

# NIS2 Survival Kit

Holger Reibold

# NIS-2 Survival Kit

Praxisleitfaden mit Sofortmaßnahmen, Checklisten und Vorlagen zur rechtssicheren Umsetzung

BRAIN-MEDIA.DE

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2026 Brain-Media.de

ISBN: 978-3-95444-318-5

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. St. 52c – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

# Inhaltsverzeichnis

Inhaltsverzeichnis .....	
Epilog .....	1
1 Einleitung .....	5
1.1 Ausgangslage: Warum NIS-2 verunsichert .....	6
1.2 Fehlwahrnehmungen rund um NIS-2 .....	8
1.3 Zielsetzung und Ansatz dieses Buches .....	10
2 Betrifft uns NIS-2 wirklich? .....	13
2.1 Betroffenheit falsch eingeschätzt .....	15
2.2 „Wichtig“ und „besonders wichtig“ .....	16
2.3 Die Rolle der Lieferkette .....	20
2.4 Typische Grenzfälle im Mittelstand.....	21
2.5 Entscheidungslogik zur Betroffenheit .....	23
2.6 Ergebnisinterpretation.....	24
2.7 Was NIS-2 nicht verlangt.....	25
3 Haftung und Verantwortung einordnen .....	29
3.1 Geschäftsführungshaftung .....	31
3.2 Organisationspflichten .....	32
3.3 Geschäftsführerhaftung herausarbeiten.....	34

3.4	Rollenklärung .....	36
3.5	Warum Verantwortung nicht delegierbar ist.....	38
3.6	Die Rolle der IT-Leitung im NIS-2-Kontext .....	39
3.7	Dokumentation als Schutz .....	41
3.8	Haftungsrelevante Fehlannahmen .....	43
3.9	Fallbeispiel 1: Produktion .....	44
4	Zehn Pflichten im Überblick .....	47
4.1	Warum Priorisierung entscheidend ist .....	48
4.2	Risikoanalyse.....	50
4.3	Vorfallsmanagement und Meldebereitschaft.....	52
4.4	Business Continuity .....	53
4.5	Backup als Voraussetzung, nicht als Lösung .....	55
4.6	Grundlegende Schutzmaßnahmen .....	56
4.7	Lieferkettensicherheit in der Praxis.....	58
4.8	Schulung und Sensibilisierung.....	59
4.9	Überwachung und Überprüfung .....	61
4.10	Nachweisführung und Dokumentation .....	62
5	Risikoanalyse ohne ISO-Theater .....	65
5.1	Warum klassische Risikomodelle scheitern .....	66
5.2	Kritische Assets identifizieren.....	68
5.3	Verfügbarkeit und Wiederherstellbarkeit.....	70

5.4	Umgang mit Unsicherheiten und Annahmen .....	71
5.5	Pragmatisches Risikokurzprofil.....	73
5.6	Nutzung und Pflege der Risikoübersicht .....	74
6	Incident Response und Meldepflichten .....	77
6.1	Was als Sicherheitsvorfall gilt – und was nicht.....	78
6.2	Incident-Meldewesen konkretisieren .....	80
6.3	Meldepflichten verständlich eingeordnet.....	82
6.4	Zeitliche Anforderungen und ihre Bedeutung .....	83
6.5	Rollen und Zuständigkeiten im Ernstfall.....	85
6.6	Kommunikation nach innen und außen .....	86
6.7	Typische Fehler im Incident Handling .....	88
6.8	Vorbereitung ohne 24/7-Betrieb .....	89
6.9	Fallbeispiel 2: Gesundheitswesen .....	91
7	Lieferkette und Dienstleister bewerten .....	93
7.1	Lieferkette als Kernpunkt von NIS-2.....	94
7.2	Welche Anforderungen realistisch sind.....	96
7.3	Mindestanforderungen an Dienstleister .....	97
7.4	Fragebögen als Steuerungsinstrument .....	99
7.5	Bewertung und Priorisierung von Lieferanten.....	100
7.6	Abhängigkeiten und Alternativen .....	102
8	Business Continuity und Wiederanlauf.....	105

8.1	Warum Backup allein nicht ausreicht .....	106
8.2	RTO und RPO als Entscheidungsgrößen .....	108
8.3	Lieferkettensicherheit vertiefen .....	110
8.4	Wiederanlaufplanung in einfachen Schritten.....	112
8.5	Testen, Überprüfen und Nachjustieren .....	114
8.6	Typische Fehlannahmen in der Praxis .....	115
8.7	Fallbeispiel 3: IT-Dienstleister .....	116
9	Netzwerkhygiene und Sicherheitsarchitektur.....	119
9.1	Warum flache Netze problematisch sind.....	120
9.2	Segmentierung .....	122
9.3	Verschlüsselung mit Augenmaß .....	123
9.4	Open-Source-Toolbox für KMU.....	125
9.5	Angriffserkennung ohne SOC-Illusionen.....	127
9.6	Technische Maßnahmen realistisch bewerten .....	129
10	Der 90-Tage-Überlebensplan .....	131
10.1	Phase 1 – Klärung und Einordnung .....	132
10.2	Phase 2 – Maßnahmen und Nachweise .....	135
10.3	Phase 3 – Tests und Lückenschluss .....	138
10.4	Übergang in den Regelbetrieb .....	141
10.5	Kosten- und Aufwandsabschätzung .....	142
	Epilog .....	145

NIS-2 als dauerhafte Aufgabe .....	146
Warum „fertig“ kein Ziel ist .....	148
Ruhe durch Struktur und Klarheit .....	149
Einordnung von NIS-2 in Resilienz und Governance .....	151
Anhang.....	VII
Entscheidungsbaum zur Betroffenheit .....	VIII
Governance-Minimalmodell.....	IX
Risikokurzprofil .....	XIII
Incident-Meldecheckliste .....	XIII
Lieferantenminimalanforderungen .....	XVII
Audit-Readiness-Check .....	XX
90-Tage-Plan .....	XXIV
Literatur- und Quellenverzeichnis .....	XXVII
Stichwortverzeichnis .....	XXIX
Mehr von Brain-Media.de .....	XXXIII
IT-Texter.one .....	XXXVI



# Epilog

Wer sich mit der NIS-2-Richtlinie beschäftigt, sucht häufig nach einem klaren Endpunkt. Nach einem Zustand, der erreicht werden kann und anschließend Bestand hat. Diese Erwartung ist verständlich, entspricht jedoch nicht der Realität, in der NIS-2 wirksam werden soll (NIS steht übrigens für Network and Information Security). Die Richtlinie ist nicht als Projektbeschreibung konzipiert, sondern als Rahmen für einen dauerhaften Zustand organisatorischer und technischer Beherrschbarkeit. Sie verlangt keine Perfektion und auch keine vollständige Kontrolle, sondern nachvollziehbare Entscheidungen, belastbare Strukturen und die Fähigkeit, auf Störungen angemessen zu reagieren.

Damit markiert NIS-2 einen grundlegenden Perspektivwechsel. In der Vergangenheit genügte es in vielen Organisationen, Sicherheitsmaßnahmen zu implementieren und deren Existenz zu dokumentieren. Künftig rückt stärker in den Vordergrund, ob diese Maßnahmen sinnvoll eingeordnet, priorisiert und begründet werden können. Die Frage lautet nicht mehr ausschließlich, ob etwas vorhanden ist, sondern ob nachvollziehbar ist, warum es vorhanden ist und in welchem Verhältnis es zu den tatsächlichen Risiken steht.

Vor diesem Hintergrund ist die Vorstellung, NIS-2 könne „abgeschlossen“ werden, irreführend. Geschäftsmodelle verändern sich, IT-Landschaften entwickeln sich weiter, Lieferketten werden neu gestaltet und Bedrohungslagen verschieben sich kontinuierlich. Ein statischer

Zustand ist unter diesen Bedingungen weder erreichbar noch sinnvoll. Organisationen, die NIS-2 als einmaliges Umsetzungsprojekt behandeln, laufen Gefahr, umfangreiche Dokumentationen zu erzeugen, deren praktischer Nutzen im Ernstfall gering ist. Organisationen hingegen, die NIS-2 als Managementaufgabe verstehen, schaffen Strukturen, die auch unter veränderten Rahmenbedingungen tragfähig bleiben.

Dabei entsteht Sicherheit nicht durch maximale Kontrolle, sondern durch Übersicht und Klarheit. In kritischen Situationen scheitern Unternehmen selten an der Abwesenheit einzelner technischer Maßnahmen. Sie scheitern vielmehr daran, dass unklar ist, welche Systeme tatsächlich kritisch sind, wer Entscheidungen treffen darf, welche Informationen meldepflichtig sind und wie Maßnahmen priorisiert werden müssen. NIS-2 adressiert genau diese Schwächen, indem es Verantwortlichkeiten, Prozesse und Entscheidungslogiken in den Mittelpunkt rückt.

Das Ziel der Richtlinie ist es nicht, Angriffe vollständig zu verhindern. Ein solches Ziel wäre weder realistisch noch überprüfbar. Das Ziel ist es, die Handlungsfähigkeit von Organisationen zu erhöhen, wenn Störungen eintreten. Wer in der Lage ist, seine kritischen Abhängigkeiten zu benennen, Zuständigkeiten klar zuzuordnen, Risiken grob, aber zutreffend einzuschätzen und Vorfälle strukturiert zu behandeln, erfüllt den Kern der Anforderungen besser als eine Organisation mit umfangreichen, aber kaum gelebten Sicherheitskonzepten.

Langfristig wird NIS-2 dort am wenigsten als Belastung empfunden, wo es nicht isoliert betrachtet wird. Als reines Compliance-Thema erzeugt es zusätzlichen Aufwand und Widerstände. Als Bestandteil von

Resilienz, Business Continuity, Architekturentscheidungen und Lieferantensteuerung kann es hingegen ordnend wirken. Integriert in bestehende Entscheidungsprozesse unterstützt es Verantwortliche dabei, begründete Prioritäten zu setzen und Unsicherheiten zu reduzieren.

Dieses Buch hat bewusst darauf verzichtet, technische Details bis in die Tiefe auszuarbeiten oder vollständige Sicherheitsarchitekturen zu entwerfen. Ein solcher Anspruch würde der Vielfalt realer IT-Landschaften und organisatorischer Rahmenbedingungen nicht gerecht. Stattdessen lag der Fokus darauf, Orientierung zu geben, Mindestanforderungen einzuordnen und eine pragmatische Entscheidungsgrundlage zu schaffen. Ziel war es, zu zeigen, was ausreichend ist, wo Übertreibung beginnt und wie begrenzte Ressourcen sinnvoll eingesetzt werden können.

NIS-2 wird in den kommenden Jahren nicht verschwinden. Neue regulatorische Anforderungen werden hinzukommen, bestehende werden konkretisiert oder verschärft. Organisationen, die heute lernen, strukturiert und sachlich mit diesen Anforderungen umzugehen, werden auch künftig handlungsfähig bleiben. Nicht, weil sie alle Risiken kontrollieren, sondern weil sie wissen, welche Risiken sie kontrollieren müssen und wie sie ihre Entscheidungen begründen können.

In diesem Sinne ist NIS-2 weniger eine Bedrohung als eine Einladung, Verantwortung klarer zu definieren und IT-Sicherheit als das zu behandeln, was sie in Wirklichkeit ist: eine kontinuierliche Führungs- und Organisationsaufgabe.



# 1 Einleitung

Die Auseinandersetzung mit NIS-2 beginnt in vielen Unternehmen nicht aus eigenem Antrieb, sondern als Reaktion auf äußeren Druck. Kunden fragen nach Nachweisen, Dienstleister stellen Anforderungen weiter, Aufsichtsbehörden kündigen Prüfungen an. In dieser Situation entsteht häufig der Eindruck, es handle sich bei NIS-2 um eine kurzfristige regulatorische Hürde, die möglichst effizient übersprungen werden müsse. Diese Sichtweise greift zu kurz und führt in der Praxis häufig zu Fehlentscheidungen.

NIS-2 ist weniger ein neues Regelwerk als vielmehr eine Verschärfung der Erwartungshaltung gegenüber Organisationen, die in erheblichem Maße von IT abhängen oder Teil kritischer Wertschöpfungsketten sind. Die Richtlinie zwingt Unternehmen dazu, sich mit Fragen zu beschäftigen, die lange Zeit implizit geblieben sind: Welche Systeme sind tatsächlich kritisch? Welche Ausfälle wären existenzbedrohend? Wer trägt die Verantwortung, wenn Entscheidungen unter Zeitdruck getroffen werden müssen? Die Antworten auf diese Fragen lassen sich nicht aus einem Gesetzestext ablesen. Sie müssen innerhalb der Organisation erarbeitet werden.

Genau an dieser Stelle setzt dieses Buch an. Es versteht NIS-2 nicht als juristische oder technische Herausforderung, sondern als organisatorische und strategische Aufgabe. Das Ziel ist es, Orientierung zu schaffen und Entscheidern dabei zu helfen, zwischen notwendigen Maßnahmen

und überzogenen Erwartungen zu unterscheiden. Nicht alles, was im Zusammenhang mit NIS-2 diskutiert wird, ist tatsächlich gefordert. Umgekehrt gibt es Anforderungen, die unterschätzt oder verdrängt werden. Beides ist problematisch.

## 1.1 Ausgangslage: Warum NIS-2 verunsichert

Die Verunsicherung rund um NIS-2 ist kein Zufall. Sie entsteht aus dem Zusammenwirken mehrerer Faktoren, die sich gegenseitig verstärken. Zum einen ist die Richtlinie bewusst offen formuliert. Sie definiert Ziele und Anforderungen, überlässt deren konkrete Ausgestaltung jedoch den Mitgliedstaaten und letztlich den betroffenen Organisationen. Was auf regulatorischer Ebene sinnvoll ist, erzeugt auf Unternehmensebene zwangsläufig Interpretationsspielräume – und damit Unsicherheit.

Hinzu kommt, dass NIS-2 unterschiedliche Themenfelder miteinander verknüpft, die in vielen Unternehmen bislang getrennt behandelt wurden. IT-Sicherheit, Business Continuity, Risikomanagement, Lieferantesteuerung und Geschäftsführungsverantwortung werden nicht mehr isoliert betrachtet, sondern als zusammenhängendes System. Für Organisationen, in denen diese Themen historisch in verschiedenen Abteilungen verankert sind, entsteht daraus ein Koordinationsproblem. Zuständigkeiten müssen geklärt, Schnittstellen definiert und Entscheidungen abgestimmt werden. Dieser Aufwand wird häufig unterschätzt.

Ein weiterer Unsicherheitsfaktor ist die öffentliche Diskussion rund um Haftung und Sanktionen. Schlagworte wie „persönliche Haftung der

Geschäftsführung“ oder „hohe Bußgelder“ prägen die Wahrnehmung, ohne dass deren tatsächliche Bedeutung eingeordnet wird. In der Folge schwanken viele Verantwortliche zwischen Aktionismus und Verdrängung. Entweder werden vorschnell umfangreiche Maßnahmenpakete beschlossen, oder das Thema wird aufgeschoben, in der Hoffnung, nicht betroffen zu sein. Beide Reaktionen sind Ausdruck derselben Unsicherheit.

Nicht zuletzt spielt die Dynamik des Marktes eine Rolle. Rund um NIS-2 ist ein umfangreiches Beratungs- und Produktangebot entstanden, das mit unterschiedlichen Interpretationen und Lösungsversprechen arbeitet. Für Unternehmen ohne tiefgehende regulatorische Erfahrung ist es schwer zu beurteilen, welche Angebote notwendig, sinnvoll oder überzogen sind. Die Grenze zwischen tatsächlicher Anforderung und kommerziellem Interesse ist nicht immer klar erkennbar.

Diese Gemengelage führt dazu, dass NIS-2 häufig als diffuse Bedrohung wahrgenommen wird, statt als strukturierende Vorgabe. Genau hier liegt jedoch der Ansatzpunkt für einen pragmatischen Umgang. Wer die Ursachen der Verunsicherung versteht, kann beginnen, NIS-2 zu entmystifizieren und auf die eigene Organisation herunterzubrechen. Die folgenden Abschnitte bauen darauf auf, indem sie typische Fehlannahmen aufgreifen und Schritt für Schritt zu einer realistischen Einordnung führen.

## 1.2 Fehlwahrnehmungen rund um NIS-2

Ein wesentlicher Teil der Verunsicherung rund um NIS-2 entsteht durch wiederkehrende Fehlannahmen, die sich in Gesprächen, Veröffentlichungen und Projektansätzen beobachten lassen. Diese Fehlwahrnehmungen führen nicht nur zu falschen Erwartungen, sondern häufig auch zu ineffizienten oder überzogenen Maßnahmen. Eine der verbreitetsten Annahmen ist die Vorstellung, NIS-2 sei in erster Linie ein technisches Sicherheitsprogramm. In dieser Logik wird versucht, Anforderungen durch zusätzliche Tools, neue Sicherheitsprodukte oder umfangreiche technische Maßnahmen zu erfüllen. Dabei wird übersehen, dass Technik allein weder Verantwortlichkeiten klärt noch Entscheidungsfähigkeit schafft.

Eine weitere Fehlannahme besteht darin, NIS-2 mit bestehenden Normen oder Zertifizierungen gleichzusetzen. Zwar gibt es inhaltliche Überschneidungen mit etablierten Sicherheits- und Managementstandards, doch NIS-2 ist kein Zertifizierungsrahmen. Es verlangt keine formale Konformität zu einem bestimmten Standard, sondern erwartet, dass Organisationen ihre Risiken kennen und angemessen behandeln. Wer versucht, NIS-2 ausschließlich über formale Strukturen oder Zertifikate abzubilden, verfehlt häufig den Kern der Anforderungen.

Ebenfalls verbreitet ist die Annahme, dass NIS-2 vor allem große Organisationen oder klassische Betreiber kritischer Infrastrukturen betrifft. Diese Sichtweise greift zu kurz. Gerade im Mittelstand entsteht Betroffenheit häufig indirekt, etwa über Lieferketten oder durch die Rolle als Dienstleister für regulierte Unternehmen. Die pauschale Aussage „Wir

sind zu klein“ oder „Wir sind kein KRITIS-Unternehmen“ führt daher in vielen Fällen zu einer trügerischen Sicherheit.

Schließlich wird NIS-2 häufig als rein regulatorische Belastung wahrgenommen, die keinen praktischen Mehrwert bietet. Diese Perspektive verstellt den Blick darauf, dass viele der geforderten Maßnahmen ohnehin notwendig sind, um den stabilen Betrieb moderner, IT-abhängiger Organisationen sicherzustellen. Die Richtlinie zwingt dazu, implizite Annahmen explizit zu machen und Entscheidungen nachvollziehbar zu dokumentieren. Dass dies als zusätzliche Last empfunden wird, ist weniger ein Zeichen überzogener Regulierung als ein Hinweis auf bestehende strukturelle Defizite.

Diese Fehlwahrnehmungen haben eines gemeinsam: Sie verengen den Blick auf einzelne Aspekte und verhindern eine ganzheitliche Einordnung. NIS-2 ist weder ein reines Technikprojekt noch ein formales Compliance-Thema. Es ist auch kein kurzfristiger Ausnahmezustand. Wer diese Missverständnisse erkennt, kann beginnen, das Thema sachlich zu strukturieren und die tatsächlichen Anforderungen von den begleitenden Nebengeräuschen zu trennen.

Um diese Kriterien greifbar zu machen, hilft eine vereinfachte Einordnung. Die folgende Landkarte zeigt, wie sich Rolle und Wirkung kombinieren lassen und zu einer belastbaren NIS-2-Einordnung führen.

Wirkung beim Kunden (kritisch)	Direkt betroffen Externe Rolle Hohe Wirkung beim Kunden	Indirekt betroffen Teil der Lieferkette Relevanz über Kunden
Wirkung beim Kunden (gering)	Aktuell nicht betroffen Interne Rolle Geringe externe Wirkung	Graubereich Einzelfallprüfung nötig Regelmäßig neu bewerten
	Rolle: intern	Rolle: extern

**NIS-2-Landkarte zur Einordnung der Betroffenheit. Die Matrix ordnet Organisationen entlang ihrer Rolle (intern/extern) und der Wirkung beim Kunden ein und unterstützt eine nachvollziehbare Managemententscheidung.**

### 1.3 Zielsetzung und Ansatz dieses Buches

Vor diesem Hintergrund verfolgt dieses Buch eine klare Zielsetzung. Es soll nicht möglichst viele Anforderungen beschreiben, sondern dabei helfen, NIS-2 einzuordnen und handhabbar zu machen. Der Fokus liegt auf Orientierung, Priorisierung und Entscheidungsfähigkeit. Die Leser sollen nach der Lektüre in der Lage sein, realistisch einzuschätzen, welche Anforderungen für ihre Organisation relevant sind, welche

Maßnahmen notwendig sind und wo bewusst auf Übererfüllung verzichtet werden kann.

Der Ansatz des Buches ist bewusst pragmatisch. Statt idealisierte Zielbilder zu entwerfen, wird von realistischen Rahmenbedingungen ausgegangen: begrenzte Budgets, gewachsene IT-Landschaften, verteilte Zuständigkeiten und ein hoher operativer Druck. NIS-2 wird hier nicht als Anlass genommen, bestehende Strukturen grundsätzlich infrage zu stellen, sondern als Impuls, diese kritisch zu überprüfen und gezielt weiterzuentwickeln.

Ein zentrales Element dieses Ansatzes ist die Unterscheidung zwischen Pflicht und Kür. Nicht jede Maßnahme, die im Zusammenhang mit NIS-2 diskutiert wird, ist zwingend erforderlich. Umgekehrt gibt es Anforderungen, die zwar wenig sichtbar sind, aber eine hohe Wirkung entfalten. Dieses Buch legt daher besonderen Wert darauf, Mindestanforderungen klar zu benennen und typische Übertreibungen einzuordnen. Ziel ist es, Ressourcen dort einzusetzen, wo sie tatsächlich zur Risikoreduktion beitragen.

Darüber hinaus versteht sich das Buch als Arbeitsgrundlage. Die enthaltenen Checklisten, Vorlagen und Strukturvorschläge sind nicht als starre Vorgaben gedacht, sondern als Hilfsmittel, die an die jeweilige Organisation angepasst werden sollen. Sie sollen Gespräche erleichtern, Entscheidungen strukturieren und Nachweise vereinfachen. Ihre Stärke liegt nicht in formaler Vollständigkeit, sondern in ihrer praktischen Nutzbarkeit.

Schließlich richtet sich dieses Buch bewusst an Personen mit Verantwortung. Es setzt kein tiefgehendes technisches Spezialwissen voraus, nimmt die Rolle der IT jedoch ernst. Technik wird dort erläutert, wo sie für Entscheidungen relevant ist, nicht dort, wo Detailwissen keinen Mehrwert bietet. Der Leser soll nicht lernen, wie einzelne Sicherheitsmaßnahmen umgesetzt werden, sondern wie deren Notwendigkeit bewertet wird.

Mit dieser Zielsetzung bildet die Einleitung den Rahmen für alle folgenden Kapitel. Bevor konkrete Anforderungen, Maßnahmen und Werkzeuge betrachtet werden, ist es notwendig, die eigene Perspektive auf NIS-2 zu klären. Erst auf dieser Grundlage lässt sich beurteilen, ob eine Organisation tatsächlich betroffen ist und welche Schritte sinnvoll sind. Genau dieser Frage widmet sich das nächste Kapitel.

# Literatur- und Quellenverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2023). IT-Grundschutz-Kompendium. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (2023). Orientierungshilfe zur Umsetzung der NIS-2-Richtlinie. Bonn: BSI.

Bundesministerium des Innern und für Heimat (2024). Referentenentwurf zur Umsetzung der NIS-2-Richtlinie in deutsches Recht. Berlin.

Europäische Union (2016). Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). Amtsblatt der Europäischen Union, L 119, 1–88.

Europäische Union (2022). Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie). Amtsblatt der Europäischen Union, L 333, 80–152.

European Union Agency for Cybersecurity (2023). Guidelines on incident reporting under NIS-2. Athen: ENISA.

European Union Agency for Cybersecurity (2023). NIS-2 Directive: An overview for stakeholders. Athen: ENISA.

- International Organization for Standardization (2022). ISO/IEC 27001: Information security management systems – Requirements. Genf: ISO.
- International Organization for Standardization (2022). ISO/IEC 27005: Information security risk management. Genf: ISO.
- National Institute of Standards and Technology (2024). Cybersecurity Framework (Version 2.0). Gaithersburg, MD: NIST.
- Ruohonen, J. (2024). A Systematic Literature Review on the NIS-2 Directive. arXiv preprint arXiv:2412.08084.
- Singh, C. (2023). The european approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (NIS-2) directive 2022/2555. *International Company and Commercial Law Review*, 5, 251-261.
- Vandezande, N. (2024). Cybersecurity in the EU: How the NIS-2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, 105890.
- Wanecki, P., Jašek, R., & Drofova, I. (2023, June). The contribution of the European NIS-2 directive to the design of the cyber security model. In *2023 International Conference on Information and Digital Technologies (IDT)* (pp. 149-154). IEEE.
- Woods, D. D. (2019). The theory of graceful extensibility. *Cognitive Systems Engineering Lab*, Ohio State University.

# Stichwortverzeichnis

## A

Abhängigkeit .....	100
Anforderung .....	19
Angriffserkennung .....	124
Anwendung .....	67
Architekturentscheidung .....	3
Audit-Readiness-Check.....	XIX

## B

Backup .....	46, 54, 104
Betroffenheit.....	10, 13, VIII
Bewertung .....	99
Business Continuity .....	3, 52, 103

## C

Checkliste.....	11
-----------------	----

## D

Delegation .....	38
Dienstleister.....	95
Dienstleisterbewertung .....	97
Dokumentation.....	35, 41
DSGVO.....	90

## E

Entscheidungsbaum.....	VIII
Entscheidungslogik .....	2, 23
Ergebnisinterpretation .....	24
Erreichbarkeit.....	85

## F

Fallbeispiel .....	44, 90, 115
Fehlannahme .....	19, 42
Frist.....	82
Führung.....	3

## G

Geschäftsführung .....	30, 36
Geschäftsführungshaftung .....	31
Governance-Minimalmodell .....	IX
Grenzfall .....	22

## H

Haftung.....	30
--------------	----

## I

Incident Handling.....	87
Incident Response.....	76
Incident-Meldecheckliste.....	XIII
Incident-Meldewesen.....	79
Informationssicherheitsbeauftragter .....	37
ISO-27001 .....	26
IT-Dienstleister .....	37
IT-Grundschutz.....	26
IT-Landschaft.....	116
IT-Leitung.....	30, 36, 39
IT-Sicherheit .....	3, 6

## K

Kommunikation.....	85
Komplexität .....	19
Koordinationsproblem.....	6
Kosten.....	140
Krisenfall.....	105

## L

Leistungsperspektive .....	23
Liefer- und Leistungsketten.....	23
Lieferant.....	98
Lieferantenminimalanforderung .....	XVI
Lieferantensteuerung .....	3

XXX I Stichwortverzeichnis

Lieferkette .....	20, 92
Lieferkettensicherheit....	46, 57, 108

## M

Meldepflicht.....	77, 81
Mittelstand .....	21

## N

Nachweisführung .....	62, 73
Network and Information Security .....	1
Netzwerkhygiene .....	116
NIS-2.....	1
Norm .....	8

## O

Open Source .....	122
Organisationspflicht .....	32
Orientierungshilfe.....	17

## P

Pflichten .....	45
Priorisierung .....	47, 98
Prozesse .....	23

## R

Recovery Point Objective.....	106
-------------------------------	-----

Recovery Time Objective.....	106
Regelbetrieb .....	138
Regelwerk.....	5
Regulatorien .....	3
Resilienz.....	3
Risikoanalyse.....	46, 49, 64
Risikokurzprofil.....	72, XIII
Risikomanagement .....	6
Risikomodell.....	65
Risikoübersicht.....	74
Rolle .....	9, 84
Rollenklärung .....	36
RPO .....	106
RTO .....	106

## S

Sanktionierung.....	99
Schnittstelle.....	67
Schulung.....	46, 58
Schutzmaßnahmen.....	55
Security Operations Center .....	26
Segmentierung .....	119
Sensibilisierung .....	59
Server .....	67
Sicherheit.....	17
Sicherheitsarchitektur.....	116
Sicherheitskonzept.....	56
Sicherheitsvorfall .....	78

## T

T-Landschaft .....	1
Toolbox .....	122
Transparenz .....	57

## U

Überlebensplan .....	128
Überprüfung .....	60
Übersetzungsleistung .....	40
Überwachung .....	60
Überwachungspflicht .....	35
Umsetzung .....	18
Unsicherheit.....	6, 70

## V

Verantwortlichkeit .....	2
Verantwortung.....	29
Verfügbarkeit .....	69
Verschlüsselung .....	120
Vorfallsmanagement.....	46, 51
Vorlage .....	11

## W

Wiederanlaufplanung.....	110
Wiederherstellbarkeit .....	52, 70

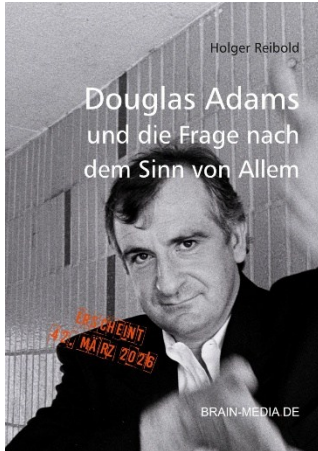
## Z

Zeitliche Anforderung..... 82

Zero-Trust ..... 117

Zertifizierung..... 8

# Mehr von Brain-Media.de



## **42 – Douglas Adams und die Frage nach dem Sinn von Allem**

Am 11 Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

Erscheint: 42. März 2026



## **Towelday, das ultimative Handtuch für alle Fans**

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



## **Code or die – Warum wir mehr Hacker brauchen**

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

Erscheint Frühjahr 2026



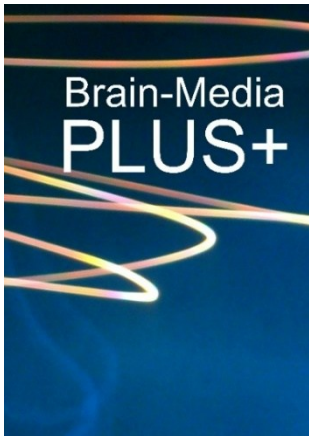
## **KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet**

Ziel- und punktgenaue Reaktionen für kritischen KI-Vorfälle.

Umfang: 140 Seiten

Preis: 16,99 EUR

Erscheint: Frühjahr 2026



**Plus+**  
– die E-Book-Flatrate –

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt Plus+ eine Renaissance.

Abonnenten erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können über 30 verfügbare E-Books herunterladen – dazu Checklisten, Vorlagen, Beispiele etc. Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die E-Books verwenden kein DRM! Auch als Team- oder Unternehmenslizenz verfügbar.

Und: Abonnenten erhalten das Handtuch zum Towelday  
im Wert von 42 EUR als **Geschenk!**

Und das alles zum **Sonderpreis** von 99 Euro!

# IT-Texter.one

100+ IT-Fachbücher

1500+ Fachartikel

30+ Erfahrung

KOMPLEXE INHALTE PUNKTGENAU AUFZUBEREITEN, IST EINE KUNST. ICH BEHERRSCHE SIE. BEI MIR ERHALTEN SIE FACH-  
TEXTE, DIE KOMPLEXES VERSTÄNDLICH MACHEN.

Seit über 30 Jahren unterstütze ich Unternehmen aus der IT-, Software- und Digitalbranche dabei, ihre technischen Inhalte klar, präzise und zielgruppenorientiert zu kommunizieren. Als promovierter Informatiker und erfahrener IT-Journalist verbinde ich fundiertes Fachwissen mit journalistischem Storytelling. Als Key Account Manager eines IT-Dienstleisters verfüge ich obendrein über konkrete Erfahrungen mit allen gängigen Technologien.

## WARUM SIE MIT MIR ARBEITEN SOLLTEN

35 Jahre Erfahrung mit Internet-,  
Netzwerk- und Webtechnologien

Kooperation mit führenden Akteuren  
der IT- und Medienbranche

Strategisches Denken: Texte, die nicht nur informieren,  
sondern auch verkaufen

THEMENSCHWERPUNKTE	WIE KANN ICH SIE UNTERSTÜTZEN?
Open-Source	Content Creation
Enterprise IT	Dokumentationen
IT-Consulting	Case Studies
SaaS	Suchmaschinenoptimierung
Künstliche Intelligenz	Tech-Marketing

### MEIN VERSPRECHEN

Ich übernehme die inhaltliche und sprachliche Brücke zwischen Technologie und Anwendung. Selbst komplexe Sachverhalte kommen beim Publikum an - fachlich korrekt, prägnant und SEO-wirksam.

### PREISMODELLE

Professionelle Leistungen, die ihresgleichen suchen, gibt es nicht umsonst. Sprechen Sie mit an. Gerne vereinbaren wir einen Fixpreis; das vereinfacht Ihre Kalkulation.

### KONTAKT AUFNEHMEN

Sprechen wir über Ihr Projekt. Schreiben Sie mir eine Mail (info@it-texter.one). Oder besser noch: Rufen Sie mich an (+49 681 91005698).