskreis UP KRITIS **3** 43
Branchenspezifische Sicherheitsstandards (B3S) **3** 32 ff.
– Bestandsprüfung **3** 49
– Dokumentationspflicht **3** 46
– Eignungsprüfung **3** 44
– Erarbeitung **3** 43
– Gültigkeitsdauer **3** 44
– Informationssicherheit **3** 42
– Interpretation **3** 46
– Rechtssicherheit **3** 45
– Sektor **3** 47
– Stand der Technik **3** 45
– Umsetzung **3** 48
– Verbindlichkeit **3** 45
Bundesamt für Sicherheit in der Informationstechnik (BSI) **4** 31, ***5*** 2 ff.
– Allgemeinverfügung ***5*** 49
– Anordnung **4** 4
– Anordnungsbefugnis ***5*** 23
– Anordnungskompetenz ***5*** 27
– Aufgaben **3** 51 ff.
– Aufsicht ***5*** 12
– Aufsichtsbehörde **3** 60, ***5*** 1
– Ausnahme ***5*** 13
– Befugnis ***5*** 19
– Behebungsbefugnis ***5*** 26
– Beratung **3** 51
– Berichterstattung ***5*** 27
– Bundesoberbehörde ***5*** 2
– Datenschutz, Verarbeitungsbefugnis ***5*** 6 f.
– Durchsetzungsbefugnis **7** 1
– Ermessensspielraum ***5*** 21
– Gefahrenabwehr ***5*** 5
– Kontrolle ***5*** 58
– Kooperationsaufgabe ***5*** 3
– Koordinatorenrolle ***5*** 39
– Meldestelle ***5*** 5
– Mindeststandard **3** 51
– Mitteilung ***5*** 33
– Ordnungswidrigkeitenverfahren ***5*** 40
– Parallelaufsicht **2** 37
– Pflicht **4** 24
– Prüfungsbehörde ***5*** 46
– Regelungsregime **2** 40
– Risikomanagementpflicht ***5*** 23
– sachliche Zuständigkeit **7** 18
– Unterrichtspflicht ***5*** 28
– Unterstützung **4** 24, ***5*** 4
– Verantwortlichkeit ***5*** 41
– Verbraucherschutz ***5*** 3
– zentrale Meldestelle **1** 24
– zentrale Stelle für Informationssicherheit ***5*** 2
– zuständige Aufsichtsbehörde ***5*** 9
– Zuständigkeit ***5*** 8, 10
Bundes-Cloud **2** 53
Bundeskoordinator für Informationssicherheit (CISO Bund) ***5*** 38 ff.
Bundesministerium der Verteidigung (BMVg), Ausnahme **2** 41
Bundesministerium des Innern (BMI), Nutzungsvorgaben **3** 56
Bundesministerium für Digitales und Staatsmodernisierung, Fachaufsicht ***5*** 39
Bundesnetzagentur (BNetzA)
– Parallelaufsicht **2** 37
– Zuständigkeit **2** 36
Bundesverwaltung
– Ausnahme **2** 19
– Einrichtung **2** 39, **3** 53, 55
– Geldbuße **7** 3
– Leitungsverantwortung **6** 6
– Mindeststandard **3** 50
Business Continuity Management, Resilienz **3** 19
Bußgeld, Geldbuße **7** 7 ff.
– Bemessung, Kriterium **7** 17
– Berechnung **7** 13 ff.

– Bußgeldtatbestand, Zuordnung **7** 7
– Geldbußen, Überblick **7** 11
– Höchstbetrag **7** 8
– Stufen **7** 8
Bußgeldbewehrte Verpflichtungen ***5*** 37

Cape-Size-Rule, Schwellenwerte **2** 3
– Berechnung **2** 24 ff.
– besonders wichtige Einrichtungen **2** 12 ff.
– wichtige Einrichtungen **2** 20 ff.
CER-Richtlinie, Resilienz **1** 11
Chemischer Stoff, Definition REACH-VO **2** 47
CISO Bund ***5*** 38 ff.
Cloud-Computing-Dienst **1** 20
– erweiterte Pflicht **2** 55
– Variante **2** 54
Computer Security Incident Response Team (CSIRT)
– Informationsaustausch **1** 54
– Zusammenarbeit **1** 54
Cyberbedrohung **1** 29
– Definition **1** 30
– Erheblichkeitskriterium **1** 30
Cyberhygiene **3** 23
– Begriff **1** 46 f.
– Risikomanagementmaßnahmen **3** 23
– Schulung **1** 46
– Umfang **1** 47
Cyber Resilience Act (CRA), Produktsicherheit **1** 10
Cybersecurity Certification Scheme
– Cloud Services **3** 35
– Common Criteria (CC) **3** 35
Cybersicherheitsstrategie, EU **1** 1, 7 ff., 51, 54
Cybersicherheitszertifizierung **3** 2, 21, 32 ff.
– EU-Schema **3** 32
– Förderauftrag **3** 34

Darlegungs- und Beweislast **3** 31
Datenschutz, Meldepflicht **4** 2
Datenschutz-Grundverordnung (DSGVO) **1** 5, **7** 19
– Verstoß **7** 19
Delegierter Rechtsakt, Vorrang **3** 33
Diensteanbieter
– Antragsberechtigung ***5*** 46
– Cloud Computing **2** 5
– Vertreterpflicht **3** 59
Dienstleistung, Begriff **2** 16
Digitaler Dienst, Cloud-Computing-Dienst **2** 53
Digital Operational Resilience Act (DORA), Finanzsektor **1** 12
Directors and Officers-Versicherung (D&O-Versicherung) **6** 14
Dokumentationspflicht **3** 30
– faktische **3** 31
– Geldbuße **7** 6
– Rechenschaftspflicht **3** 2
– Risikomanagementmaßnahme **3** 29
Doppelbestrafung, Verbot **7** 19
Durchführungsrechtsakt **1** 34

Einrichtung **2** 1, 24, **3** 3
– Abhilfepflicht **4** 18
– Anwendung **2** 41
– Cybersicherheitsrisikomanagement ***5*** 15
– digitaler Dienst **2** 23
– Kategorie **2** 19
– Kriterium **2** 14
– Mitarbeitergrenze **2** 22
– öffentliches Telekommunikationsnetz **4** 23
– Reaktionspflicht **4** 16
– Schwellenwert **2** 14
– Umsatzgrenze **2** 22
Einrichtungsart **2** 3
– Bestimmung **2** 8 ff.
– Cloud-Computing-Dienst **2** 52
– grenzüberschreitende Tätigkeit ***5*** 13
– Haupttätigkeit **2** 9
– Kategorie **2** 8
– Kriterium **2** 44
– Managed Service Provider **2** 52

– Monopolstellung **2** 10
– NACE **2** 42
– NACE-Code **2** 45 f.
– Nebentätigkeit **2** 9
– vernachlässigbare Tätigkeit **2** 9
Einrichtungsregister **4** 30
Einvernehmen, Aufsichtsbehörde ***5*** 36
Einzelfallbetrachtung **1** 23
Einzelhändler **2** 48
E-Learning **3** 24
– Beschäftigtenschulung **3** 24 f.
– Geschäftsleiterschulung, Fortbildung **6** 7 ff.
Energiespeicheranlage **2** 43
Energiewirtschaftsgesetz, IT-Sicherheitspflicht **1** 16
Erheblicher Sicherheitsvorfall
– grenzüberschreitende Auswirkungen **4** 13
– Kriterium **1** 35
Ermessen, Mitgliedstaat **7** 3
Erstmeldung
– Fristbeginn **4** 20
– Prognose **4** 13
Erzeugungsanlage **2** 43
EU-Cybersicherheitsstrategie
– kollektive Fähigkeit **1** 7
– Ziel **1** 7
EU-CyCLONe
– Informationsaustausch **1** 55
– Koordination **1** 55
– Mitglieder **1** 56
EU-Kommission, Delegierter Rechtsakt **3** 33

Finanzsektor, Ausnahmeregelung **1** 48
Finanzunternehmen, Ausnahme **2** 32
Fortbildungspflicht
– Bundesverwaltung **6** 7
– Geschäftsleitung **6** 7
Fortschrittsmeldung **4** 19; *siehe* Meldepflicht
Fristberechnung
– einheitliche **4** 21
– grenzüberschreitende **4** 21

Gebietskörperschaft, Ausschluss des Anwendungsbereichs **2** 38
Gefahrenübergreifender Ansatz, äußere Ereignisse **3** 12
Geldbuße **7** 7 ff.
– Abschöpfung **7** 9
– Abschreckungseffekt **7** 13
– alternative Höchststufe **7** 10
– Berechnung **7** 13
– Höchstsumme **7** 11
– Mindesthöchstbetrag **7** 4
Geschäftsleitung
– Begriffsbestimmung **1** 36
– Berichtspflicht **6** 1
– D&O Versicherung **6** 14
– Delegation **6** 4, 7
– Fortbildungspflicht **6** 7 ff.
– Fortbildungspflicht, Schulung **6** 7 ff.
– Haftung **1** 37, **6** 10 ff., **7** 1
– Legalitätsprinzip **6** 2
– Risikomanagement **6** 1, 5
– Risikomanagementpflicht **1** 37
– Überwachungspflicht **6** 4
– Umsetzung **6** 2
– Umsetzungspflicht **6** 4
– Vertretungsbefugnis **6** 3
Geschäftstätigkeit, Zuordnung **2** 28
Gesellschaft für Telematik **2** 32
Gesetzgeber, Regelungskompetenz **2** 4, **3** 14
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)
– Änderung **1** 16
– Anwendungsbereich **1** 4, 13
– Befugnisse BSI **1** 4, **5** 1 ff.
– Beschränkung Betroffenenrechte **1** 6
– Datenverarbeitungszulässigkeit **1** 6
– Definitionen **1** 17
Grundschutz++, Methodik **3** 52

Haftung, Innenhaftung **6** 10
Händler, Regulierung **2** 48
Hauptniederlassung **5** 15
– Beschäftigtenzahl **2** 6

– Cybersicherheitsmaßnahme **5** 16
– Entscheidungsort **2** 6
Herrschendes Unternehmen, Unternehmensgruppe **5** 16
Hersteller
– Anwendbarkeit **2** 50
– Definition **2** 49
– Freigabeanspruch **5** 48
– IT-Sicherheitsanforderung **5** 58
– Konformitätsbewertungsverfahren **5** 45
– Plausibilitätsnachweis **5** 50
– Produktkennzeichnung **2** 49
– REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) Definition **2** 51
– Security-by-Design **3** 1
– Sicherheitsanforderung **1** 10
– Verstoß **5** 56
Herstellererklärung
– Aktualisierung **5** 55
– Mitteilungspflicht **5** 47
Hinweis, Sicherheitsinformation **5** 57
Höchstsumme
– Nachweispflicht **7** 12
– vollziehbare Anordnung **7** 12

IKT-Dienst
– Definition **1** 38
– Verarbeitung **1** 38
IKT-Dienstleister, Vertragsverpflichtung **1** 12
IKT-Produkt
– Definition **1** 41
– smarter Stromzähler **1** 41
IKT-Prozess, Definition **1** 42
Importeur **2** 45, 47
Incident Response
– Kommunikationsmanagement **3** 20
– Plan **3** 20
Informationspflicht
– Ausnahme **4** 6
– Beschränkung **5** 7
– erhebliche Cyberbedrohung **4** 6
– Sicherheitsvorfall **4** 4
Informationssicherheit
– Defizit **2** 40
– Gewährleistung **6** 6
Informationstechnik des Bundes, Informationssicherheit **3** 57
Informationstechnisches System, kritische Anlage **2** 37
Informationstechnologie-Sicherheitsmaßnahme **3** 10
Informations- und Kommunikationstechnologie (IKT)-Produkt, Zertifizierungspflicht **3** 32
Institution der Sozialen Sicherung
– bußgeldbewehrte Verpflichtungen **5** 37
– Ordnungswidrigkeit **5** 36
Integrität **1** 27
– Authentizität **1** 27
ISO/IEC 27001 **3** 11
ISO/IEC 27002 **3** 11
IT-Grundschutz, Gesetzesrang **3** 50
IT-Grundschutz-Kompendium, Fortentwicklung **3** 52
IT-Sicherheitsanforderung, Norm **5** 50
IT-Sicherheitskennzeichen **5** 41 ff.
– Änderung **5** 55
– Beschleunigung **5** 51
– dynamische Sicherheitsinformation **5** 44
– Erlöschen **5** 54, 57
– Etikett **5** 52
– Freigabe **5** 48
– Freiwilligkeit **5** 8, 41, 43
– Herstellererklärung **5** 44
– Produktkatalog **5** 42
– Produktkategorie **5** 49
– Rücknahme **5** 54
– Sterne-Skala **5** 42
– Widerruf **5** 56
– Zweck **5** 43
IT-Sicherheitsorganisation
– Kryptografie **3** 16
– Sicherheitsvorfall **3** 16
IT-Sicherheitsprodukt, Abrufpflicht **3** 56

Jahresarbeitseinheit, Definition **2** 29
Jahresbilanzsumme, Berechnung **2** 30
Jahresumsatz
– Berechnung **2** 30
– Schwelle **7** 9

Kenntniserlangung, Sicherheitsvorfall **4** 20
Kommunikationstechnik, Bund **3** 54
Kooperation, global **1** 51 ff.
Kooperationsgruppe
– Informationsaustausch **1** 52
– Orientierungshilfe **1** 53
– Risikobewertung **1** 53
– Zusammenarbeit **1** 52
Koordinierte Risikobewertung, Lieferkette **3** 28
Krankenhaus, Übergangsfrist **5** 24
Kritische Anlage **1** 19 f., 49, **3** 37
– Betreiber **1** 19, 48 ff., **2** 35
Kritische Dienstleistung **1** 49
– Sektorinkonsistenz **1** 50
Kritische Einrichtung, Pflichten **1** 11
Kritische Infrastruktur **3** 40
Kritische Komponente, Typ **4** 27

Leiter, Bundesverwaltung **6** 3
Leitungsorgan **1** 36
Lieferkette
– Risikomanagement, Sicherheit **3** 26 ff.
– Risikomanagementsystem **6** 5

Managed Security Service Provider **1** 18, 45
– Auswahl **1** 45
– Risikomanagement **1** 45
Managed Service Provider (MSP)
– Definition **1** 43
– eigenständige Rechtspersönlichkeit **1** 44
– Verantwortung **1** 43
Maßnahme/Maßstab *siehe* Risikomanagement
Mehrspartenunternehmen, Nebentätigkeit **2** 36
Meldepflicht **4** 1 ff.
– Abschlussmeldung **4** 11, 17
– Auslöser **4** 14
– Ausnahme **4** 23
– Bestätigung **4** 15 f.
– dreistufiges Melderegime **1** 2
– (erheblicher) Sicherheitsvorfall **4** 2 f.
– freiwillige Meldung **2** 33
– Frist **4** 12
– frühe Erstmeldung **4** 11
– Verdachtfall **4** 12
– Zwischenmeldung **4** 16
Meldeprozess, Mustermeldung **4** 22
Melderegime, dreistufig **4** 8
Meldestelle **4** 9
Meldeverfahren, Ausgestaltung **4** 10
Meldung, Inhalt/Konkretisierung **4** 10
Mindestmaßnahme *siehe* Risikomanagement
Mitarbeiter, Schwellenwertberechnung **2** 29
Monopolist, kritische Dienstleistung **2** 10

Nachweispflicht, Betreiber kritischer Anlagen **3** 34
Nationale Aufsichtsbehörde, Zuständigkeit **2** 5
Nebentätigkeit, Umsatz **2** 8
Netz- und Informationssystem **1** 39
– elektronisches Kommunikationsnetz **1** 39
Niederlassungsprinzip, räumlicher Anwendungsbereich **5** 10

One-Stop-Shop **5** 14
Online-Plattform, BSI-Portal **1** 24
Ordnungswidrigkeit
– Bedeutung **7** 17
– Geldbuße **7** 2
Ordnungswidrigkeitenverfahren **5** 1
Organisation, Anforderung **2** 7

Partnerunternehmen, Datenanrechnung **2** 26
Pflicht, organspezifische **6** 12

Pflichtenkanon, sektorbezogene **2** 2
Pflichtverletzung, Unterlassen **6** 11
Phishing-Kampagne, Sensibilisierung **3** 24
Physische Sicherheit, Zugang **3** 12
Priorisierung, Risikoexposition **5** 21
Produktkategorie, pharmazeutisches Erzeugnis **2** 45
Prüfungsfrist **5** 47

Qualifizierter Vertrauensdiensteanbieter **2** 11

Räumlicher Anwendungsbereich **2** 4
Rechtsverordnung, BSIG **1** 35
Registrierung **4** 32
Registrierungspflicht **4** 25 ff.
– Änderungsmitteilung **4** 32
– Ausnahmen **4** 33
– besondere Registrierungspflicht **4** 30
– Betreiber kritischer Anlagen **4** 27
– Durchführungsbefugnis **4** 31
– Fristen **4** 26, 32
– Verfahren, Ausgestaltung **4** 39
– Verstoß **4** 28
Registrierungsverfahren, Ausgestaltung **4** 29
Resilienz **1** 11 f., 24, **3** 19, 38, **4** 11
Risikomanagement
– Anforderungen **3** 9
– Business Continuity Management (BCM) **3** 19
– Bußgeld **7** 8
– Dokumentation, Pflicht **3** 29 ff.
– Lieferkette **3** 26 ff.
– Maßnahmen **3** 1 ff., **6** 9
– Maßstab **3** 4 ff.
– Mindestmaßnahmen **3** 13 ff.
– Mindestvorgabe **3** 55
– Pflicht **4** 1
– Risikoanalyse, Bewertung **3** 17
– Risikoermittlung **3** 8
– Risikoprognose **3** 5
– Sanktionen **7** 2
– Stand der Technik **3** 10
Risikomanagementmaßnahme **3** 1 ff.; *siehe* Risikomanagement
Risikomanagementsystem, Bestandteil **6** 5
Risikoprognose **3** 5

Schaden, Rechtsfolge **1** 31
Schulung, Sensibilisierung **3** 22
Schutzziel, Verfügbarkeit **1** 22
Schwachstelle, Management **3** 26
Schwellenwert *siehe auch* Cap-Size-Rule)
– Berechnung **2** 24 ff.
– Kriterium **2** 3, 27
Security-by-Design **3** 1
Sektor/Sektoren **2** 18 ff.
– chemische Stoffe **2** 47 ff.
– digitale Infrastruktur **2** 52 ff.
– Energie **2** 18, 34 ff., 43 ff.
– Finanzwesen **2** 32 f.
– Gesundheitswesen und digitale Infrastruktur **2** 28
– Siedlungsabfallentsorgung **1** 50
– Telekommunikation **2** 34 ff.
– Telematik **2** 32 f.
– Verarbeitendes Gewerbe/Herstellung von Waren **2** 49 ff.
Sensibilisierungsmaßnahmen **3** 23
Sicherheitslücke, intransparente Offenhaltung **3** 58
Sicherheitsniveau, erhöhtes **3** 38
Sicherheitsvorfall **3** 5, **4** 1 ff.; *siehe auch* Meldepflicht
– Betriebsstörung **1** 33
– Definition **1** 32
– erheblicher **1** 33
– Kriterien **1** 34
Signalübertragung **1** 40
Soziale Sicherung, Institution **2** 39
Spezialgesetz, Pflicht **2** 31
Stand der Technik **3** 5, 9 f.
– B3S **3** 43 ff.
– Definition **3** 10
– Grundschutz **3** 52
Supply-Chain-Angriff **3** 27

Tochtergesellschaft, Weisungsbindung **7** 15

Übergangsfrist, Krankenhaus ***5*** 24
Übertragungssystem, Signalübertragung **1** 40
Umsetzung, europarechtswidrige **1** 14
Umsetzungsanordnung ***5*** 25
– Gefahr im Verzug ***5*** 25
Unabhängige Partnerschaft KRITIS (UP KRITIS), Branchenarbeitskreise **3** 43
Unionsrechtswidrigkeit, Legislative **1** 15
Unternehmen
– Begriff **7** 14 ff.
– Einzelunternehmen **2** 25
– Geldbuße **7** 16
– Partnerunternehmen **2** 25
– wirtschaftliche Einheit **7** 15
Unternehmensgruppe, globaler Umsatz **7** 16
Unterrichtung
– Formfreiheit **4** 5
– Website **4** 5
Unterrichtungspflicht
– Abwehrmaßnahmen ***5*** 29
– Bedrohungsart ***5*** 29
– Meldepflicht **3** 58
Untersagungsbefugnis, vorübergehende ***5*** 32
Unterstützung, Beratung **4** 9

Verarbeitung personenbezogener Daten
– Informationspflichten, Beschränlung ***5*** 7
– Rechtmäßigkeit ***5*** 6
Verdacht, Schwelle (keine) **4** 14
Verfügbarkeit
– Fehlertoleranz **1** 26
– Redundanz **1** 26
Verhältnismäßigkeit ***5*** 34
Vernachlässigbare Tätigkeit **2** 44
Verordnung, IT-Sicherheitskennzeichen (BSI-ITSiKV) ***5*** 45
Versicherung, Ausschlussklausel ***6*** 14
Versorgungssicherheit, angemessene **3** 39
Vertragssteuerung, Dienstleister **4** 22
Vertragsverletzungsverfahren **1** 15
– EU **1** 3
Vertrauensdiensteanbieter, (nicht) qualifizierter **2** 11, 20
Vertraulichkeit, unbefugte Einsicht **1** 28
Vertreter
– Benennungspflicht **3** 59, ***5*** 18
– Niederlassungsort **3** 60
Verwaltungsbehörde, örtliche Zuständigkeit **7** 18
Verwaltungsgebühr, Zeitaufwand ***5*** 51
Verwaltungszwang ***5*** 35
Vor-Ort-Kontrolle ***5*** 30

Ware, Begriff **2** 16
Waren- und Dienstleistungsverkehr, Freiheit **2** 15
Wichtige Einrichtung **2** 41 ff.
– anlassbezogene Maßnahme ***5*** 20
– Bestimmung Schwellenwerte **2** 24 ff.
– Betroffenheit **2** 19 ff.
– Einrichtungsarten **2** 19 ff.
– Kategorien **2** 19 ff.
– Mitarbeitergrenze **2** 21
– Schwellenwert **2** 9, 21 f.
Widerruf, Verfahren ***5*** 59

Zertifizierung, Cybersicherheit **3** 32 ff.
Zugriffskontrolle, Konzept **3** 22
Zuständigkeit, parallele ***5*** 11
Zwangsgeld, Höchstbetrag ***5*** 35
Zwischenmeldung, Meldepflicht **4** 16