CII STUDENT PAPER SERIES

Cybersicherheit für KMU nach NIS2 – Spezifische Anforderungen an die betroffenen Branchen in Deutschland

Sebastian Knittler

CYBER|INTELLIGENCE
.Institute

Executive Summary

Die Bedrohungslage im Bereich der Cybersicherheit ist kritisch, insbesondere für kleine und mittlere Unternehmen (KMU), die oft über begrenzte Ressourcen verfügen. Mit der Einführung der NIS-2-Richtlinie weitet die EU die Sicherheitsanforderungen massiv aus und verpflichtet Unternehmen zur Umsetzung von Risikomanagementmaßnahmen nach dem dynamischen „Stand der Technik“.

Diese Masterarbeit analysiert die regulatorischen Anforderungen und deren Operationalisierung für KMU. Methodisch basiert die Untersuchung auf einer umfassenden Literaturrecherche sowie sieben qualitativen Experteninterviews, die mittels einer strukturierenden Inhaltsanalyse nach Kuckartz ausgewertet wurden. Die Ergebnisse verdeutlichen, dass ein strukturiertes Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 oder BSI IT-Grundschutz das notwendige Fundament für die Compliance bildet. Während sektorübergreifende Gemeinsamkeiten wie MFA, Patch-Management und Backups identifiziert wurden, ergeben sich branchenspezifische Unterschiede primär aus Spezialgesetzgebungen wie DORA im Finanzwesen oder dem IT-Sicherheitskatalog in der Energiewirtschaft. Die Arbeit bietet KMU durch die Aufarbeitung konkreter technischer und organisatorischer Controls eine praxisnahe Unterstützung bei der Umsetzung gesetzlicher Vorgaben. Ein zentrales Ergebnis ist die Notwendigkeit pragmatischer Dokumentationsansätze nach dem KISS-Prinzip, um die administrative Belastung beherrschbar zu halten.

Key Findings

- NIS-2 verpflichtet KMU zu Umsetzung von Maßnahmen nach dem dynamischen „Stand der Technik“.
- Ein ISMS nach ISO 27001 oder BSI IT-Grundschutz bildet das unverzichtbare Fundament der Compliance.
- Technische Maßnahmen wie MFA, Patching und Backups sind sektorübergreifend als Minimum anzusehen.
- Die persönliche Haftung der Führungsebene erfordert ein echtes, strategisches Security-Commitment.
- Sektor-Spezifika wie DORA oder EnWG erfordern individuelle Anpassungen der Sicherheitsstrategie.
- Pragmatische Dokumentation nach dem KISS-Prinzip ist entscheidend, um KMU nicht bürokratisch zu lähmen.

Über den Autor

Sebastian Knittler ist Co-Founder der Saphira Security und Research Associate am Cyberintelligence Institute.

Er verbindet Forschung mit Praxis, um KMU bei der NIS-2-Compliance und digitalen Resilienz zu unterstützen.

Abstract

Die Bedrohungslage im Bereich der Cybersicherheit in Deutschland ist unvermindert hoch, wobei besonders kleine und mittlere Unternehmen (KMU) aufgrund begrenzter personeller und finanzieller Ressourcen vor großen Herausforderungen stehen.
Mit der Einführung der NIS-2-Richtlinie weitet die Europäische Union die Sicherheitsanforderungen auf weitere Sektoren aus und verpflichtet betroffene Unternehmen zur Umsetzung von Risikomanagementmaßnahmen. Diese sollen nach dem unbestimmten Rechtsbegriff des „Stands der Technik" umgesetzt werden. Für KMU stellt dies eine erhebliche wirtschaftliche Belastung dar, da die Identifikation passender technischer und organisatorischer Maßnahmen (TOMs) zusätzlich durch die Heterogenität der branchenspezifischen Anforderungen erschwert wird.

Das Ziel dieser Masterarbeit ist es, den „Stand der Technik" für die betroffenen Branchen zu erarbeiten und sektorübergreifende Gemeinsamkeiten sowie Unterschiede bei den Risikomanagementmaßnahmen zu identifizieren. Dabei beschäftigt sich die zentrale Forschungsfrage damit, welche spezifischen Anforderungen sich für KMU aus der regulatorischen Vorgabe ergeben und wie diese operationalisiert werden können.

Methodisch basiert die Arbeit auf einer umfassenden Literaturrecherche sowie einer empirischen Untersuchung mittels sieben qualitativer Experteninterviews mit Fachleuten aus den Bereichen IT-Sicherheit und KRITIS. Die Datenauswertung erfolgt durch eine strukturierende qualitative Inhaltsanalyse nach Kuckartz.

Die Ergebnisse zeigen, dass ein strukturiertes Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 oder BSI IT-Grundschutz das notwendige Fundament für die Compliance bildet. Branchenspezifische Unterschiede ergeben sich primär aus bestehenden Spezialgesetzgebungen wie DORA oder dem EnWG sowie der unterschiedlichen Priorisierungen der Schutzziele je nach Branche. Die Arbeit bietet KMU durch die Aufarbeitung konkreter Kontrollmaßnahmen (Controls) eine praxisnahe Unterstützung bei der Umsetzung der gesetzlichen Vorgaben, welche auch die Basis für den FitNIS2-Navigator bilden.

Schlagworte

Cybersicherheit, KMU, NIS2, Stand der Technik, ISMS, Risikomanagement

Inhaltsverzeichnis

Inhalt

Abkürzungsverzeichnis

Abkürzung	Definition
KMU	Kleine und mittlere Unternehmen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG)
NIS2	Network and Information Security Directive 2
TOM	Technische und Organisatorische Maßnahmen
TM	Technische Maßnahmen
OM	Organisatorische Maßnahmen
DSGVO	Datenschutz-Grundverordnung
ISO	International Organization for Standardization
KRITISV	KRITIS-Verordnung
BCM	Business-Continuity-Management
n.F.	Neue Fassung
CSIRT	Computer Security and Incident Response Team
IoC	Indicators of compromise
TKG	Telekommunikationsgesetz
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
ICS	Industrial Control Systems
SCADA	Supervisory Control and Data Acquisition
OT	Operational Technology
B3S	Branchenspezifische Sicherheitsstandards
IKT	Informations- und Kommunikationstechnik

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Diese Masterarbeit untersucht die Auswirkungen und spezifischen Anforderungen aus der europäischen Gesetzgebung zur NIS-2-Richtlinie für KMU, mit Fokus auf den deutschen Markt. Dabei werden die betroffenen Branchen und für diese geltenden gesetzlichen Anforderungen betrachtet, die ihren Fokus auf Informationssicherheit legen. Die folgenden Unterabschnitte widmen sich zunächst der Darlegung der Problemstellung und der Definition der daraus abgeleiteten Forschungsziele. Anschließend wird die Relevanz der Thematik herausgestellt und die zugrunde liegende Motivation für die Untersuchung erläutert.

1.1.1 Problemstellung

Die Bedrohungslage im Bereich der Cybersicherheit hat sich in den letzten Jahren deutlich verschärft. Laut dem BSI-Lagebericht 2024 ist das Risiko durch Cyberangriffe in Deutschland unvermindert hoch. Insbesondere kleine und mittlere Unternehmen (KMU), die mit einem Anteil von 99,3% (vgl. statistisches Bundesamt, 2023) eine tragende Säule der deutschen Wirtschaft darstellen, stehen vor der Herausforderung, ihre Informationssysteme angemessen zu schützen. Diese KMU verfügen häufig nur über begrenzte finanzielle und personelle Ressourcen, im Vergleich zu Großunternehmen.
Mit der Einführung der NIS-2-Richtlinie verfolgt die Europäische Union das Ziel, den Cybersicherheitsstandard in allen Mitgliedsstaaten zu harmonisieren und zu erhöhen. Dabei erweitert sich nicht nur der Anwendungsbereich - von bislang vor allem KRITIS-Unternehmen auf nunmehr 18 Sektoren -, sondern auch die an betroffene Unternehmen gerichteten Sicherheitsanforderungen werden deutlich ausgeweitet. Dadurch werden auch viele Unternehmen erstmals verpflichtet, ein strukturiertes Informationssicherheits-Managementsystem (ISMS) nach dem „Stand der Technik“
einzuführen. Die Unternehmen sind verpflichtet, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen und zu dokumentieren“. Diese geforderten Maßnahmen werden in der NIS2 als Risikomanagementmaßnahmen aufgeführt und umfassen mindestens die 10 Maßnahmen laut Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555. (EUROPÄISCHES PARLAMENTS, 2022, S.172)

Für KMU stellt dies eine erhebliche organisatorische und wirtschaftliche Belastung dar.
Zudem unterscheiden sich die Anforderungen zwischen den betroffenen Branchen, etwa im Gesundheitswesen, in der Energieversorgung oder im produzierenden Gewerbe, teils erheblich. Diese Heterogenität erschwert es KMU, die für sie passenden technischen und organisatorischen Maßnahmen (TOMs) zu identifizieren und umzusetzen.

1.1.2 Problemnachweis

Eine wissenschaftliche Auseinandersetzung mit den Herausforderungen der Cybersicherheit im Kontext der NIS-2-Richtlinie findet in der Arbeit von Kipker (2024) „Auf der Suche nach dem Heiligen Gral der Cybersicherheit?“ statt. Hier werden die Implikationen der NIS-2-Richtlinie für Unternehmen untersucht und der Verfasser hebt hervor, dass der Begriff nach „Stand der Technik“ oft ungenau definiert ist. Durch diese Unschärfe des Rechts liegen auch die Chancen und Möglichkeiten in der NIS2 und der Ausarbeitung der Spezifika in den Branchen.
Die IHK München und Oberbayern hebt in ihrem Artikel "NIS-2 und Kritis: Pflichten für wichtige und besonders wichtige Unternehmen" hervor, dass die Umsetzung der NIS-2-Richtlinie Unternehmen vor erhebliche Herausforderungen stellt. Besonders die Notwendigkeit, eigenständig zu prüfen, ob das eigene Unternehmen von der Richtlinie betroffen ist, kann für viele Betriebe problematisch sein. Die IHK betont, dass Unternehmen nicht automatisch informiert werden und daher selbstständig anhand von Kriterien wie Branchensektor, Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme ihre Betroffenheit feststellen müssen. Diese Selbstverantwortung kann insbesondere für kleine und mittlere Unternehmen (KMU) eine erhebliche Belastung darstellen, da sie oft nicht über die notwendigen Ressourcen oder das Fachwissen verfügen, um solche Prüfungen eigenständig durchzuführen.
In dem Artikel „Eine Frage der Kapazität: Expertise und ihre Verfügbarkeit im Kontext von NIS-2“ von Trampnau beschreibt der Autor die fehlende Klarheit und Heterogenität der Anforderungen aus NIS2 und dass sich der Geltungsbereich erheblich erweitert hat. Des Weiteren werden pragmatische Lösungen für KMU gefordert, was gezielte Unterstützungstools wie den NIS2 Navigator, beinhalten kann. Ein solches Unterstützungstool ist der FitNIS2-Navigator (Deutschland sicher im Netz, 2025), entwickelt in Zusammenarbeit mehrerer Spezialisten unter der Leitung von „Deutschland sicher im Netz e.V. (DSIN)“. Der Navigator ist darauf ausgelegt, Unternehmen bei der Umsetzung der NIS-2-Richtlinie zu unterstützen, indem er von der Prüfung der eigenen Betroffenheit über die Erhebung des Status Quo und den daraus resultierenden Handlungsbedarfen bis hin zur Erstellung individueller Aktionspläne begleitet.

1.2 Forschungsziel

Ziel dieser Arbeit ist es, für die betroffenen Branchen den „Stand der Technik“ zu erarbeiten und welche Gemeinsamkeiten und Unterschiede für die anzuwendenden Risikomanagementmaßnahmen ergeben können. Hierbei wird zuerst ein theoretischer Überblick über die TOMs im Zusammenhang mit Cybersicherheit für KMU nach der NIS2-Richtlinie erstellt. Hierfür wird eine umfassende Recherche sowohl in wissenschaftlicher Literatur (wie Journals,

Proceedings, Dissertationen etc.), als auch in nicht-wissenschaftlicher Literatur (wie Veröffentlichungen des BSI, Bücher, Blogs, Studien, etc.) durchgeführt.

Um den aktuellen Stand der Forschung auf diesem Gebiet zu untersuchen, wird als Erstes eine Literaturanalyse durchgeführt. Anschließend werden Experten aus den betroffenen Branchen sowie allgemeinen Informationssicherheitsexperten und KRITIS-Experten interviewt, um eine qualitative Analyse der Einschätzungen und Erfahrungen für die durchzuführenden Maßnahmen zu erhalten.
Die Ergebnisse dieser Untersuchung werden genutzt, um die aktuell geltenden, sowie passenden Gesetzgebungen für die Branchen auszuwerten und als Basis für den Stand der Technik aufzuarbeiten. Die daraus resultierenden Controls sollen dann als Basis für den FITNIS2-Navigator zur Verfügung gestellt werden. Unternehmen können die für sie relevanten gesetzlichen Vorgaben sowie die daraus abgeleiteten Kontrollmaßnahmen ihrer Branche im Rahmen der NIS-2-Richtlinie als Unterstützung bei der Umsetzung nutzen.

1.3 Forschungsfragen

Zur Erreichung der im vorherigen Unterkapitel genannten Ziele sollen folgende Forschungsfragen beantwortet werden:

Cybersicherheit für KMU nach NIS2 – welche Anforderungen ergeben sich unter Berücksichtigung des ‚Stands der Technik' in den betroffenen Branchen, welche Unterschiede bestehen zwischen ihnen und welche Gemeinsamkeiten lassen sich feststellen?

1.4 Methode

Um die Forschungsfragen zu beantworten, wurde zunächst ein theoretischer Überblick über die technischen und organisatorischen Maßnahmen (TOMs) im Zusammenhang mit Cybersicherheit für kleine und mittlere Unternehmen (KMU) nach der NIS-2-Richtlinie erstellt. Hierfür wurde eine umfassende Recherche sowohl in wissenschaftlicher Literatur (wie Journals, Proceedings, Dissertationen, etc.), als auch in nicht-wissenschaftlicher Literatur (wie Veröffentlichungen des BSI, Bücher, Blogs, Studien etc.) durchgeführt. (Hagenhoff, 2007)

Im weiteren Verlauf der Arbeit erfolgte die Erkenntnisgewinnung durch empirische Forschung unter Anwendung einer qualitativen Inhaltsanalyse. Hierfür wurden ein Leitfaden und ein Fragekatalog entwickelt, die als Grundlage für Experteninterviews dienten. Anschließend wurden die Interviews mit fünf Expertinnen und Experten aus den in der Literatur identifizierten

Branchen durchgeführt, die spezifische Merkmale im Kontext kritischer Infrastrukturen aufweisen, sowie mit einer Person mit übergreifender KRITIS-Expertise. (Döring, 2023)

Ziel war es, die branchenspezifischen Unterschiede, Gemeinsamkeiten und Anforderungen im Hinblick auf den „Stand der Technik“ zu analysieren. Die Expertinnen und Experten sollten über praktische Erfahrung und fundiertes Wissen in Bereichen wie IT-Sicherheit, Risikomanagement oder der technologischen Umsetzung in kritischen Infrastrukturen verfügen. Da einige der Experten in mehreren Branchen Wissen mitbrachten, musste die Anzahl der durchgeführten Interviews nicht erhöht werden. Die Interviews wurden transkribiert und die daraus gewonnenen qualitativen Informationen im Hinblick auf die Forschungsfragen ausgewertet. (Kuckartz, 2024)
Die Methodik orientiert sich anhand der Erläuterungen zur Wissenschaftskommunikation nach Hagenhoff (2007) und zu „Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften“ nach Döring (2023) sowie zur Inhaltsanalyse nach Kuckartz (2024)

1.5 Aufbau der Arbeit

In diesem Abschnitt erfolgt eine Darstellung der Inhalte der einzelnen Kapitel.
Kapitel 2 legt die konzeptionellen Grundlagen und definiert die zentralenTerminologien dieser Masterarbeit. Darauffolgend werden die Suchstrategien und Selektionskriterien für die Literaturrecherche dargelegt.
Kapitel 3 beschreibt die angewandten methodischen Ansätze für das Forschungsvorgehen, die Realisierung der Experteninterviews sowie der Umfrage und präsentiert deren Ergebnisse.
Kapitel 4 fasst die gewonnenen Erkenntnisse zusammen und beantwortet die Forschungsfragen.
Kapitel 5 zieht Schlussfolgerungen und diskutiert offene Problematiken, die Anknüpfungspunkte für weiterführende Forschungsarbeiten bieten.

2 Grundlagen

Um ein besseres Verständnis für die NIS2 Regelung in kleinen und mittleren Unternehmen zu erlangen, werden im Folgenden die grundlegenden Konzepte und Terminologien vorgestellt. Des Weiteren wird auf den aktuellen Stand der Forschung in diesen Bereich eingegangen.

2.1 Terminologie

2.1.1 KMU

Der Begriff KMU umfasst Kleinst-unternehmen, kleine Unternehmen und mittlere Unternehmen, die sich hinsichtlich der Mitarbeiterzahl und des Jahresumsatzes von Großunternehmen abgrenzen. Das Statistische Bundesamt definiert KMU in Anlehnung an die Empfehlung (2003/361/EG) der Europäischen Kommission nach Umsatz- und Beschäftigten-größenklassen. Diese Empfehlung definiert die Größenklasse, die Anzahl der beschäftigten Personen und den Jahresumsatz, welche in Tabelle 2.1 dargestellt ist

Größenklasse	Tätige Personen	Jahresumsatz
Kleinstunternehmen	Bis 9	und bis 2 Mill. EUR
Kleine Unternehmen	Bis 49	und bis 10 Mill. EUR
Mittlere Unternehmen	Bis 249	und bis 50 Mill. EUR
Großunternehmen	Über 249	Oder über 50 Mill. EUR

Tabelle 2.1 KMU-Definition (Eigene Darstellung nach Europäischer Kommission Empfehlung 2003/361/EG)

Aufgrund der begrenzten finanzieller, sowie personeller Ressourcen verfügen KMU jedoch über eingeschränkte IT-Sicherheitsstrukturen, was ihre Verwundbarkeit gegenüber Cyberbedrohungen erhöht.

2.1.2 KRITIS

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. (*BSI KRITIS*, o. J.)
Die KRITIS Sektoren, sowie deren Beschreibung werden in Tabelle 2.2 dargestellt:

Sektor	Beschreibung (Beispiele)
Energie	Stromerzeugung und -verteilung, Gasversorgung, Mineralöl- und Kraftstoffversorgung
Informationstechnik und Telekommunikation	Bereitstellung von Internetzugang, Mobilfunknetzen, TK-Diensten, Rechenzentren
Transport und Verkehr	Luftverkehr, Schienenverkehr, Straßenverkehr, Schifffahrt, Logistik, ÖPNV
Gesundheit	Krankenhäuser, medizinische Versorgung, Arzneimittel- und Impfstoffversorgung, Labore
Wasser	Trinkwasserversorgung, Wasseraufbereitung, Verteilung und Abwasserentsorgung
Ernährung	Lebensmittelproduktion, -verarbeitung und -handel
Finanz- und Versicherungswesen	Banken, Finanzmarktinfrastrukturen, Versicherungen, gesetzliche Krankenversicherungen
Siedlungsabfallentsorgung	Sammlung, Transport, Behandlung und Beseitigung von Siedlungsabfällen
Medien und Kultur	Rundfunk (TV, Radio), gedruckte und elektronische Presse, Archive, Bibliotheken, Museen, Kulturgüter, symbolträchtige Bauwerke
Staat und Verwaltung	Parlament, Regierung und Verwaltung, Justizeinrichtungen, Notfall- und Rettungswesen

Tabelle 2.2 KRITIS-Definition (Eigene Darstellung nach BSI-KRITISV)

Die Sektoren „Medien und Kultur“ sowie „Staat und Verwaltung“ werden zwar als kritische Infrastrukturen geführt, unterliegen aber bislang nicht den spezifischen Pflichten der BSI-KRITIS-Verordnung, weshalb sie in vielen Darstellungen zu „regulierten KRITIS-Sektoren“ fehlen und in der Folge auch keine weitere Relevanz haben werden.
Die detaillierten Schwellenwerte der BSI-Kritisverordnung (BSI-KritisV) wurden in diesem Abschnitt bewusst nicht dargestellt, da sie über den terminologischen Grundlagenrahmen hinausgehen. Sie dienen primär der operativen Identifikation einzelner Anlagen und deren Klassifizierung als KRITIS-Betreiber (Anlagenkategorien I-III) und sind sektorspezifisch an Leistungs- oder Versorgungsparameter gekoppelt (BSI-KritisV, Anlagen 1–8).

Die Betreiber solcher Anlagen unterliegen besonderen Pflichten hinsichtlich der Sicherheitsstandards, Meldepflichten und beim Risikomanagement. KMU sind in diesem Zusammenhang relevant, wenn sie Teil der KRITIS-Lieferkette sind oder als Dienstleister kritische Prozesse unterstützen.

2.1.3 NIS2

Die NIS-2-Richtlinie ist die überarbeitete Fassung der ursprünglichen NIS-Richtlinie (Network and Information Security Directive) und zielt darauf ab, ein einheitlich hohes Cybersicherheitsniveau innerhalb der Europäischen Union sicherzustellen.

Sie erweitert den Anwendungsbereich erheblich und betrifft nun neben Betreibern kritischer Infrastrukturen auch viele KMU, sofern sie als „wichtige Einrichtungen“ klassifiziert werden.
Bis Oktober 2024 ist die Richtlinie in nationales Recht umzusetzen. In Deutschland geschah dies ein Jahr später durch die Verkündung des Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung 06.12.2025. Das BSI geht davon aus, dass gut 29500 Unternehmen von der neuen Regelung direkt betroffen sein werden.
Für KMU bedeutet dies, dass Cybersicherheit zunehmend zu einer gesetzlichen Verpflichtung wird und damit auch strategisch in der Unternehmensführung verankert werden muss.

2.1.4 Stand der Technik

Der Begriff des „Stand der Technik“ ist zentraler Bestandteil der Risikomanagement-Maßnahmen in der NIS2. In der deutschen Gesetzgebung lautet es: „Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen.“

Der Stand der Technik wird im Handbuch der Rechtsförmlichkeit des Bundesjustizministeriums definiert und dort heißt es: "Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Ziels gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten - wenn dies noch nicht der Fall ist - möglichst in der Praxis mit Erfolg erprobt worden sein."
Der Stand der Technik ist somit abzugrenzen sowohl von Regeln, die auch ohne Expertenwissen für vollständige Laien sofort ersichtlich sind ("Anerkannte Regeln der Technik") als auch von höchsten Anforderungen, die nach dem Stand der Wissenschaft und Technik zwar zweckmäßig sind, sich jedoch noch nicht unbedingt in der Praxis bewährt haben. („BSI Stand der Technik“, 2025)

Laut BSI soll der Stand der Technik automatisiert und dynamisch als verifizierte digitale Plattform bereitstellen. Dies soll als zentrale, maschinenlesbare Stand der Technik Bibliothek stattfinden und sich an bestehenden Normen, wie der ISO orientieren. Eine entsprechende Pilotphase wurde 2025 abgeschlossen. (*BSI-Magazin 2025/01 Mit Sicherheit*, 2025).

2.1.5 Informationssicherheit

Informationssicherheit bezeichnet gemäß § 2 Nr. 17 BSIG den angemessenen Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Dieser Schutz erstreckt sich auf alle Formen von Daten, unabhängig von ihrer Speicherung oder Verarbeitung in informationstechnischen Systemen. Dies umfasst präventive, detektierende sowie reaktive Maßnahmen gegen unbefugten Zugriff, Manipulation oder Verlust. (BSIG, 2025)

Der Begriff grenzt sich von reiner IT-Sicherheit ab, indem er nicht-digitale Informationen wie physische Dokumente, Wissensbestände einbezieht und ein ganzheitliches Risikomanagement fordert. Informationssicherheit wird durch technische und organisatorische Maßnahmen (TOM) umgesetzt, unter Berücksichtigung rechtlicher Rahmenbedingungen.

Dabei bildet die CIA-Triade den Kern bei der Umsetzung:

- Vertraulichkeit (Confidentiality): Schutz vor unbefugtem Zugriff.
- Integrität (Integrity): Gewährleistung der Vollständigkeit und Richtigkeit.
- Verfügbarkeit (Availability): Sicherstellung des jederzeitigen Zugriffs für Berechtigte.

2.2 NIS-2-Richtlinie und rechtlicher Rahmen

Die Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie(EU)) bildet seit dem 14.12.2022 den Rahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. Diese führt zur Veränderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS). In der aktualisierten Version sollen die Maßnahmen zur Cybersicherheit für kritische und wichtige Einrichtungen, sowie Maßnahmen bei IT-Ausfällen innerhalb der EU Mitgliedstaaten harmonisiert werden, sowie Aufsichtsmechanismen für Netz- und Informationssysteme geschaffen werden. (NIS2: Einfach erklärt, 2025)

Rechtssystematisch handelt es sich bei einer EU-Richtlinie um eine Vorgabe, die von den Mitgliedsstaaten in nationales Recht umzusetzen ist. In Deutschland wurde die Richtlinie wie 2.1.3 bereits beschrieben am 06.12.2025 durch das BSIG umgesetzt. Diesen ersetzt in Deutschland

die Gesetzgebungen G 206-2 v. 14.8.2009 I 2821 (BSIG 2009). Die Pflichten im neuen BSIG sind unmittelbar verbindlich und bilden die konkrete Rechtsgrundlage für Aufsicht, Meldewege und Sanktionen in Deutschland. (Enaux & Radlanski, 2025)
Durch das neue BSIG wurde nicht nur die vorherige Gesetzgebung ersetzt, sondern auch Regelungsrahmen, der sich sehr stark auf klassische KRITIS konzentrierte, deutlich ausgeweitet. Dazu wurde in der neuen Gesetzgebung ein zweistufiges System für „wichtige“ und „besonders wichtige“ Einrichtungen eingeführt.

Das BSIG n.F. ist der horizontale Grundrahmen der Cybersicherheit. Es gilt sektorübergreifend als lex generalis, wird aber dort durch spezialgesetzliche Regelungen verdrängt, wo diese den betreffenden Bereich gleichwertig und abschließend regeln. Konkret bedeutet das: Das BSIG n.F. ist lex generalis in horizontaler Hinsicht, weil es allgemeine, sektorunabhängige Mindestanforderungen an die IT- und Cybersicherheit festlegt, etwa zu Risikomanagement, Meldepflichten und Leitungsverantwortung. Daneben existieren sektorale Vorschriften wie das TKG, das EnWG oder DORA, die als lex specialis vertikal auf einzelne Wirtschaftsbereiche zugeschnitten sind und dort spezifische oder weitergehende Sicherheitsanforderungen enthalten. Um eine Doppelregulierung zu vermeiden, ordnet das BSIG n.F. selbst an, dass bestimmte Pflichten aus dem BSIG nicht gelten, wenn für denselben Sachbereich bereits gleichwertige spezialgesetzliche Regelungen bestehen. (Enaux & Radlanski, 2025)

2.3 Zielsetzung und Inhalte der NIS2

Die Zielsetzung der NIS2 ist eine Anhebung des allgemeinen Cybersicherheitsniveaus innerhalb der EU, um schwerwiegende Störungen von kritischen Diensten und wirtschaftliche Schäden durch Cyberangriffe zu reduzieren. Dabei wird zum einen die wachsende Abhängigkeit von digitalen Diensten als auch die zunehmende Vernetzung von Lieferketten und Dienstleistern adressiert. Grundlegend lassen sich vier Zielsetzungen aus der Richtlinie unterscheiden:

1. Einführung von einem systematischen Cyber-Risikomanagement
2. Corporate Accountability, also die klare Verantwortung bei der Geschäftsführung
3. Gezielte Schulungsmaßnahmen für Führungskräfte
4. Zentrale Meldung von Sicherheitsvorfällen durch eine verschärfte und mehrstufige Meldepflicht

Zu 1.: Die Kernbereiche für die Risikomanagementmaßnahmen im Bereich der Cybersicherheit werden in der NIS2 im Artikel 21 durch einen Katalog technischer und organisatorischer Maßnahmen konkretisiert und sind von den betroffenen Einrichtungen risikobasiert und verhältnismäßig umzusetzen. Die umzusetzenden Maßnahmen sind unter 1.1 Problemstellung bereits gelistet.

Zu 2.: Die Verantwortung für die Geschäftsführung und der Durchsetzung der zu erfüllenden Maßnahmen regelt die NIS-2-Richtlinie im Artikel 32 Absatz 5 und 6. Der Artikel 32 Absatz 5 der NIS2 legt ein eskaliertes Sanktionsregime für die betroffenen Einrichtungen fest, das greift, wenn mildere Durchsetzungsmaßnahmen gemäß Absatz 4 unwirksam bleiben. Als ein solches eskaliertes Sanktionsregime versteht man Sanktionen, die nicht einheitlich oder einmalig sind, sondern gestuft und verschärfend ausgestaltet sind und sich nach Schwere, Häufigkeit oder Verhalten des Normadressaten steigern. Diese Struktur ergibt sich aus dem Absatz 5, der explizite Maßnahmen für den Fall vorsieht, wenn sich die „gemäß Absatz 4 Buchstaben a bis d und f ergriffenen Durchsetzungsmaßnahmen als unwirksam“ erweisen, also eine Eskalationsstufe zur temporären Aussetzung von Zertifizierungen oder Genehmigungen für betroffene Dienste, sowie Verbote für Führungskräfte, Leistungsaufgaben auszuüben, beschreiben. Für die Verhängung solcher vorübergehenden Aussetzungen oder Verbote muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, der Unschuldsvermutung und der Verteidigungsrechte, entsprechen. (NIS-2-Richtlinie, 2022, S.57)
Eine Ergänzung durch personalisierte Verantwortung findet im Artikel 32 Absatz 6 statt. Dort wird festgelegt, dass jede natürliche Person, die die für eine wesentliche Einrichtung verantwortlich und Entscheidungsbefugt ist, befugt ist zu gewährleisten, dass die Einrichtung die Richtlinie erfüllt und diese natürlichen Personen für Verstöße gegen Ihre Pflichten zu Gewährleistung der Einhaltung der Richtlinie haftbar gemacht werden kann. (NIS-2-Richtlinie, 2022)

Zu 3.: Die Mitgliedstaaten müssen laut Artikel 20 Absatz 2 sicherstellen, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, sowie die Einrichtungen dazu auffordern, allen Mitarbeitenden Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Zu 4.: Die verschärften Meldepflichten in der NIS-2-Richtlinie sind einer der Kernfortschritte gegenüber der Vorgängerrichtlinie und sollen vor allem der Transparenz, der schnellen

Koordination und der Risikominimierung dienen. Durch die Meldungen sollen die zentralen Stellen der EU-Mitgliedsstaaten andere Unternehmen über mögliche akute Risiken informieren und den betroffenen Unterstützung anbieten können. Dabei wurde vor allem die zeitliche und inhaltliche Komponente der Meldepflichten deutlich konkreter und strenger gefasst.

Die Meldefristen sind dabei für wesentliche und wichtige Einrichtungen wie folgt in drei Stufen definiert: (NIS-2-Richtlinie, 2022)

- Frühwarnung (Erstmeldung)
    - Frist: Unverzüglich, spätestens binnen 24 Stunden nach Kenntnisnahme
    - Inhalt: Notwendige Informationen zur Unterrichtung des CSIRT oder die zuständige Behörde über den Sicherheitsvorfall zu unterrichten. Die Meldung soll die meldende Einrichtung nicht von der Bearbeitung des Sicherheitsvorfalls beeinträchtigen.
- Sicherheitsvorfall (detaillierte Meldung des Sicherheitsvorfalls)
    - Frist: Unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntnisnahme
    - Inhalt: erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich der Schwere und seine Auswirkungen, sowie etwaiger Kompromittierungsindikatoren (IoC), sofern verfügbar.(Kommission, 2023)
- Abschlussbericht
    - Frist: Spätestens 1 Monat nach Meldung des Sicherheitsvorfalls
    - Inhalt:
        - eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrades und seiner Auswirkungen
        - Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat
        - Angaben zu den getroffenen und laufenden Abhilfemaßnahmen
        - gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls
    - Sonderregelung: im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts muss die betreffende Einrichtung zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls vorlegen.

2.4 Umsetzung in deutsches Recht und Relevanz für KMU

Die nationale Umsetzung erfolgte erst mit dem Inkrafttreten des novellierten BSIG im Dezember 2025, womit Deutschland die europäische Umsetzungsfrist deutlich überschritt. Dies hatte vor allem mit langen Abstimmungsverfahren der Referentenentwürfe und der vielen Stellungnahmen

der Verbände zu tun. Vor allem die Diskussionen zu der ausschließlichen Einbeziehung der Bundesministerien und des Kanzleramtes, aber nicht der nachgeordneten Behörden des Bundes und auch nicht der kommunalen Ebene, sowie dem Koalitionsbruch und der Neuwahlen der Bundesregierung 2024/2025 führten zu Verzögerungen.
Die Umsetzung im BSIG erweitert den bislang auf klassische KRITIS-Betreiber (vgl. Tabelle 2.2 KRITIS-Definition) beschränkten Regelungsrahmen erheblich.
Zur Feststellung der Betroffenheit wird im BSIG n.F. im § 28 zwischen „Besonders wichtige Einrichtungen und wichtige Einrichtungen unterschieden. Die Absätze 1 und 2 definieren dabei die Größenzuordnungen der Unternehmen:

(1) Als besonders wichtige Einrichtung gelten
    1. Betreiber kritischer Anlagen,
    2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,
    3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
        a. mindestens 50 Mitarbeiter beschäftigen oder
        b. einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen,
    4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind, und
        a. mindestens 250 Mitarbeiter beschäftigen oder
        b. einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.

(2) Als wichtige Einrichtungen gelten

1. Vertrauensdiensteanbieter,
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a. weniger als 50 Mitarbeiter beschäftigen und
   b. einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen,
3. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und die einer der in den Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und
   a. mindestens 50 Mitarbeiter beschäftigen oder
   b. einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.

Die vom BSIG n.F. betroffenen Sektoren finden sich in der Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen und Anlage 2 Sektoren wichtiger Einrichtungen, welche in Tabelle 2.4.1 und 2.4.2 in verkürzter Form ohne die Einrichtungsart dargestellt sind:

Sektor	Branche
Energie	
	Stromversorgung
	Fernwärme- oder Fernkälteversorgung
	Kraftstoff- und Heizölversorgung
	Gasversorgung
Transport und Verkehr	
	Luftverkehr
	Schienenverkehr
	Schifffahrt
	Straßenverkehr
Finanzwesen	
	Bankwesen
	Finanzmarktinfrastrukturen
Gesundheit	
Wasser	
	Trinkwasserversorgung
	Abwasserbeseitigung
Digitale Infrastruktur	
Weltraum	

Tabelle 2.4.1 Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen (Eigene Darstellung nach BSIG n.F.)

Sektor	Branche
Transport und Verkehr	
	Post- und Kurierdienste
Abfallbewirtschaftung	
Produktion, Herstellung und Handel mit chemischen Stoffen	
Produktion, Verarbeitung und Vertrieb von Lebensmitteln	
Verarbeitendes Gewerbe/Herstellung von Waren	
	Herstellung von Medizinprodukten und In-vitro-Diagnostika
	Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
	Herstellung von elektrischen Ausrüstungen
	Maschinenbau
	Herstellung von Kraftwagen und Kraftwagenteilen
	Sonstiger Fahrzeugbau
Anbieter digitaler Dienste	
Forschung	

Tabelle 2.4.2 Anlage 2

Sektoren wichtiger Einrichtungen (Eigene Darstellung nach BSIG n.F.)

Für KMU hat die Betroffenheit allerdings noch eine weitere Dimension, da viele Unternehmen Zulieferer oder Dienstleister für vom BSIG n.F. direkt betroffene Unternehmen sind.

Laut dem BSI führt diese Regelung dazu, dass für rund 29500 seit Inkrafttreten der NIS-2-Umsetzungsgesetztes am 06.12.2025 (es gelten keine Übergangsfristen) neue gesetzliche Pflichten in der IT-Sicherheit gelten. (BSI, 2026)

Da diese direkt betroffenen Unternehmen aufgrund der Risikomanagementmaßnahme § 30 Absatz 2 Nr. 4 BSIG die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern sicherstellen müssen, kann dies zu einer sogenannten „indirekten Betroffenheit“ führen. Dadurch werden direkt regulierte Unternehmen gezwungen, die Informationssicherheit ihrer Lieferanten und Dienstleister zu bewerten, steuern und regelmäßig zu überwachen.

In der deutschen Gesetzgebung werden die vier zentralen NIS2-Zielsetzungen (vgl. 2.3) mit gesetzlichen Pflichten für die betroffenen Unternehmen operationalisiert, sowie Kompetenzen des BSI in Deutschland erweitert.

Zur Erfüllung der Vorgaben des systematischen Cyber-Risikomanagements wurden die Mindestanforderungen aus dem EU-Richtlinie 2022/2555 des Europäischen Parlament im BSIG n.F. im § 30 Absatz 2 übernommen und es wurden keine weiteren Maßnahmen in der deutschen Gesetzgebung ergänzt:

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Somit sind die vom BSIG betroffenen Unternehmen verpflichtet, diese Vorgaben mit geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen umzusetzen, 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. (BSIG, 2025, S. 17)

Um die Corporate Accountability, also die klare Verantwortung bei der Geschäftsführung, sicherzustellen, werden im § 38 Absatz 1 BSIG die Geschäftsleitungen besonders wichtiger

Einrichtungen und wichtiger Einrichtungen dazu verpflichtet, die nach § 30 BSIG zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen. Im Absatz 2 wird die persönliche Haftung der Geschäftsleitung geregelt. Der Begriff der Geschäftsleitung wird hierzu im § 2 Absatz 13 BSIG geregelt: „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung. (BSIG, 2025, S. 20)
Diese natürlichen Personen, die nach dieser Definition als Geschäftsleitung definiert sind, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Dies bedeutet für die Praxis, dass die Haftung nach dem § 38 Absatz 2 BSIG n.F. bei einem schuldhaften Nichteinhalten (Vorsatz oder Fahrlässigkeit) der Aufsichtspflichten nach § 38 Absatz 1 BSIG n.F. es zu einem tatsächlichen Schaden, wie z.B. durch einen Ransomware-Angriff, Datendiebstahl, oder Ausfallzeiten führt, greift. Entscheidend für die Beurteilung ist dabei die Kausalität zwischen der Pflichtverletzung und dem Schaden. Nicht gepatchte Systeme können einen Ransomware-Angriff begünstigen, der zu Umsatzausfällen führt. Die Schadenshöhe umfasst dabei alle direkten Kosten, wie Lösegeld, oder Wiederherstellungskosten und die indirekten Verluste durch entgangene Umsätze und Reputationsschäden. Wenn dies festgestellt wurde, kann die Einrichtung Schadensersatz von der Geschäftsleitung verlangen, wofür dessen persönlichen Vermögen haftet. Dies führt zu einer massiven Verschärfung der individuellen Verantwortung für Geschäftsleitungen. (Buchholz, 2024) (Tiedtke, 2026)

Des Weiteren werden im § 38 Absatz 3 BSIG die verpflichtenden Schulungsmaßnahmen für Geschäftsleitungen geregelt: Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.
In der gesetzlichen Regelung gibt es keine weitere Definition zur Länge und zu den genauen Inhalten, sowie den anzuwendenden Schulungsmaßnahmen. Für die Definition dieser Parameter wurde vom BSI am 30.09.2025 eine Vorläufige Handreichung „NIS-2-Geschäftsleitungsschulung“ veröffentlicht. In der Handreichung schreibt das BSI: „In Anbetracht der bisher nicht erfolgten nationalen Umsetzung der NIS-2-Richtlinie kann und soll diese Handreichung keine abschließende Empfehlung für die Schulungen machen, sondern gibt das Verständnis des BSI zu den gesetzlichen Vorgaben aus § 38 Abs. 3 BSIG-E wieder.“ (BSI, 2025b, S. 5)

Da es hierzu noch keine aktualisierte Version, oder eine andere Regelung gibt, ist davon auszugehen, dass diese Inhalte aus der Handreichung als zu erfüllen gelten. Der deutsche Gesetzgeber schreibt in der Begründung zum NIS-2 Umsetzungsgesetz: "Als „regelmäßig“ im Sinne dieser Vorschrift gelten Schulungen, die mindestens alle drei Jahre angeboten werden. Für Einrichtungen der Bundesverwaltung gilt abweichend § 43 Abs. 2 BSIG-E." (Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, 2024, S. 146).
Des Weiteren ist es aber unabhängig von der gesetzlichen Definition von „regelmäßig“ als alle drei Jahre entscheidend, dass die im § 38 Absatz 1 BSIG n.F. geforderte Verantwortung der Geschäftsleitung effektiv nachgekommen wird.
Die Schulungsintervalle müssen dem Risiko angemessen sein und sich nach der Risikoexposition der Einrichtung und individuellen Fähigkeiten der Geschäftsleitungen richten, wobei gewährleistet sein muss, dass informierte Entscheidungen getroffen werden können. Mindestens aber sollen die Schulungen alle drei Jahre stattfinden.
Sinnvolle Anhaltspunkte, von diesem Mindest-Intervall abzuweichen können sein:

1. Wechsel in der Geschäftsleitung
2. Signifikante Änderungen in den Geschäftsprozessen
3. Signifikante Änderungen der Risikoexposition
4. Signifikante Änderungen bei implementierten oder geplanten Risikomanagementmaßnahmen

Zur Dauer der Schulungen macht der Gesetzgeber keine Vorgaben, geht aber in der Gesetzesbegründung von durchschnittlich halbtägigen Schulungen (vier Stunden) aus.
Die Dauer einer Schulung kann je nach Risikoexposition der Einrichtung und individuellen Fähigkeiten der Geschäftsleitungen, die vom Gesetzgeber veranschlagten vier Stunden auch deutlich überschreiten. Es ist entscheidend, dass alle geforderten Kenntnisse und Fähigkeiten sinnvoll übermittelt werden. (BSI, 2025b, S. 7)

Um diese Vorgaben zu erfüllen, ist für die betroffenen Branchen mit einem erheblichen Aufwand zu rechnen. Hierzu stellt der Gesetzgeber folgende Annahme auf: (Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), 2024, S. 106)
„Es wird geschätzt, dass jährlich rund 298 500 Geschäftsleiter Schulungen absolvieren. Dies liegt der freien Annahme zu Grunde, dass einmal im Jahr zehn leitende Beschäftigte je Unternehmen an einer solchen Schulung teilnehmen (29 850 Unternehmen * 10). Es ist jedoch davon auszugehen, dass Unternehmen aus eigenem Interesse zum Teil bereits heute ihren führenden

Mitarbeitenden Cybersicherheitsschulungen anbieten. Es wird daher angenommen, dass dies für 50 Prozent der Unternehmen zutrifft, sodass davon auszugehen ist, dass sich für rund 150 000 leitende Beschäftigte eine Veränderung des Status Quos ergibt."

Dadurch ergibts sich folgende Aufstellung:

Fallzahl	Zeitaufwand pro Fall (in Stunden)	Lohnsatz pro Stunde (in Euro)	Personalkosten (in Tsd. Euro)
150 000	4	58,40	35 040
Änderung des Erfüllungsaufwands (in Tsd. Euro)			158 940

Tabelle 2.4.3 Veränderung des jährlichen Erfüllungsaufwands (Eigene Darstellung nach Gesetzentwurf der Bundesregierung 20/13184)

Für KMU hat diese Änderung der Verantwortung für die Geschäftsleitungen, sowie die Schulungspflichten zu dieser einhergehenden Rolle eine maßgebliche Relevanz. Die zu schulenden Inhalte sind zusätzlich zu den Intervallen alle drei Jahre für vier Stunden in zwei Teile zu splitten. Der erste Teil zur Risikoanalyse (Erkennung und Bewertung), Risikomanagementmaßnahmen und zu den Auswirkungen von Risiken und Risikomanagementmaßnahmen kann theoretisch vermittelt werden. Da die Rolle der Geschäftsleitungen und des Risikomanagement sehr abstrakt und wenig greifbar sein können, sollten die theoretisch vermittelten Inhalte mit Hilfe von Beispielszenarien, interaktiven Übungen oder Fallstudien handhabbarer gemacht werden. Zusätzlich sollten Sektor- und einrichtungsspezifische Inhalte vermittelt werden. (BSI, 2025b)
In der Handreichung des BSI werden einige Beispiele für die praxisnahe Vermittlung der Inhalte mittels Leitfragen ab „3. Leitfragen für Geschäftsleitungen" angeführt. (BSI, 2025b) In einem Webinar des BSI vom 21.11.2025 wurde als weitere sinnvolle Ergänzung das „Toolkit für das Management von Cyber-Risiken" von der Allianz für Cybersicherheit empfohlen. (Blok & Nissing, 2025)
Die durchgeführten Schulungen sind vollständig zu dokumentieren, dazu zählen die Teilnehmer, Datum, Dauer, Inhalte und Trainer, intern zu archivieren und bei behördlichen Prüfungen vorzulegen. (Baldus, 2025, S. 6)

Das novellierte BSIG n.F. übernimmt die Meldefristen der NIS-2-Richtlinie nahezu identisch. Es gibt somit keine wesentlichen Unterschiede in den Fristen selbst, sondern eine direkte Übernahme des europäischen dreistufigen Modells in nationales Recht. In der Neufassung des BSIG sind die Meldefristen identisch zur NIS-2-Richtlinie strukturiert. Das BSIG stellt in der Formulierung zu der einmonatigen Frist für den Abschlussbericht explizit klar, dass die Frist nach Einreichen der 72-Stunden-Meldung beginnt.

In der alten Fassung des BSIG fungierte das BSI als zentrale Melde- und Anlaufstelle für KRITIS. In der neuen Fassung wird festgelegt, dass das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) eine zentrale Meldestelle einrichten soll. Dies soll der Harmonisierung mit dem geplanten KRITIS Dachgesetz dienen, um Synergien beim Störungsmonitoring zu nutzen.
Das Registrierungs- und Meldeportal des BSI steht den Unternehmen seit dem 16.01.2026 zur Verfügung. Für die Registrierung ist ein Elsterzertifikat und ein MUK (Mein Unternehmenskonto) notwendig. Das Portal bietet den registrierten Unternehmen die Möglichkeit der Vorfallsmeldung und bietet Informationen zu aktuellen Vorfällen.

2.5 Kritische Infrastruktur

Der Begriff der KRITIS wurde im Zuge der NIS-2-Richtlinie signifikant konzeptionell erweitert. Während die vorherige Regulierung in der Vergangenheit primär auf einer anlagenspezifischen Betrachtung lag, also der Identifizierung einzelner physischer Komponenten, rückt nun die gesamte Einrichtung (Entity) als rechtliche Einheit in den Fokus. Aufgrund moderner Infrastrukturen ist dies ein wichtiger Schritt, da diese ein Teil eines vernetzen Ökosystems sind, dessen Resilienz nur durch eine ganzheitliche Compliance sichergestellt werden kann. (Kommission, 2023)
Kritische Infrastrukturen bilden das Rückgrat moderner und hochgradig arbeitsteiliger Gesellschaften. Darunter fallen die in Tabelle 2.2 dargestellten Bereiche, deren zuverlässige Funktionsfähigkeit die Voraussetzung für staatliche und wirtschaftliche Handlungsfähigkeit, als auch die Versorgung der Bevölkerung darstellen. Somit haben diese Einrichtungen eine wichtige Bedeutung für das staatliche Gemeinwesen.

2.5.1 Definition und Abgrenzung

Eine Definition der Kritischen Infrastruktur findet sich unter § 56 Absatz 22 – 24 zu der Begriffsbestimmung von „kritische Anlage“, „kritische Komponente“ und „kritische Dienstleistung“. Betreiber solcher kritischer Anlagen, die zu der Erbringung von kritischen Dienstleistung notwendig sind, werden im § 28 Absatz 1 Satz 1 als besonders wichtige Einrichtung definiert. Um als solche zu gelten, haben bei den Betreibern von kritischen Analgen weder die Größe der Einrichtung, noch die Umsatzzahlen eine Relevanz. Hier ist rein die Definition der oben genannten Punkte relevant. Einige dieser Einrichtungen wäre rein über die klassischen Schwellenwerte schwer zu greifen, haben aber aufgrund des Betriebs einer kritischen Anlage einen entscheidenden Beitrag an der Funktion des digitalen Ökosystems. Durch diese Definition

wird „kritische Rolle“ zum zentralen Kriterium der Defintion und somit der Betroffenheit im BSIG n.F. und nicht mehr nur die physische Versorgungskapazität der Anlagen.

2.5.2 Bedeutung für die Cybersicherheit

Die besondere Bedeutung der kritischen Infrastrukturen für die Cybersicherheit resultiert aus der tiefgreifenden Vernetzung und Digitalisierung der modernen Systeme. Der Betrieb von Kritischen Anlangen, wie Energie-, Verkehrs-, Wasser, oder Gesundheitsinfrastrukturen ist, ohne die komplexen Netz- und Informationssysteme kaum noch zu gewährleisten. Die eingesetzten Steuerungs- und Leitsysteme (ICS/SCADA), sowie Kommunikationsnetze sind mit der betrieblichen IT eng miteinander verbunden und kaum noch zu trennen. Die eingesetzten OT Systeme in den Anlangen steuern und regeln viele wichtige Dienstleistungen und müssen daher gesichert werden. Forschung und Praxis legen nahe, dass technische Störungen, Naturkatastrophen, Sabotage und Cyberangriffe auf solche Infrastrukturen potenziell verheerende Auswirkungen auf die Versorgungssicherheit haben können. Die Verwundbarkeit solcher kritischen Anlagen wird daher breit in der Gesellschaft diskutiert und durch das BSIG n.F. wurden die Maßnahmen dahingehen weiter verschärft. (Schaudwet, 2026) (Atug, 2026)

Gezielte Angriffe auf solche kritischen Infrastrukturen können unterschiedliche Auswirkungen haben. Von Ransomware Angriffen auf die Krankenhaus-IT über gezielte Manipulation von Steuerungssystemen, bis hin zu DDoS – Attacken auf Telekommunikationsnetze. Illustriert die Verschränkung von physischer und digitaler Sicherheit: Krankenhäuser sind nicht nur Betreiber Kritischer Infrastrukturen, sondern in besonderem Maße von Cybervorfällen betroffen und müssen neben allgemeinen datenschutzrechtlichen Pflichten (DSGVO), sowie Branchenspezifische Sicherheitsstandards, (B3S) zusätzliche Melde- und Sicherheitsvorgaben nach BSIG erfüllen. (Teichmann, 2025)

Regulatorisch spiegelt sich die besondere Schutzbedürftigkeit in der Menge an regulatorischen Vorgaben für KRITIS Sektoren. Bereits in der ersten NIS-Richtlinie (EU) 2016/1148 wurde ein erster europäischer Rahmen geschaffen, der ein hohes Schutzniveau von Netz- und Informationssystemen für insbesondere die KRITIS Sektoren zu gewährleisten. Die neuen Vorgaben der EU werden im BSIG n.F. weiter konkretisiert. (Vogel & Ziegler, 2023)

2.6 Der „Stand der Technik“ in der Informationssicherheit

Der „Stand der Technik“ stellt das zentrale Kriterium für die Angemessenheit von den Risikomanagementaufgaben dar und ist für wichtige und besonders wichtige Unternehmen im § 30 BSlG n.F., als auch für KRITIS im § 31 BSIG n.F. verankert. Er beschreibt den Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, deren praktische Eignung zum Schutz der Funktionsfähigkeiten von IT-Systemen nach herrschender Auffassung von Fachleuten als gesichert erscheint. Maßgeblich für den „Stand der Technik“ ist der allgemein anerkannte Regelstand aus Normen und Best Practices, wobei die Maßnahmen verhältnismäßig zum Risiko und den Auswirkungen eines Ausfalls sein müssen. Die Zumutbarkeit ist somit inhärent in der gesetzlichen Verhältnismäßigkeitsprüfung verankert. Im Rahmen des IT-Sicherheitsgesetzes wird nach dessen Begründung unter „Stand der Technik“ verstanden der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. (Witt, 2018, S. 6)

Die Abbildung 2.5.1 verdeutlicht, dass der Stand der Technik neben internationalen Standards und gesetzlichen Vorschriften eine der externen Anforderungen ist, die die Compliance eines Unternehmens bestimmen. Er fungiert somit als Maßstab für die Regeltreue im Bereich der Informationssicherheit.

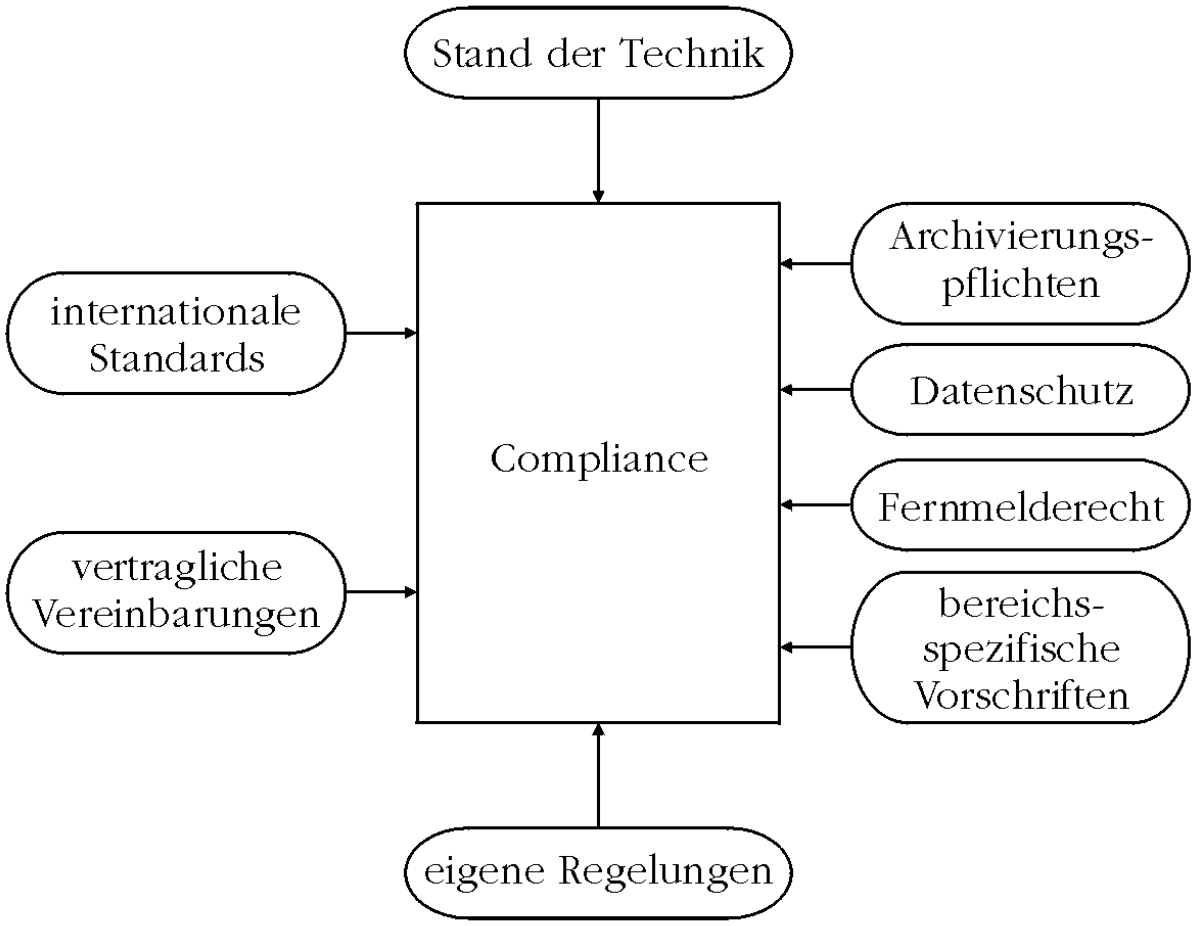

Abbildung 2.6.1 Stand der Technik und Compliance (Witt, 2018, S. 4)

Die Abbildung 2.5.2 stellt die operative Struktur und deren Dynamik des Stands der Technik dar. Der Technische Fortschritt, sowie aktuelle Vorkommnisse (z.B. politische Veränderungen (Prof. Dr. Kipker, 2025)) sind die treibenden Kräfte für Veränderungen am Stand der Technik. Diese beeinflussen das Framework für den Stand der Technik direkt und haben Auswirkungen auf dessen Veränderung. Zwischen dem „Stand des Rechts“ und dem „Technischen Fortschritt“ besteht eine Wechselwirkung. Dadurch können Änderungen im technischen Fortschritt das IT-Recht zur Anpassung zwingen und Änderungen des IT-Rechts den technischen Fortschritt beeinflussen. Der technische Fortschritt, als auch das IT-Recht stellen Forderungen und Veränderungen für den „Stand der Technik“ auf. In BSIG wird im IT-Recht gefordert, dass die TOMs (Risikomanagementmaßnahmen) dem Stand der Technik zu entsprechen haben. Dieser kann sich durch technischen Fortschritt im Laufe der Zeit weiterentwickeln. Somit ist es für betroffenen Einrichtungen essenziell die eingeführten Maßnahmen regelmäßig neu zu bewerten und bei Bedarf an den aktuellen technischen Fortschritt anzupassen. Die TOMs bilden den Kern im „Stand der Technik“. Um den Zusammenhang der Risikomanagementmaßnahmen und den

Auswirkungen dieser auf KMU in Deutschland zu vervollständigen, werden TM und OM noch weiter beleuchtet.

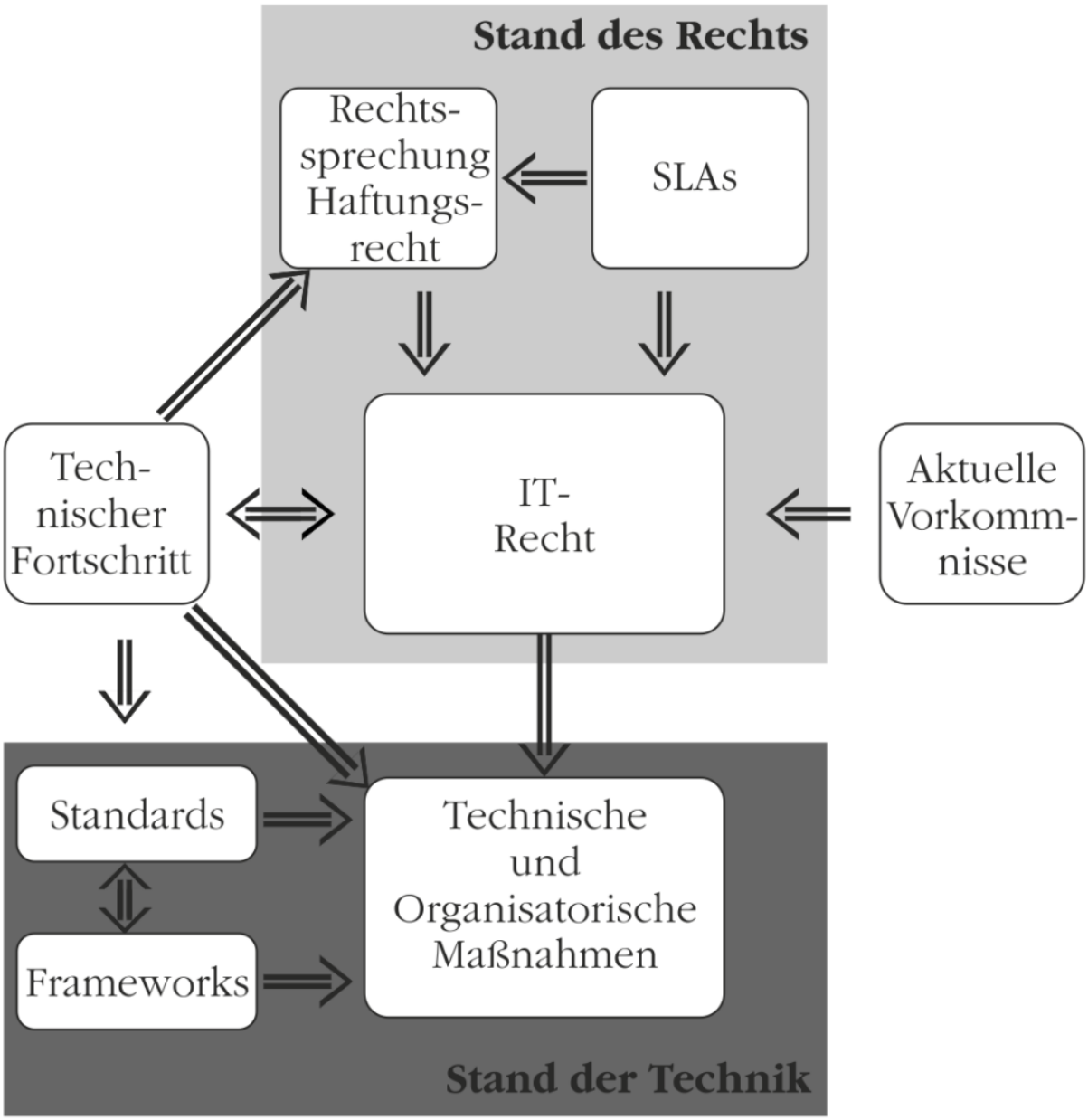

Abbildung 2.6.2 Stand der Technik und Compliance 2 (Witt, 2018, S. 5)

2.6.1 Technische Maßnahmen

Die technischen Maßnahmen (TM) umfassen die Risikomanagementmaßnahmen, die primär systemseitig, hardwarebasiert oder durch Softwarekonfigurationen realisiert werden können. Diese Maßnahmen dienen der Absicherung der IT-Systeme (Informationstechnik) und deren Komponenten, sowie Prozessen, die für die Erbringung der Dienste der vom BSIG n.F. betroffenen Branchen notwendig sind. Um die bestmögliche Leistung der technischen Schutzmaßnahmen zur

gewährleisten, müssen die Einrichtungen sich am „Stand der Technik“ orientieren. Dadurch soll die Bestleistung für die unter 2.5.1 ausgeführten Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit erreicht werden.

2.6.2 Organisatorische Maßnahmen

Die organisatorischen Maßnahmen (OM) umfassen die Rahmenbedingungen, Prozesse und Richtlinien, die das menschliche Verhalten innerhalb einer Institution betreffen. Aufgrund dieser Maßnahmen entsteht das Fundament für die Umsetzung der technischen Maßnahmen, sowie die schriftliche Dokumentation der umgesetzten Maßnahmen. Durch die organisatorischen Maßnahmen werden die technischen Maßnahmen erst wirksam und regeln die Verantwortlichkeiten, sowie den kontrollierten Ablauf innerhalb der Organisation. Da sich aufgrund dieses Zusammenspiels die Maßnahmen ergänzen, sind die geforderten Risikomanagementmaßnahmen aus dem BSIG n.F. nicht immer klar in TM, oder OM zu trennen. Grundsätzlich gilt ein Dokumentationspflicht bei allen zu erfüllenden Maßnahmen.
Zur Veranschaulichung kann man dies der Tabelle 2.5.1 entnehmen:

Nummer	BSIG § 30 Abs. 2 Maßnahme	Technische Maßnahme (TM)	Organisatorische Maßnahme (OM)
1	Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik		**X**
2	Bewältigung von Sicherheitsvorfällen		**X**
3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	**(X) Backup / Redundanz**	**(X) Strategie / Krise / Testung**
4	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern		**X**
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen	**(X) Härtung / Patches / Schwachstellen Scans**	**(X) Prozess / Erwerb**
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik		**X**
7	grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik		**X**

8	Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren	**X**	
9	Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKTSystemen, -Produkten und -Prozessen		**X**
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	**X**	

Tabelle 2.6.1

Zusammenfassung Zuordnung TOM (Eigene Darstellung nach BSIG n.F.)

X = Zuordnung, (X) = Teilweise Zuordnung

2.7 Studien

Um die Forschungsfrage beantworten zu können, wurde im Zeitraum von 01.07.2025 bis zum 28.02.2026 eine Literaturrecherche durchgeführt. Aufgrund der gesetzlichen Änderungen in diesem Zeitraum wurden die aktualisierten Gesetzgebungen bis zum Inkrafttreten des BSIG am 06.12.2026 in dieser Arbeit berücksichtigt. Um relevante Publikationen der aktuellen Forschung zu finden, wurden diverse Suchmaschinen eingesetzt. Ebenfalls wurden KI-Tools für die Suche solcher Publikationen angewendet. Die eingesetzten Suchmaschinen sind in Tabelle 2.7 aufgelistet.

Eingesetzte Suchmaschinen
Google
Google Scholar
Suchmaschine der Bibliothek der Hochschule Burgenland
Pro Quest
Notebook LM
Perplexity Pro

Tabelle 2.7.1

Eingesetzte Suchmaschinen (Eigene Darstellung)

2.7.1 Such- und Selektionskriterien

Zur Auffindung der passenden Literatur wurde nach der Auswahl der Suchmaschinen festgelegt, welche Such- und Selektionskriterien verwendet werden sollen.
Um die Suche mit Google Scholar möglichst präzise durchführen zu können, bieten Selektoren die Option, nach gewissen Dokumententypen zu suchen, oder Begriffe ein und auszuschließen. In der Tabelle 2.7.2 werden diese aufgeführt und beschrieben.

Suchparameter	Beschreibung
"Begriff"	Phrasensuche: Es werden nur Treffer angezeigt die genau die eingegebene Zeichenfolge beinhalten.
-Begriff	Ausschlusssuche: Begriffe mit vorgestelltem - werden aus der Suche ausgeschlossen.
Filetype: **Bzw.** **Ext:**	Die Suchparameter "filetype:" und „ext.“ ermöglichen die Suche nach Dokumenten in einem bestimmten Dateiformat wie pdf, doc oder pptx
Site:	Eine Suche mit dem Suchparameter "site" in Verbindung mit einer Domain oder URL liefert alle Seiten dieser Domain, die im Google-Index verfügbar sind.

Des Weitern wurde für die Präzisierung der Suche „erweiterter Modus“ in Google Scholar verwendet.
In den KI gestützten Tool wurde stehts die Modi „Deep Search“ und „Akademisch“ verwendet und manuell ausgewertet, um die bestmögliche Fachliteratur zu erhalten.
Für die orientierende Literarturrecherche fand keine zeitliche Begrenzung statt, es wurde allerdings für die Bestimmung der Branchenspezifischen Controls nur aktuell geltende Gesetzgebungen verwendet und darauf basierende Erkenntnisse nach „Stand des Rechts“ und „Stand der Technik“. Generelle geltende Definitionen für z.B. Unternehmensgrößen wurde sich auf bewährte Erkenntnisse berufen.

2.7.2 Auswahl der Literatur

Die Auswahl der Literatur erfolgte durch drei grundlegende Faktoren:

1. Relevanz der Literatur: Es wurde ausschließlich Literatur ausgewählt, die einen direkten Bezug zum Thema der Arbeit aufweist, sowie bei gesetzlichen Vorgaben dem aktuellen Stand entspricht. Besonders wurde auch der Kontext für KMU berücksichtigt, damit alle relevanten Themen abgedeckt werden.
2. Glaubwürdigkeit und Quellenqualität: Die Überprüfung der Glaubwürdigkeit und der Quellenqualität erfolgte durch eine Überprüfung der Quellen über Google Scholar oder die

Bibliothek der Hochschule. Dabei wurde analysiert, wie häufig die jeweilige Quelle zitiert wurde. Dieser Ansatz wurde in einen zeitlichen Kontext gesetzt, da ältere Literatur aufgrund ihrer historischen Relevanz oft häufiger zitiert werden kann als neuere Werke. Besonders entscheidend ist hier, dass sich aufgrund der Aktualität der Thematik ältere Quellen nicht mehr eignen. Hier wurde immer nur Referenzen auf das BSI-Gesetz in der neuen Fassung verwendet.

3. Aktualität: Es gab grundsätzlich keine zeitliche Beschränkung bei der Auswahl der Literatur. Dennoch wurde in spezifischen Bereichen, wie beispielsweise der Gesetzgebung zu NIS2, besonderer Wert auf aktuelle Quellen gelegt. Zusätzlich wurden nur aktuelle Standards für die Erstellung der Controls verwendet, da nur diese dem „Stand der Technik“ entsprechen können.

Die Literaturrecherche ergab insgesamt 49 Quellen zu den relevanten Themen, basierend auf diesen drei Faktoren. Die gefundenen Quellen wurden nach ihrer Publikationsart sortiert, darunter Bücher (einschließlich Methodenbücher), Fachzeitschriftenartikel, Konferenzbeiträge, Umfragen sowie Blog-Einträge bzw. Webseiten. Die Aufteilung kann in Tabelle 2.7.3 eingesehen werden. Der hohe Anteil an Blogs, Webseiten und Vorträge ist auf die Aktualität der Thematik zurückzuführen.

Die Publikationsarten wurden manuell in dem Open Source Programm Zotero in der Version 7.0.32 durch Analyse der Dokumente ermittelt, mit Metadaten gefüllt und anschließend manuell überprüft.

3 Methode und Vorgehen

In diesem Kapitel wird das Vorgehen und die angewandten Methoden in der Arbeit erläutert. Diese dienen als Grundlage zur Beantwortung der Forschungsfragen und werden zu Beantwortung dieser damit begründet. In den Unterkapiteln werden die ausgewählten Methoden, die Datenerhebung und -auswertung im Detail beschrieben.

3.1 Methodenwahl

Wissenschaftlichkeit erfordert nicht nur die Produktion von Erkenntnissen, sondern auch die Reflexion des Erkenntnisprozesses. Jede Studie muss daher ihr methodisches Vorgehen transparent offenlegen, Ergebnisse vorsichtig interpretieren und Limitationen, Fehlerquellen sowie offene Fragen selbstkritisch darlegen. Die Wissenschaftstheorie begründet normativ auf Metaebene das Fundament empirischer Forschung und wird durch deskriptive Disziplinen wie Wissenschaftsgeschichte bereichert. In der empirischen Sozialforschung unterscheidet man drei Paradigmen:
Quantitative Forschung: Diese verläuft linear-strukturiert von Hypothesen über repräsentative numerische Daten zur statistischen Prüfung;
Qualitative Forschung: Diese verläuft zirkulär und offen mit kleinen Stichproben sowie interpretativer Auswertung verbaler Daten zur Theorienbildung;
Mixed-Methods-Forschung: Diese verknüpft beide systematisch für komplexe Fragestellungen. Paradigmen unterscheiden sich in Realitätsvorstellungen und Forschungslogik – der Strukturierungsgrad bestimmt den Datentyp, nicht umgekehrt. (Döring, 2023, S. 32).
Aus diesem Grund wurde in dieser Arbeit ein qualitativer Forschungsansatz ausgewählt. Das Ziel dieser Arbeit besteht darin, die Auswirkungen des BSIG n.F. (NIS2) unter Berücksichtigung des „Stands der Technik" daraufhin zu bewerten, inwiefern sie kleine und mittelständische Unternehmen (KMU) in betroffenen Branchen beeinflussen, welche branchenspezifischen Unterschiede bestehen und welche Gemeinsamkeiten erkennbar sind. Zur Erreichung dieses Ziels wurden qualitative Experteninterviews mit sieben Fachpersonen aus verschiedenen NIS2-relevanten Branchen, sowie allgemeinen KRITIS Experten durchgeführt und inhaltsanalytisch ausgewertet, um vertiefte Einsichten in die praktische Auslegung, Umsetzung und Wahrnehmung der Anforderungen zu gewinnen. Dieser Ansatz ermöglicht es, komplexe Zusammenhänge zu erschließen und branchenspezifische Besonderheiten des „Stands der Technik" zu beleuchten.

3.2 Durchführung der Experteninterviews

In diesem Abschnitt wird zunächst die Zielgruppe der Interviews und das Vorgehen zur Erstellung der Interviewleitfäden eingegangen, sowie die Gegebenheiten und die Durchführung der Interviews beschrieben

3.2.1 Zielgruppe

Potenzielle Experten bzw. Fachleute können Compliance-Verantwortliche aus Unternehmen, externe Berater, die KMU bei NIS2-Compliance-Anforderungen unterstützen, oder Führungskräfte aller Karrierestufen sein, die im Bereich Cybersicherheit tätig mit dem Schwerpunkt „Informationssicherheit" verantworten. Eine langjährige Berufserfahrung ist nicht zwingend erforderlich, jedoch von Vorteil. Entscheidend ist, dass die Person zielorientiert, sachkundig, methodengeleitet und in der Lage ist, Aufgaben eigenständig zu lösen. Wenn diese Eigenschaften gegeben sind, kann sie als Experte betrachtet werden.
Die Experten für die vorliegende Arbeit wurden anhand folgender Kriterien ausgewählt:

- Fachliche Kompetenz: Umfassende Erfahrung und Fachkenntnisse im Bereich NIS2/BSIG n.F., Cybersicherheit, Compliance-Umsetzung; entweder als interne Compliance-Verantwortliche in KMU oder als externe Berater in mindestens einer oder mehreren vom BSIG n.F. betroffenen Branchen.
- Ausbildung: Mindestens eine anerkannte Ausbildung (z. B. in IT-Sicherheit, Rechtswissenschaften oder Wirtschaftsinformatik), Zertifizierung (Lead Auditor) oder eine ausreichende Berufserfahrung vorweisen kann, die zur beruflichen Qualifikation führt.
- Variabilität: Fähigkeit, sowohl objektive, datenbasierte Informationen als auch subjektive Einschätzungen aus der Praxis zu liefern; ergänzt durch einen KRITIS-Experten, der Einrichtungen kritischer Infrastruktur berät und branchenübergreifende Perspektiven einbringt.

Die einschränkenden Voraussetzungen wurden bereits vor der Einladung der Experten berücksichtigt. Falls eine eigenständige Validierung nicht möglich war, wurden die Experten in der Anfrage explizit danach gefragt.

3.2.2 Entwicklung der Interviewleitfäden

Der Prozess der qualitativen Experteninterviews in dieser Arbeit folgte den standardisierten Verfahren in zehn Schritten (Döring, 2023, S. 360 ff.)

1. Inhaltliche Vorbereitung: Es wurden das Befragungsthema „Cybersicherheit für KMU nach NIS2/BSIG n.F. unter Berücksichtigung des ‚Stands der Technik'" und die Forschungsfragen festgelegt, die Zielgruppe (Compliance-Verantwortliche, Berater, KRITIS-Experte) sowie die halbstrukturierte Interviewtechnik ausgewählt und der Leitfaden (inkl. Auftakt, Einleitfragen, Schlüsselfragen zu Branchen, Umsetzung, Tools) erprobt. Am Ende war präzise klar, welcher Experte zu welchen Branchen interviewt wird.
2. Organisatorische Vorbereitung: Eine Rollenspiel-Schulung entfiel aufgrund der umfangreichen Erfahrung der Experten. Die Rekrutierung erfolgte gezielt per E-Mail und LinkedIn mit einem Screener zu NIS2-Kompetenz, unter Berücksichtigung potenzieller Absagen durch Nachrekrutierung bis zur Sättigung. Alle Termine wurden online per Microsoft Teams vereinbart (inkl. Pufferzeiten). Das Material umfasste Teams-Funktionen (Aufzeichnung/Transkription), Einverständniserklärung, Leitfaden und Infoblatt.
3. Gesprächsbeginn: Nach digitalem Eintreffen in Teams entstand durch Smalltalk ein entspanntes Warming-up. Der Interviewer stellte sich vor, erläuterte das Untersuchungsanliegen (NIS2-Analyse für KMU), informierte umfassend zu Zweck/Dauer und holte die Zustimmung ein (Vertraulichkeit, Löschung nach Projektende). Die Teams-Aufnahme- und Transkriptionsfunktion wurde getestet und nach Zustimmung aktiviert.
4. Durchführung und Aufzeichnung: Die Hauptaufgabe war die Steuerung des Gesprächs per Teams (45–60 Min.), mit Beobachtung nonverbalen Verhaltens (via Video) und flexiblen Nachfragen aus dem Leitfaden. Bei wortkargen Experten förderte ein direkterer Stil Themenabdeckung, bei redseligen ein non direkterer Authentizität. Es musste eine Balance zwischen Eingreifen und Freiraum gewährleistet werden, um Dauer und den NIS2-Fokus zu schärfen (z. B. Branchenanforderungen oder „Stand der Technik").
5. Gesprächsende: Nach Leitfaden-Abschluss folgte ein informelles Nachgespräch (aufgezeichnet), in dem Experten oft ergänzende Praxisbeobachtungen (z. B. zu Incidents oder Produktinformationen) lieferten. Die Aufnahmebeendigung wurde explizit angekündigt, um ethische „off the record"-Konflikte zu vermeiden.
6. Verabschiedung: Übergabe von Kontaktdaten per Teams-Chat, Angebot einer anonymisierten Ergebnismitteilung (Abgabe Frühjahr 2026) und Nachbetreuung bei Fragen unter der Einhaltung der Forschungsethik.
7. Gesprächsnotizen: Unmittelbar nach dem Interview entstand ein Postskriptum mit Notizen, Expertenverhalten (via Video), technischer Qualität und situativen Details (wie Datum und Uhrzeit) zur späteren Validierung.

8. Die im Rahmen der Experteninterviews erstellten Audioaufnahmen sollten ursprünglich über die integrierte Transkriptionsfunktion von Microsoft Teams automatisch verarbeitet werden. Da dieses Verfahren jedoch keine hinreichend präzisen Ergebnisse für die weitere wissenschaftliche Analyse lieferte, wurden die Aufzeichnungen im Anschluss mit der Software F4transkript transkribiert. Dieses Vorgehen entspricht der methodischen Empfehlung von Kuckartz (2018), der F4 als spezialisiertes und bewährtes Werkzeug für die computerunterstützte Transkription qualitativer Daten hervorhebt. Da eine rein automatisierte Transkription in der Praxis selten eine Fehlerquote von 0 % erreicht, wurden die generierten Texte einer intensiven manuellen Nachbearbeitung unterzogen. Hierbei wurden verbleibende Transkriptionsfehler korrigiert, um die inhaltliche Validität für die anschließende Codierphase sicherzustellen. Im Sinne der Forschungsethik und zur Wahrung der Vertraulichkeit erfolgte während der Verschriftlichung eine konsequente Anonymisierung. Alle personenbezogenen Daten sowie spezifische Informationen zu Unternehmen wurden generalisiert oder unkenntlich gemacht, um eine DSGVO-konforme Auswertung zu gewährleisten und die Anonymität der Experten (E1–E7) zu schützen.
9. Analyse der Transkripte: Die verbalen Daten wurden mittels qualitativer Inhaltsanalyse ausgewertet und ergänzende Quantifizierungen (z. B. Häufigkeit von Themen) unterstützten die Interpretation.
10. Archivierung des Materials: Sämtliche Erzeugnisse der Interviews sind zu archivieren und vor Dritten zu schützen. Dies erfolgte durch den Einsatz von Zugangsberechtigungen und dem Einsatz von Verschlüsselung in einer eigenen Cloud Umgebung.

3.2.3 Gegebenheiten und Durchführung der Interviews

Die Durchführung der Interviews erfolgte ausschließlich online via Teams. Im Verlauf der Arbeit wurden zwischen dem 11.08.2025 und dem 05.09.2025 insgesamt sieben Experten befragt. Tabelle 3.2.3 zeigt auf, welche ID den Experten zugeordnet wurde, in welchen Branchen die Experten tätig sind, welche Berufsbezeichnung und -erfahrung sie haben und die Dauer der Interviews.

ID	Funktion	Branche	Berufserfahrung	Tatsächliche Dauer
E1	Principal	Beratung / Prüfung (KRITIS)	30 Jahre	1 Std. 15 Min.
E2	ISB / Datenschutzkoordinator	Stadtwerke (Energie & Wasser)	25 Jahre (seit 2018 in IT-Sicherheit)	1 Std. 40 Min.
E3	Teamleiter Informationssicherheit	Managed Service Provider (MSP) /	15 Jahre	45 Min.

		Beratung (ISMS-Management)		
E4	Leiter IT Security / InfoSec	Sondermaschinenbau	10 Jahre (3 Jahre in der aktuellen Rolle)	1 Std. 2 Min.
E5	IT Governance / AI Governance	Claims Management (Finanzen)	2 Jahre	1 Std. 4 Min.
E6	Geschäftsführender Gesellschafter	Beratung (ISMS-Management)	27 Jahre	52 Min.
E7	Compliance - Berater/Vorstand	Beratung (ISMS-Management)	34 Jahre	40 Min.

Tabelle 3.1 Übersicht der Experten (Eigene Darstellung)

3.2.4 Datenauswertung der Interviews und Erstellung der Sektoren-Matrix

Zur Bestimmung der Anforderung für die KMU mit der Bestimmung des „Stands der Technik" wurde die qualitative Inhaltsanalyse nach Kuckartz angewandt, um eine systematische und methodisch kontrollierte Auswertung der durchgeführten Experteninterviews (vgl. Tabelle 3.1) und der ergänzenden BSI-Leitfäden zu gewährleisten. Durch die Iteration in den fünf Phasen kann sichergestellt werden, dass keine relevanten Daten übersehen werden.

Obwohl die sieben Experteninterviews tiefgehende qualitative Einblicke ermöglichen, stellen die fehlende Repräsentativität für alle 18 Sektoren sowie der auf knapp einen Monat begrenzte Erhebungszeitraum eine methodische Limitation hinsichtlich der sektoralen Breite und zeitlichen Dynamik dar.

Die Operationalisierung fand in den folgenden fünf Phasen statt: (Kuckartz, 2022, S. 65)

1. Planungsphase: In dieser Initialen Phase wurde die Forschungsfrage beleuchtet und der Fokus auf die allgemein geltenden Standards nach BSIG n.F. und die Branchenspezifika gelegt. Dazu wurde das theoretische Vorwissen über die NIS-2-Richtlinie, das BSIG n.F. und aktuell geltende Standards der Informationssicherheit reflektiert, um die notwendige theoretische Sensibilität für die Analyse der Datenbasis, bestehend aus den sieben Experteninterviews sowie den geltenden Standards, zu schaffen.
2. Entwicklungsphase: In der zweiten Phase wurde als zentrales Analyseinstrument ein Kategoriensystem erstellt. Als Logik für die Anwendung wurde die deduktive Kategorienbildung nach Kuckartz verwendet. (Kuckartz, 2022, S. 70 ff.) Die Hauptkategorien konnten dabei direkt aus den Anhängen 1 und 2 dem theoretischen Rahmen des BSIG n.F. abgeleitet werden. Parallel dazu wurde aufgrund der Frage nach den Gemeinsamkeiten in der Forschungsfrage eine Basiskategorie geschaffen, die das informationstechnische „Grundrauschen" abbildet. In dieser Phase wurde durch den Vergleich der Experteninterviews deutlich, dass ein ISMS nach einem gültigen Standard, wie der ISO 27001, dem BSI IT-Grundschutz, oder für kleine Unternehmen (unter 50

Mitarbeitende) der DIN SPEC 27076 als Basis für die Compliance nach BSIG n.F. dient und das Fundament darstellt.

3. Testphase: Die Projektcodierung bestätigte die Eignung des definierten Kategoriensystems. Die Experten E1 – E7 erwähnten die ISO 27000-Reihe alle als anerkannten Nachweisrahmen für die Risikomanagementmaßnahmen. Die Experten E1, E2, E4, E5, E6 und E7 validierten zusätzlich den BSI IT-Grundschutz als maßgeblichen Standard zur Konkretisierung der TOMs. Die DIN SPEC 27067 wurde aufgrund der Größenbeschränkung der Unternehmen mit unter 50 Mitarbeitenden nicht weiter berücksichtigt. Diese wurde nur von den drei Experten E2, E3 und E6 erwähnt, wobei E6 den nicht vollumfänglichen Ansatz zusätzlich kritisierte. Die beiden zuerst genannten Standards wurden zusätzlich in einem Blogbeitrag des BSI als Standards für Risikoanalysen erwähnt. (BSI, o. J.-a, S. 5)
4. Codierungsphase: In der Phase der systematischen Bearbeitung wurden entlang der „Logik der Entdeckung“ die branchenspezifischen Fachstandards induktiv erschlossen. Die folgende Tabelle 3.2.1 stellt die von den Experten genannten branchenspezifischen Standards, oder in dem vom BSI bereitgestellten Informationen nach dem „Stand der Technik“ dar:

Sektor	Relevante Standards & „Stand der Technik“	Experte & Quellen
Energie	EnWG (§ 11a/5c), IT-Sicherheitskatalog (ITSIK), ISO/IEC 27019, VDE-Richtlinien, B3S Fernwärmenetze, B3S Aggregatoren.	E2, E6, BSI
Transport und Verkehr	TISAX (besonders Logistik/Automotive), Luftsicherheitsanforderungen, B3S kommunaler Straßenverkehr, B3S Bundesautobahn.	E1, E7, BSI
Finanz- und Versicherungswesen	DORA (Digital Operational Resilience Act), BaFin-Vorgaben (VAIT/BAIT), PCI DSS, B3S Allianz, B3S Electronic Cash, B3S GKV/PV.	E1, E5, E6, BSI
Gesundheit	B3S Krankenhaus, B3S Pharma, GAMP 5, GXP, Medizinproduktegesetz (MPG), B3S Laboratoriumsdiagnostik.	E1, E6, BSI
Wasser / Abwasser	B3S Wasser/Abwasser, Risikokatalog BSI Wasser.	E2, E1, BSI
Digitale Infrastruktur / IT	Cyber Resilience Act (CRA), C5 (Cloud-Katalog), ENISA-Vorgaben, NIST CSF, B3S Housing, Hosting, CDN.	E3, E6, BSI
Ernährung (Lebensmittel)	IFS (International Food Standard), HACCP, B3S Ernährungsindustrie, B3S Lebensmittelhandel.	E7, BSI
Verarbeitendes Gewerbe / Maschinenbau	IEC 62443 (OT-Sicherheit), Maschinenverordnung (MVO), CRA, AI Act, Data Act.	E4
Siedlungsabfallentsorgung	B3S Siedlungsabfallentsorgung.	BSI
Weltraum	Fokus auf Bodeninfrastruktur und weltraumgestützte Dienste (§ 2 BSIG).	BSI
Forschung	Fokus auf angewandte Forschung für kommerzielle Zwecke (Anlage 2 BSIG).	BSI

Tabelle 3.2.1 Sektorspezifische Anforderungen und Standards (Eigene Darstellung)

In der finalen Phase wurden die Ergebnisse der Matrix „Sektoren-Standard“ (Tabelle 3.2.2) zusammengeführt. Zur wissenschaftlichen Absicherung wurden die Nennungen der Experten nochmals gegen die offizielle B3S-Liste des BSI geprüft.

Branche / Sektor (gemäß BSIG/NIS2)	Allgemein geltende Standards (ISMS)	Branchenspezifika / Erwähnte Fachstandards
Energie	ISMS nach ISO 27001 oder BSI IT-Grundschutz	IT-Sicherheitskatalog (ITSIK), EnWG (§ 11a/5c), ISO/IEC 27019, B3S Fernwärmenetze, B3S Aggregatoren.
Transport und Verkehr	ISMS nach ISO 27001 oder BSI IT-Grundschutz	TISAX (Automobil/Logistik), Cyber-Luftsicherheitsanforderungen, B3S kommunaler Straßenverkehr, B3S Bundesautobahn, NIST SCF.
Finanz- und Versicherungswesen	ISMS nach ISO 27001	DORA (Digital Operational Resilience Act), BaFin-Vorgaben, B3S Allianz, B3S Electronic Cash, B3S GKV/PV.
Gesundheit	ISMS nach ISO 27001 oder BSI IT-Grundschutz	B3S Krankenhaus, B3S Pharma, B3S Laboratoriumsdiagnostik, GAMP 5, GXP, Medizinproduktegesetz (MPG).
Wasser / Abwasser	ISMS nach BSI IT-Grundschutz oder ISO 27001	B3S Wasser/Abwasser, Risikokatalog BSI Wasser.
Digitale Infrastruktur / IT	ISMS nach ISO 27001 oder BSI IT-Grundschutz	Cloud-Sicherheitskatalog C5, B3S Housing, Hosting, CDN, ENISA-Vorgaben.
Ernährung (Lebensmittel)	ISMS nach ISO 27001 oder BSI IT-Grundschutz	IFS (International Food Standard), HACCP, B3S Lebensmittelhandel, B3S Ernährungsindustrie.
Verarbeitendes Gewerbe / Maschinenbau	ISMS nach ISO 27001	IEC 62443 (OT-Sicherheit), Maschinenverordnung (MVO), Cyber Resilience Act (CRA), AI Act.
Siedlungsabfallentsorgung	ISMS nach BSI IT-Grundschutz oder ISO 27001	B3S Siedlungsabfallentsorgung.
Weltraum	ISMS nach ISO 27001	Spezifische Anforderungen an Bodeninfrastrukturen.
Forschung	ISMS nach ISO 27001 oder BSI IT-Grundschutz	Spezifische Anforderungen für Forschungseinrichtungen.

Tabelle 3.2.2 Sektorspezifische Anforderungen und Standards (Eigene Darstellung)

3.2.5 Ergebnisse der Experteninterviews

Um die Anforderungen an die von BSIG n.F. betroffenen KMU noch weiter zu schärfen, wurden die Interviews einer detaillierten Inhaltsanalyse unterzogen, um die Anforderungen an die Einrichtungen weiter zu schärfen. Dies ist entscheidend, um die spezifischen Anforderungen weiter in Controls für die Branchen zu definieren und zu operationalisieren. Dazu wurden drei Kategorien (Betroffenheit und regulatorischer Rahmen, Stand der Technik, Herausforderungen und Barrieren) festgelegt, die im Folgenden ausgewertet wurden.

3.2.5.1 Betroffenheit und regulatorischer Rahmen

Die Experten ordnen ihre Tätigkeitsbereiche einem oder mehreren Sektoren gemäß Anhang 1 und 2 zu. Die erste Hürde bei der gesetzlichen Umsetzung stellt für viele Unternehmen die Betroffenheitsprüfung dar. Die Bestimmung basiert auf den wirtschaftlichen Kennzahlen sowie den Kernbereichen des Unternehmens. E2 berichtet, dass die Nutzung von Onlinetools hier oftmals zu ungenauen Angaben führen kann und eine endgültige Prüfung somit nur mit einer Rechtsberatung zu Stande kommen kann.
Ein weiterer genannter Punkt ist die häufige Doppelregulierung. Hier betont E5, dass Finanzdienstleister sowohl von den Vorgaben des BSIG n.F. betroffen sind, als auch unter den DORA (Digital Operational Resilience Act) fallen, was bei der Compliance Umsetzung zu redundanten Aufwand führt. Ähnliches berichtet E1 für die Luftfahrtbranche, in der zum Beispiel die Luftsicherheitsgesetzgebung parallel zu der BSI-Gesetzgebung umgesetzt werden muss. E6 fasst zusammen, dass die NIS2 als übergeordneter Nachweisrahmen fungiert und dessen Umsetzung in der Praxis auf etablierte Normen wie die ISO 27001 zurückzuführen ist, was auch im Erwägungsgrund 79 der RICHTLINIE (EU) 2022/2555 (NIS-2-Richtlinie, 2022, S. 16) so verankert wurde: „Bei den Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten daher auch die physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen berücksichtigt werden, indem Maßnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen im Einklang mit europäischen und internationalen Normen, wie denen der Reihe ISO 27000, einbezogen werden.

3.2.5.2 Stand der Technik

Dieser ist im Kontext der NIS-2-Umsetzung ein zentraler, jedoch unbestimmter Rechtsbegriff. Durch die Experteninterviews konnte dieser im Kontext der Gesetzgebung sowohl theoretisch definiert als auch praktisch konkretisiert werden. Er beschreibt laut den Experten den

Entwicklungsstand fortschrittlicher Verfahren und Einrichtungen, deren praktische Eignung in Zusammenhang mit der Angemessenheit zur Absicherung von Systemen als geeignet gilt. Diese Einordnung deckt sich mit der theoretischen Einordnung aus Kapitel 2.6.

Der Usus der Experten lautet, dass ein systematisches Risikomanagement den Rahmen bildet, um den Stand der Technik für die jeweilige Einrichtung überhaupt bewerten zu können. E1 definiert diesen Ansatz pragmatisch: „Das, was in der Branche genutzt wird, ist der Stand der Technik." Es wird betont, dass der BSI IT-Grundschutz aufgrund seiner konkreten Anforderungen als „Minimum für den Stand der Technik" anzusehen ist. E3 verknüpft den Begriff unmittelbar mit der „Angemessenheit und Verhältnismäßigkeit". Er führt des Weiteren aus, dass dies nur bewertet werden kann, wenn man das Asset zuvor einer Risikobewertung unterzogen hat: „Das Wort Verhältnismäßigkeit steht ja exakt so drin in der Richtlinie auch und das kann man eigentlich nur beurteilen, wenn man halt vorher mal das Asset, was man schützen möchte, eine Risikobewertung unterzogen hat und sagt okay, das ist jetzt sehr riskant. Was wäre denn die Gegenmaßnahme, was kostet die? Und wenn das jetzt nicht im krassen Missverhältnis steht, dann würde man sagen, das wäre so okay. Das ist halt immer ein Spagat." Ein wissenschaftlicherer Ansatz wird von E5 geliefert, der erklärt: „Also wir versuchen das nicht auf den Standard zu mappen, sondern auf den aktuellen Forschungsstand. Also wir schauen uns da wirklich die Forschung an, also wir nehmen nicht die ISO 42001, weil die sehr abstrakt ist und auch sehr weit auslegbar ist. Wir nehmen das vom BSI, nehmen das von Research Papern und versuchen das alles so einzubauen." In der Praxis wird sich demzufolge auch an Research Papern orientiert, um technische Metriken präziser zu definieren, als dies abstrakte ISO-Normen erlauben.

Einige der TOMs kristallisieren sich bei Nichteinhaltung bei den Experten als besonders kritisch heraus:

MFA: Diese wird sektorübergreifend, gerade im Kontext von Fernzugriffen als absolutes Muss definiert. E6 zählt MFA zu den Maßnahmen, die „wirklich sofort jetzt und hier etwas bringen". Die Experten E1, E4, E6 und E7 sehen die Implementierung der Multi-Faktor-Authentisierung als absolutes technisches Minimum.

Aktualität und Patch-Management: E4 stellt hier klar, dass veraltete Konzepte wie einfache VPNs und manuelles Patchen nicht mehr ausreichen: „Das war Stand der Technik vor 10–15 Jahren [...] das ist kein Stand der Technik mehr". Er fordert auch ein striktes Patchen von Clients: „Clients sind bei uns mittlerweile nach 72 Stunden gepatcht, fertig".

Transparenz und Scans: E6 setzt hier auf automatisierte Schwachstellenscans, um technische Flanken wie von End-of-Life-Produkten sofort und objektiv sichtbar zu machen.

Schulung und Mitarbeitersensibilisierung: Als ein wesentlicher Teil des Stands der Technik wird die Sensibilisierung der Mitarbeitenden betrachtet. E2 und E7 machen hier den Vorschlag der „Gamification" und interaktive Ansätze. Gerade auch auf Hinblick der Verantwortung in der Geschäftsleitung wird von E1 davor gewarnt, dass gerade in den Managementetagen ein „digitales

Kompetenzdefizit“ vorherrscht. Des Weiteren warnt er davor, die Umsetzung durch überbordende Bürokratie zu lähmen, und empfiehlt das KISS-Prinzip („Keep it short and simple“) bei der Dokumentation.

Lieferkettensicherheit: Diese bleibt laut den Experten ein Schmerzpunkt bei der Umsetzung für KMU, da die Anforderungen an überforderte Unterlieferanten weitergeben müssen, was laut E5 zu einer problematischen Haftungsverschiebung führt.

Backupmanagement: Ein passendes Backupmanagement mit Wiederherstellungstests wird als Lebensversicherung der Unternehmen betrachtet. E7 sagt hierzu: „No backup no mercy ist zwar immer ganz witziger Spruch, aber es tut halt schon immer weh, wenn man sieht, dass Unternehmen vom Markt verschwinden, weil sie eben kein geeignetes Backup gehabt haben.“ Hier sollten laut den Experten in den Wiederherstellungstests auch die physische Resilienz mit betrachtet werden, zum Beispiel Notstromtests im Energiesektor, wie E2 erwähnt.

Prävention: generell mahnen die Experten zu Prävention, da diese zu enormen Ersparnissen bei der Reaktion führt. E1 sagt hier, dass „1€ in Prävention 7-9€ in der Reaktion spart.“

3.2.5.3 Herausforderungen und Barrieren

Als einer der zentralen Punkte stellte sich bei den Interviews heraus, dass die Hindernisse bei der Compliance nicht rein technischer Natur sind, sondern tief in der Unternehmenskultur, den finanziellen Ressourcen und der regulatorischen Komplexität verwurzelt sind. Als eines der zentralen Hindernisse wurde der Mangel an finanziellen und personellen Kapazitäten benannt. Dabei betonen die Experten, dass Informationssicherheit oft als unproduktiver Kostenfaktor wahrgenommen wird. E6 stellt dabei fest, dass die Einführung eines ISMS für viele KMU eine enorme administrative Belastung darstellt. Dabei können bei der erstmaligen Umsetzung der Maßnahmen enorme Kosten für KMU aufkommen. Die kurzfristige Budgetfreigabe spielt laut den Experten ebenfalls eine Rolle, da die Cybersicherheit oftmals in Konkurrenz zur Erlösmaximierung steht.

Des Weiteren wird bei den Barrieren auf die fehlende Sensibilisierung der Führungsebene hingewiesen, die dazu führt, dass es kein echtes Commitment der Geschäftsleitung gibt. E4 ergänzt hier aus der Sicht des Maschinenbaus, dass die Akzeptanz auf der technischen Leitungsebene ebenfalls fehlt: „Ingenieure betrachten IT oft als notwendiges Übel, nicht als Wurzel des Erfolgs“. Für eine erfolgreiche Umsetzung ist demnach oftmals eine Verhaltensänderung auf allen Ebenen Voraussetzung. E7 betont hier, dass diese allerdings notwendig ist, auch wenn sie als unbequem wahrgenommen wird: „Wenn die Veränderung nicht schmerzt, war es keine“.

Gerade auch am Fachkräftemangel scheitern viele Maßnahmen in der Umsetzung. KMU haben hier die Herausforderung, mit Konzernen im Wettbewerb um IT-Security-Experten zu stehen. Der Fachkräftemangel führt zudem auch zu „grauen Eminenzen“ (E4), also einzelnen Wissensträgern,

die ein Klumpenrisiko darstellen. Der Ausfall einzelner Wissensträger führt dazu, dass bei deren Ausfall Wissen zur Absicherung der Einrichtung verloren geht. Zu diesen genannten Herausforderungen werden der bürokratische Aufwand und die Lieferkettensicherheit erwähnt. Beide führen dazu, dass die Compliance Aufgaben im Unternehmen und in der gesamten Lieferkette des Unternehmens zunehmen. E5 problematisiert, dass große Unternehmen ihre Compliance-Vorgaben vertraglich an kleine Partner weitergeben, welche damit völlig überfordert sind. Als Beispiel wird hier ein kleiner Dienstleister oder Handwerksbetrieb genannt, der plötzlich komplexe Sicherheitsfragebögen erfüllen muss. E3 weist auch auf die dadurch existentiellen Folgen für das betroffenen Unternehmen hin: „Wer Compliance in der Lieferkette verschläft, verliert plötzlich 20% Umsatz“, da Kunden ohne entsprechenden Nachweis abwandern. Ein weiterer Aufwand entsteht alleine durch die Prüfung der Regulierungen wie NIS2, DORA, CRA und AI-Act. Aus diesem Grund plädieren die Experten auf einen pragmatischen Ansatz in der Dokumentation und im Nachweis. E1 erwähnt hier den KISS Ansatz bei der Dokumentation, während E7 hier erwähnt, dass z.B. Teams im Unternehmen zur Nachverfolgbarkeit dient: „Aber wir machen es immer praktisch vom Sprungpunkt Teams aus, weil das die Leute verstehen. Und so bildest du die Nachverfolgbarkeit ab: Indem du festlegst, dass ein gegebener Daumen eindeutig dir zugeordnet wird und damit als Bestätigung gilt, dass du die Information zur Kenntnis genommen hast“. Allgemein wird davor gewarnt, KMU durch überfordernde bürokratische Anforderungen handlungsunfähig zu machen. Der Fokus sollte vielmehr auf den sichereren Betrieb der Anlagen gelegt werden, statt auf der bloßen Erzeugung von „Papierkrieg“ – was die zentrale Aussage von E1 darstellt.

Es lässt sich also insgesamt feststellen, dass die größte Herausforderung in der Umsetzung der Maßnahmen darin liegt, die richtige Balance zwischen der regulatorischen Compliance und der betrieblichen Realität zu finden. Die Experten empfehlen bei Umsetzung ein unaufgeregtes Herangehen und die offensichtlichen Maßnahmen, wie oben genannt, zu beginnen. Hier wird auch empfohlen, pragmatische Einstiegslösungen zu finden, um die Barrieren schrittweise abzubauen und das Unternehmen dadurch langfristig und nachhaltig zu verbessern.

3.3 Durchführung der Analyse

Die durchgeführte Auswertung der Experteninterviews hat verdeutlicht, dass die Umsetzung der NIS-2-Richtlinie in KMU nicht alleine durch das Studium der Gesetzestexte des BSIG n.F., sondern maßgeblich durch die Operationalisierung der etablierten Standards erfolgt. Die Experten wiesen übereinstimmend darauf hin, dass der unbestimmte Rechtsbegriff des „Stands der Technik“ erst durch den Abgleich von allgemeinen Frameworks eines ISMS, wie der ISO 27001 oder dem BSI IT-Grundschutz mit sektorspezifischen Anforderungen greifbar macht. Um KMU eine konkrete

Hilfestellung in Form von Maßnahmen (Controls) an die Hand zu geben, werden in diesem Kapitel die genannten Standards systematisch miteinander verglichen. Hier werden die theoretischen Anforderungen aus dem § 30 BSIG n.F. in technischen und organisatorische Controls überführt. Die Analyse gliedert sich dabei aufgrund der Fragestellung nach Gemeinsamkeiten und Unterschiede in zwei Unterkapitel. Zuerst werden in den geltenden Standards die Anforderungen für die gemeinsamen Anforderungen an ein risikobasiertes ISMS aller betroffenen Branchen in SOLL- und MUSS-Anforderungen erarbeitet. Die Durchführung der Analyse zur Operationalisierung der NIS2-Vorgaben folgt der inhaltlich qualitativen Inhaltsanalyse nach Kuckartz. Dies stellt eine systematische und methodisch kontrollierte Überführung der rechtlichen Normen in operative TOMs sicher. In diesem Prozess sollen die Ergebnisse in einer .csv Datei in Controls überführt werden. Der Prozess stellt zudem sicher, dass die dokumentierten Ergebnisse (Controls) sowohl theoretisch im BSIG n.F. fundiert, als auch empirisch durch die etablierten Sicherheitsstandards (Ergebnisse der Interviews) gesättigt sind. (Kuckartz, 2022, S. 39)

Das methodische Vorgehen nach Kuckartz gliedert sich für die inhaltlich strukturierende Analyse in folgende Schritte:

1. Initiierende Textarbeit: Zunächst erfolgte eine intensive Auseinandersetzung mit dem Gesetzestext des BSIG n.F., sowie den Rahmenwerken der ISO 27001 und dem BSI-IT-Grundschutz. Für die Findung der Gemeinsamkeiten wurde zusätzlich die Tabelle des BSI „Zuordnungstabelle Zuordnung ISO 27001 zum IT-Grundschutz“ verwendet (BSI, 2023b). Bei der Auseinandersetzung mit den Texten wurden zentrale Stellen identifiziert, die Anforderungen an das Risikomanagement definieren
2. Deduktive Kategorienbildung (A-priori-Kategorien): Basierend auf den gesetzlichen Anforderungen an das Risikomanagement aus dem BSIG n.F. wurden die Hauptkategorien deduktiv festgelegt. (Kuckartz, 2022, S. 70) Diese finden sich in der .csv als „NIS2-Themencluster“ wieder. Die Forschungsfrage nach den Gemeinsamkeiten und Unterschieden leitet hierbei die Strukturierung des Kategoriensystems.
3. Induktive Kategorienbildung: In einem zyklischen Prozess (vgl. 3.2.4) wurden die konkreten Controls aus den Standards den Hauptkategorien zugeordnet. Dabei wurden induktive Subkategorien gebildet, um den abstrakten gesetzlichen Vorgaben in spezifische operative Handlungsanweisungen zu unterteilen. (Kuckartz, 2022, S. 102)
4. Operationalisierung durch MUSS- und SOLL-Anforderungen: Zur praktischen Hilfestellung wurden die Anforderungen gemäß der Terminologie der Standards bewertet. (Förster et al., 2023, S. 22)

   MUSS-Anforderungen: Diese kennzeichnen uneingeschränkte gesetzliche Pflichten oder Basis-Anforderungen des BSI-IT-Grundschutzes, für die keine Risikoübernahme vorgesehen ist.

SOLL-Anforderungen: Diese repräsentieren den „Stand der Technik“ nach der Standardabsicherung. Diese sollten für ein angemessenes Sicherheitsniveau grundsätzlich erfüllt werden.

5. Strukturierung nach Gemeinsamkeiten (3.3.1) und Unterschieden (3.3.2): In dieser Phase wurden die Controls als Gemeinsamkeiten identifiziert, die in allen Sektoren als essenzielles „Grundrauschen“ gelten. Die Unterschiede wurden durch die Einbeziehung der sektorspezifischen Anforderungen (lex specialis) als zusätzliche, spezialgesetzliche Kategorien operationalisiert.

Die Ergebnisse dieser Untersuchungen wurden zu einem geordnetem Kategoriensystem, in dem jede ID in der .csv eine Sinneinheit ergibt. (Kuckartz, 2022, S. 90 ff.). Die csv-Ergebnis-Datei ist aufgrund ihrer Größe und damit schlechten Darstellbarkeit dem Anhang zu entnehmen. In diesem Kapitel wird die systematische Erarbeitung beschrieben.

Durch die Zuordnung der Maßnahmen zu einer Cyberframework-Dimension (z.b. präventiver Schutz) und die Definition der SOLL-Zustände wird die Analyse für KMU direkt anwendbar und überprüfbar. Die systematische Dokumentation erhöht die Nachvollziehbarkeit für die wissenschaftliche Gemeinschaft. Die operationalisierten Controls stellen bei Erfüllung keinen zertifizierbaren Zustand nach anerkannten Standards dar. Die Erfüllung der Controls soll dazu dienen, den KMU eine Unterstützung bei der Herstellung der Compliance nach den BSIG n.F. zu erleichtern und anwendbare Maßnahmen zu erhalten.

3.3.1 Gemeinsamkeiten

Die Abstrakten gesetzlichen Anforderungen aus dem § 30 BSIG n.F. werden in konkrete gemeinsame Ergebnisse für alle Branchen überführt, die ein Set aus Controls (technisch und organisatorisch) bilden. Dazu wurden die unter 2.4 genannten Risikomanamgentmaßnahmen einzeln betrachtet und hier den Maßnahmen aus dem BSI-IT-Grundschutz, sowie der ISO 27001 diesen zugeordnet. Die Controls wurden innerhalb der Risikomanagementmaßnahmen sinnvoll geclustert. Ziel ist es, die Maßnahmen zu operationalisieren, die sich als gemeinsame und überschneidenden Maßnahmen darstellen lassen.

Konzepte in Bezug auf die Risikoanalyse und die Sicherheit in der Informationstechnik:

Um eine Risikoanalyse der Einrichtung vornehmen zu können, beschreibt das BSI in ihrem Standard 200-2 in dem Kapitel 8.1 die Strukturanalyse. Diese umfasst mehrere Bausteine nach dem BSI-IT-Grundschutz: ORP.1.A2 Zuweisung der Zuständigkeiten, ORP.1.A8 Betriebsmittel- und Geräteverwaltung, OPS.1.1.1.A6 Durchführung des IT-Asset-Managements, APP.6.A9 Inventarisierung von Software, IND.1.A4 Dokumentation der OT-Infrastruktur, NET.1.1.A2

Dokumentation des Netzes und INF.11.A5 Erstellung einer Inventarliste. (BSI, 2023b, S. 8) In der ISO 27001 wird das Assetmanagement im Annex A.5.9 genauer erläutert. Dieses Assetmanagement (Strukturanalyse) bildet das notwendige Fundament für eine Risikoanalyse. Die schützenswerten Assets (digitale Vermögenswerte) sind dabei eindeutig zu kennzeichnen, um einen angemessen Umgang zu gewährleisten. Die Assets müssen im gesamten Lebenszyklus so verwaltet werden, wozu auch die Festlegung spezifischer Richtlinien für unterschiedliche Asset-Kategorien (strukturierte Bündelung der Assets) gehört. Zudem ist es in diesem Schritt notwendig eindeutige Nachvollziehbarkeit über die Verwendung oder Zuweisung von Geräten an Personen zu gewährleisten, um eine lückenlose Inventarisierung vorliegen zu haben. Ein weiteres Merkmal der Inventarisierung im Rahmen der Strukturanalyse, dass dort alle Geschäftsprozesse, Anwendungen, IT- und OT-Systeme sowie Räume und Gebäude abgebildet werden. Zur Dokumentation und anschließenden Durchführung der Risikoanalyse ist es hier notwendig, Listen mit den zu schützenden Informationen und deren Abhängigkeiten zwischen den Assets anzufertigen. Um eine Einschätzung über das Sicherheitsniveau der Infrastruktur vornehmen zu können, sollte zudem ein vollständiger Netzplan angefertigt werden, der die Struktur und Verbindungen innerhalb der Systemlandschaft grafisch darstellt.

Aufbauend auf der Strukturanalyse findet anschließend die Schutzbedarfsbestimmung der einzelnen Asset-Gruppen statt. Dazu werden Schutzbedarfe für alle Assets systematisch für die inventarisierten Geschäftsprozesse, Anwendungen, IT- und OT-Systeme, ICS, Gebäude und Kommunikationsverbindungen festgelegt. Diese wird BSI-Standard 200-2, Kapitel 5.1 Klassifikation von Informationen, 8.2 Schutzbedarfsfeststellung, sowie dem Baustein ISMS.1.A10 Erstellung eines Sicherheitskonzepts und in der ISO 27001 im Annex A.5.12 beschrieben.(BSI, 2023b, S. 8 f.)

Die geforderten Konzepte in Bezug auf die Risikoanalyse und Sicherheit in der Informationstechnik kann mit einem gefahrenübergreifenden Ansatz nur erstellt werden, wenn die beiden Schritte der Strukturanalyse und Schutzbedarfsbestimmung durchgeführt wurden. Dieser Ansatz wird im BSI-Standard 200-3 beschrieben und sollte Teil des Sicherheitskonzepte aus dem BSI-Standard 200-1 Kapitel 8 sein. (BSI, 2017, S. 32) Für eine vollständige Bewertung müssen die Gefährdungen aus Kapitel 3 des BSI-Standard 200-3 betrachtet und auf den jeweiligen Asset-Gruppen zugewiesen werden. (BSI, 2017c, S. 13 ff.) Aufgrund dieser Zuordnung entsteht eine eindeutige Gefährdungsübersicht, für die entsprechenden Maßnahmen erarbeitet werden können. Die entsprechenden Vorgaben aus der ISO finden sich im Annex A.6.1 bis A.6.2.

Als weiterer Punkt wurde in der Analyse die Netzwerksicherheit aufgrund der engen methodischen und gesetzlichen Verzahnung diesem Oberpunkt zugewiesen. Die Netzwerksicherheit stellt im BSIG n.F. für die „Sicherheit in der Informationstechnik“ hier eine tragende Säule dar. Die Netzwerksicherheit ist eine direkte Folge aus der Risikoanalyse, da die technischen Schutzmaßnahmen wie Netzwerksegmentierung und Perimeter Sicherheit erst dann

effektiv geplant werden können, wenn die Struktur- und Risikoanalyse anhand der vorhandenen Asset-Gruppen durchgeführt wurde. Diese Maßnahmen tragen aktiv zum ganzheitlichen Ansatz bei und schaffen eine Prävention durch Architektur.
Anschließend ist in den Konzepten ein kontinuierliches Sicherheitsmonitoring sowie die Reaktion auf Alarme zu verankern. Dies umfasst das Monitoring von Schwachstellen und die Ableitung von Behebungsmaßnahmen. Idealerweise wird in den Einrichtungen ein sogenanntes Security Operations Center (SOC) betrieben, dass die Angriffserkennungssysteme kontinuierlich überwacht und in der Lage ist, angemessen darauf zu reagieren. Die ist im BSI-Standard 200-2 Kapitel 10 Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit, sowie in mehreren Bausteine festgelegt. Die vollständige Liste der Bausteine in SOLL- und MUSS-Anforderungen ist in der csv-Ergebnis-Datei dokumentiert. Die ISO 27001 definiert diese Maßnahmen im Annex A.8.6 und A.8.16. (BSI, 2023b, S. 22 u. 26)

Bewältigung von Sicherheitsvorfällen:
Die Bewältigung der Sicherheitsvorfälle wurde aufgrund der strukturierten Analyse in vier Subkategorien aufgeteilt, die sich aus dem BSI-IT-Grundschutz und der ISO 27001 ergeben.
Zunächst ist es notwendig, Sicherheitsrichtlinien zu erstellen, die die Planung der Protokollierung und deren Umsetzung dokumentieren. Es müssen alle wichtigen Ereignisse in der Infrastruktur systematisch erfasst werden, die nach den Ergebnissen aus der Risikoanalyse priorisiert werden. Dazu dient in der Regel ein zentraler Log-Server, der diese relevanten Ereignisse in der Infrastruktur sammelt und koordiniert aufbereiten kann. Diese aufbereiteten Daten sind dann für automatische Auswertungen nutzbar. Als ein kritischer Punkt ist hierbei der Zugriffschutz zu identifizieren, da ausschließlich Administrierende darauf Zugriff haben sollten und eine Veränderung oder Löschung zu vermeiden. Dies ist insbesondere in den Bausteinen OPS.1.1.5 Protokollierung, DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten und DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse geregelt. Die ISO 27001 regelt dies im Annex A.8.15. (BSI, 2023b, S. 25)
In der zweiten Kategorie wird die Reaktion und Behandlung von Sicherheitsvorfällen operationalisiert. In dem ersten Bereich der Reaktion die zuerst die Definition eines Sicherheitsvorfalls das primäre Ergebnis, um eine Abgrenzung zum regulären IT-Betrieb herzustellen. Es müssen hier die Rollen und Verantwortlichkeiten für ein Incident Response Team (IRT) festgelegt werden, dass im Ernstfall die Entscheidungsbefugnis und das Know-How für Erstmaßnahmen und bei Bedarf forensische Untersuchungen besitzt. Der definierte Prozess gliedert sich in die Phasen der Eindämmung, der Beseitigung der Ursache und der anschließenden systematischen Wiederherstellung des sicheren Betriebszustands. Abschließend ergab die Analyse, dass eine standardisierte Nachbereitung vorgesehen ist, um die aus den gewonnenen

Erkenntnissen die Sicherheitsmaßnahmen präventiv verbessert werden können. Dies wird im IT-Grundschutz in den Bausteinen DER.2.1 Behandlung von Sicherheitsvorfällen, DER.1 Detektion von sicherheitsrelevanten Ereignissen, DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen, DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen und DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen, sowie in der ISO 27001 im Annex A.5.26 und A.5.27 geregelt. (BSI, 2023b, S. 11)
Das BSI empfiehlt hier zusätzlich die Erstellung eines Notfallhandbuchs in dem Baustein DER.4.A1 Erstellung eines Notfallhandbuchs, in dem die wichtigsten Informationen zu den Rollen, Sofortmaßnahmen, Alarmierung und Eskalation sowie den Kommunikations-, grundsätzlichen Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen enthalten sind (Förster et al., 2023, S. 347). Dieses Handbuch sollte allen Mitarbeitenden zur Verfügung gestellt werden. Eine direkte Zuordnung in der ISO 27001 konnte hier nicht gefunden werden, allerdings stellt diese Maßnahme eine allgemein sinnvolle Maßnahme für die betroffenen Einrichtungen dar und wird deshalb hier aufgeführt und in der Ergebnisdatei operationalisiert.

Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement:
Die an dieser Stelle erstellten Controls bilden die operative Grundlage für die Belastbarkeit und Überlebensfähigkeit der Einrichtungen im Falle einer Störung. Diese Maßnahmen sollen sicherstellen, dass der Geschäftsbetrieb selbst bei massiven Störungsereignisse in angemessener Zeit auf einem definierten Mindestniveau fortgeführt werden kann. Ein zentrales Ergebnis ist, dass die Einrichtungen aufgefordert werden, einen systematischen Datensicherungsplan zu erstellen, der auf der Analyse der vorhandenen Systeme basiert (vgl. Strukturanalyse). Dies ist im IT-Grundschutz in den Bausteinen CON.3 Datensicherungskonzept und OPS.1.2.2 Archivierung, sowie in der ISO 27001 im Annex A8.13 geregelt. (BSI, 2023b, S. 24 f.) Die Unternehmen sollten die Backups der IT-Systeme, als auch der darauf befindlichen Daten in regelmäßigen Abständen prüfen, so dass ein funktionsfähige Wiederherstellung im Notfall gewährleistet werden kann. Des Weiteren ist es notwendig, dass die Speichermedien räumlich getrennt von den IT-Produktivsystemen aufbewahrt werden. Idealerweise in einem anderen Brandabschnitt und unter geeigneten klimatischen Bedingungen, wie unter anderem im Baustein CON.3.A12 Sichere Aufbewahrung der Speichermedien für die Datensicherungen beschrieben. Um die Integrität und Vertraulichkeit der Backups sicherzustellen, müssen diese in geeigneter Weise vor unbefugten Zugriff geschützt werden und sollten kryptografisch verschlüsselt werden. Diese wird im Baustein CON.3.A14 Schutz von Datensicherungen beschrieben. Zusätzlich muss regelmäßig getestet werden, ob die Datensicherung wie gewünscht funktionieren und ob sichergestellt ist, dass die Kenngrößen RTO (Wiederanlaufzeit) und RPO (maximal tolerierbarer Datenverlust) aus den

Datensicherungsplänen eingehalten werden können. (Förster et al., 2023, S. 159 f.) Das Notfall- und Krisenmanagement wir im BSI-IT-Grundschutz im Baustein DER.4 Notfallmanagement, sowie in der ISO 27001 im Annex A.5.23 und A.5.30 geregelt. (BSI, 2023b, S. 12) Dort wird gefordert, dass die Unternehmen diese Pläne erstellen und den Ernstfall und die Abwehr zur Krisenbewältigung üben. Es soll auch sichergestellt werden, dass eine Notstromversorgung für den Notfall bestimmt wird, zum Beispiel durch eine USV (Unterbrechungsfreie Stromversorgung). Um im Krisenfall entsprechend angemessen und schnell reagieren zu können sollten die Organisation eine „Besondere Aufbauorganisation" (BAO) definieren, in der für außergewöhnliche Situationen zeitlich begrenzte Zuständigkeiten, Hierarchien sowie Kommunikations- und Entscheidungswege, die von dem täglichen Normalbetrieb abweichen können, festgelegt werden. Diese greift laut BSI-Standard 200-4 ab einem Notfall. Die Begriffe zu den Zuständen „Störung", „Notfall" und „Krise" sind in den Konzepten festzulegen. (BSI, 2023a, S. 18 ff.)

Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern:

Um die Sicherheit der Lieferkette zu gewährleisten, muss zunächst ein formalisierter Rahmen geschaffen werden. Hierzu sollte zunächst Mitarbeitende identifiziert werden, die in Verbindung mit der Lieferkette stehen und/oder spezifische Richtlinien und Prozesse zum Schutz der unmittelbaren Lieferkette entwickeln. Ziel ist es, die Aufrechterhaltung eines vereinbarten Sicherheitsniveaus über den gesamten Zeitraum der Lieferantenbeziehung hinaus zu gewährleisten und regelmäßig zu evaluieren. Um diese Risiken angemessen steuern zu können, müssen die betroffenen KMU zunächst Transparenz über die Abhängigkeiten herstellen. Dazu soll ein Verzeichnis der Lieferanten erstellt werden, in dem die Art und die Beziehungen von der Einrichtung zu den Lieferketten dokumentiert werden. Die ist in der ISO 27001 im Annex A.5.19 dokumentiert. Die BSI Standards liefern hier verschiedene Bausteine, in denen zum Beispiel die Nutzung von Outsourcing (OPS.2.3) geregelt wird. Für die Operationalisierung wird sich hier am Annex A.5.19 – A.5.21 der ISO 27001 orientiert, da das Vorgehen dort eindeutig beschrieben wird, während im BSI-Grundschutz eine Vielzahl an Bausteinen betrachtet werden muss, um die Maßnahmen sinnvoll zu operationalisieren. (BSI, 2023b, S. 10) Aufgrund des Verzeichnisses sollen besondere vertragliche Regelungen für die Zulieferer je nach Kritikalität festgelegt werden. Diese Regelungen zu Cybersicherheitskriterien sollen sich im Rahmen der Betroffenheit nach dem BSIG n.F. an der selbigen Gesetzgebung orientieren. Dies bedeutet, dass die Lieferkette der Einrichtung dieselben Risikomanagementmaßnahmen erfüllen muss, um eine einheitliche Strategie in der Lieferkette zu gewährleisten. Die Unternehmen müssen in der Lage sein, einen sicheren Betrieb ihrer Anlagen und Systeme sicherzustellen. Betroffenen Einrichtungen können hierzu Fragebögen für die Lieferkette erstellen, die den Inhalten des BSIG n.F. entsprechen, um

den Reifegrad objektiv bewerten zu können. Des Weiteren können bei KRITIS Audit- und Prüfungsrechte vereinbart werden, um die Einhaltung der Maßnahmen sowie der vorgegebenen Standards zu kontrollieren. Besonders sollte geprüft werden, ob die Lieferanten über angemessene Notfallpläne verfügen, um auf Sicherheitsvorfälle zu reagieren. So kann sichergestellt werden, dass die Mechanismen zur frühzeitigen Erkennung und Reaktion greifen und Cyberangriffe oder ein Ausfall nur geringe Auswirkungen auf die eigene Einrichtung haben.
Abschließend ergeben die Ergebnisse, dass sichere Ausstiegsszenarien (Exit-Strategie) definiert werden müssen, um den unverzüglich Entzug von Zugangsrechten, die Rückgabe von Vermögenswerten sowie die sichere Löschung oder Rückgabe von Daten sicherzustellen. So kann die Integrität der eigenen Informationen dauerhaft gewahrt werden.

Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen:

Die Analyseergebnisse dieser Anforderungen zeigen einen ganzheitlichen Lebenszyklus-Ansatz auf. KMU müssen klare Richtlinien und Verfahren für die Beschaffung von Informationstechnischen Systemen etablieren, die bereits für die Beschaffung Sicherheitskriterien erfüllen. Hierzu soll zunächst ein Anforderungskatalog erstellt werden, in dem die Auswahl von Software aus vertrauenswürdigen Quellen und der Abschluss von Wartungsverträgen, die zeitnahe Patches für Sicherheitslücken garantieren, festgelegt werden. Dies wird im IT-Grundschutzkompendium in den Bausteinen APP.6.A2 Erstellung eines Anforderungskatalogs für Software und APP.6.A3 Sichere Beschaffung von Software geregelt. Der gesamte Prozess bei der Entwicklung von Software wird im Baustein CON.8 Softwareentwicklung geregelt, welcher in der Ergebnisdatei mit den Unteranforderungen operationalisiert wurde. Die wichtigsten Controls stellen dabei die Trennung von Entwicklungs-, Test- und Produktionsumgebungen, die Durchführung statischer Code-Analysen sowie die Versionsverwaltung des Quellcodes dar. Bei der Entwicklung von Individualsoftware müssen KMU zudem klare Sicherheitsanforderungen an den Prozess definieren und Funktionen zur sicheren Systemintegration festlegen. (Förster et al., 2023, S. 171 ff.) Für die Analyse wurden zusätzlich die Controls A.8.25 - A.8.31 aus dem Annex der ISO 27001 ausgewertet und operationalisiert. Für Unternehmen, die eigene Software entwickeln und in Europa vertreiben, kann hier zusätzlich der Cyber Resilience Act (CRA) greifen. Dieser wurde hier aufgrund von dessen speziellen Anforderungen nicht weiter berücksichtigt.
Als ein weiteres Control aus diesem Cluster wurde die Anforderung an ein systematisches Patch- und Änderungsmanagement (Change Management) operationalisiert. Die Einrichtungen sollen Verfahren definieren, die sicherstellen, dass sicherheitskritische Patches für Systeme, Anwendungen und Firmware zeitnah nach deren Veröffentlichung eingespielt werden. Die ist im

Baustein OPS.1.1.3 Patch- und Änderungsmanagement geregelt. (Förster et al., 2023, S. 221 ff.) Um dies in ausreichender Form bewerkstelligen zu können, ist es notwendig, ein Management und die Offenlegung von Schwachstellen vorliegen zu haben. Das Schwachstelleninventar soll auf Basis der eingesetzten Software erstellt und gepflegt werden, um Sicherheitslücken im IT- und OT-Bereich zentral zu erfassen und deren Behebung nachzuhalten. Die Erhebung kann über regelmäßige und automatisierte Schwachstellenscans erfolgen, oder durch sogenannte Penetrationstests und Red Teaming. (BSI, 2023b, S. 23 f.) Abschließend betonen die Ergebnisse, dass auch die Außerbetriebnahme von legacy Software ein Teil des Lebenszyklus sein soll. KMU müssen sicherstelle, dass bei der Außerbetriebnahme von Systemen alle schützenswerten Daten und Zugänge sicher gelöscht werden, um eine nachträgliche Offenlegung von Informationen zu verhindern. Dies wird im BSI-IT-Grundschutz in mehrere Bausteinen geregelt, sowie in der ISO 27001 im Annex A.7.14. (BSI, 2023b, S. 20). Diese sind in der Ergebnisdatei operationalisiert.

Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik:

Die Ergebnisse dieses Clusters zeigen, dass die bloße Umsetzung der Controls nicht ausreicht, um die Effektivität abschließend bewerten zu können. Ein zentrales Element stellt dabei die Verpflichtung für das Management, den Risikomanagementprozess regelmäßig auf seine Wirksamkeit und Effizienz hin zu prüfen. Gemäß dem BSI 200-1 Kapitel 7.4 und 8.3 (BSI, 2017a, S. 30 ff.) und der ISO 27001 Kapitel 9.3 sollen die Maßnahmen dazu beitragen, dass die Aufrechterhaltung, sowie die Verbesserung der Informationssicherheitsmaßnahmen gewährleistet ist. Dazu können Management-Berichte dienen, die über den aktuellen Status des Sicherheitsprozesses, Ergebnisse von Prüfungen sowie über aktuelle auftretende Bedrohungen Auskunft erteilen. Die Leitungsebene soll dabei kritisch hinterfragen, ob die Sicherheitsziele noch angemessen sind und ob die gewählte Strategie angesichts sich veränderter Rahmenbedingungen angepasst werden muss. Zur objektiven Bewertung fordern die Controls regelmäßige Audits und Revisionen, die sich an einer unabhängigen Prüfung – also von Personen durchgeführt werden sollten, die nicht an der Planung der Maßnahmen beteiligt waren, um „Betriebsblindheit“ zu vermeiden - orientieren. Die Revisionen können auf den BSI-Leitfäden basieren und sollten sowohl Dokumentenprüfungen als auch vor-Ort-Kontrollen umfassen. Speziell für KMU können hierbei auch einfache technische Checks der IT-Systeme in Kombination mit Workshops zu Problemen im Sicherheitskonzept einen ausreichenden Überblick verschaffen. Zur Modellierung der Controls wurde hier besonders der Baustein DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision in Kombination mit dem Annex A.9.1 – A.9.3 der ISO 27001 berücksichtigt. (BSI, 2023b, S. 5) Des Weiteren finden sich sinnvolle Informationen und Maßnahmen in dem BSI-Standard 200-2 Kapitel 10, die in der Ergebnisdatei Anwendung finden. (BSI, 2017b, S. 163 ff.) Die Wirksamkeit des implementierten ISMS, oder „ISMS-light“ wird durch die Definition und

Auswertung von Kennzahlen (KPIs) messbar gemacht. Hier liefert das BSI im Dokument „Reife- und Umsetzungsgrad-bewertung im Rahmen der Nachweisprüfung (RUN)“ für KRITIS Unternehmen fünf verschiedene Reifegrade zur Überprüfung des Management Systems in den Kategorien Organisatorische Maßnahmen (OrgM) Umsetzungsgrad, Personenbezogene Maßnahmen (PerM), Physische Maßnahmen (PhyM) und Technische Maßnahmen (TecM). Die dort definierten Messgrößen sollen von den Einrichtungen als zusätzliche Indikatoren über deren eigenen Stand berücksichtigt werden.
Die Bewertung der Wirksamkeit ist dabei kein Selbstzweck, sondern ist zwingend erforderlich, um einen kontinuierlichen Verbesserungsprozess zu etablieren. Die Erkenntnisse aus den Überprüfungen, wie Audits, Übungen (Wiederherstellungstests) oder realen Sicherheitsvorfällen müssen konsequent zur Korrektur des Sicherheitskonzeptes und zur Optimierung der Maßnahmen beitragen.

Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik:

Es sollten je nach Größe der Einrichtung Zielgruppenorientierte Schulungsmaßnahmen etabliert werden. Die allgemeinen Schulungen für alle Mitarbeitenden dienen der Erlernung und Vertiefung von Basiskompetenzen und der Schärfung des Sicherheitsbewusstseins im gesamten Unternehmen sowie der in der Informationssicherheitsrichtlinie definierten Betriebspolitik. Es sollten ergänzend dazu fachspezifische Schulungen angeboten werden, die besonders in Abteilungen durchgeführt wird, in denen die Personen direkt mit der Informationssicherheit in Berührung kommen. Dazu zählen unter anderem die IT-Abteilung (intern, wie extern), der ISB und das ISMT (Informationssicherheitsmanagementteam), für die regelmäßige und tiefergehende Qualifizierungen notwendig sind, um den technisch-organisatorischen „Stand der Technik“ zu wahren. (Förster et al., 2023, S. 208)
Die Vermittlung des Wissens wird hier als kontinuierlicher Prozess betrachtet, der eine wesentliche Verankerung im Onboarding-Prozess der Mitarbeitenden darstellt. Es soll sichergestellt werden, dass bei Neueinstellungen oder internem Positionswechsel über Richtlinien und Verhaltensregeln informiert wird. Dazu wurden in der Ergebnisdatei die BSI 200-1 Kapitel 6 und mehrere Bausteine, sowie die Controls A.6.3 und A.7.4 operationalisiert. (BSI, 2023b, S. 4, 14) Ergänzend dazu ergibt sich aus der Analyse, dass es notwendig ist, die Ergebnisse der Schulungsmaßnahmen kontinuierlich zu messen. Die Lernerfolge sollten auch hier zielgruppenorientiert ausgewertet werden, um Schwachstellen im Wissensstand zu identifizieren. So kann das Schulungsprogramm basierend auf den Erkenntnissen in Kombination mit den aktuellen Bedrohungen stetig verbessert werden. Zur Messung des aktuellen Standes können sogenannte „Phishing-Kampagnen“ dienen, bei der die Belegschaft eigens für das Unternehmen erstellte Mails mit Phishing-Link bekommt. Diese werden in zufälligen Abständen

ausgesendet und die Ergebnisse über die Klickrate und die Eingabe von Informationen wie Zugangsdaten und Passwörter ausgewertet.
Für Informationskampagnen können niederschwellige Kanäle wie Plakate, Flyer oder digitale Aushänge genutzt werden, um die Sicherheitsthemen im Alltag präsent zu halten.

Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren:
Die Ergebnisse der Analyse resultieren maßgeblich auf dem Baustein CON.1 Kryptokonzept aus dem BSI-IT-Grundschutz, sowie dem Control A.8.24 der ISO 27001. (BSI, 2023b, S. 29) Die kryptographischen Verfahren stellen ein essenzielles Mittel dar, um die Schutzziele sowohl für gespeicherte, als auch für übertragene Informationen sicherzustellen. Zunächst muss das Kryptokonzept erstellt werden, welches eine verbindliche Richtlinie ist, in der festgelegt wird, auf Basis welcher Kriterien kryptographische Verfahren und Funktionen ausgewählt werden. KMU sollten hierbei etablierte Verfahren einsetzen, die den aktuellen Stand der Technik entsprechen, die beispielsweise in der technischen Richtlinie BSI TR-02102 empfohlen werden. In dem Konzept soll zudem beschrieben sein, wie sichergestellt wird, dass kryptographische Funktionen von Hard- und Software sicher konfiguriert und korrekt eingesetzt werden.
Das Risikomanagement in diesem Bereich erfordert einen prozessualen Rahmen für den gesamten Lebenszyklus der kryptographischen Schlüssel. Dazu zählen die Erzeugung und der Austausch dieser Schlüssel, wie auch die sichere Aufbewahrung und die Löschung/Vernichtung. Dies bildet den gesamtem Lebenszyklus und verhindert Missbrauch während der Lebenszeit, sowie bei nicht mehr verwendetem Schlüssel. Um die Wirksamkeit der Maßnahmen zu bewerten, wird die Führung eines Krypto-Katasters empfohlen. In diesem werden dann die IT-Systeme mit deren Einsatzzweck, die Verantwortlichen sowie die verwendeten Algorithmen und weitere sicherheitsrelevante Parameter dokumentiert. Die Einrichtungen sollten mindestens jährlich prüfen, ob die eingesetzten Verfahren noch ausreichend sind, oder ob eine Ablösung eines Systems notwendig ist.
Die kryptographischen Verfahren müssen in den Unternehmen konsequent in den operativen Betrieb integriert werden, um die Informationen des Unternehmens während der Übertragung, aber auch bei der Datenspeicherung auf mobilen Endgeräten, Wechseldatenträgern oder in der Cloud-Umgebung ausreichend zu sichern. Beim Einsatz einer starken Verschlüsselungsstrategie kann das Risiko Vertraulichkeitsverlusts bei Diebstahl oder Verlust der Hardware minimiert werden.

Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen:
Die Analyse der Bausteine und Vorgaben verdeutlichen in diesem Cluster, dass der Schutz von Informationen untrennbar mit der Kontrolle über Personen, Identitäten und physischen

Ressourcen verbunden ist. Die Ergebnisse wurden in vier Sub-Kategorien geteilt, wobei die erste vor allem bei KRITIS-Unternehmen zur Anwendung kommt:

1. Sicherheit des Personals (personelle Maßnahmen)

Die Einrichtungen müssen Konzepte etablieren, die das Sicherheitsrisiko durch Mitarbeitende über den gesamten Beschäftigungszyklus minimieren. Vor Beginn des Arbeitsverhältnisses sollten Sicherheitsprüfungen durchgeführt werden. Dazu zählt die Validierung von Lebensläufen, Zeugnissen und Referenzen. Bei sensiblen Positionen sollte zusätzlichen ein polizeiliches Führungszeugnis angefordert werden. Bei der vertraglichen Bindung sollten ergänzende Dokumente, wie die Informationssicherheitsrichtlinie, sowie dazu ergänzende Anhänge - wie die Verschwiegenheitserklärungen - beigelegt und durch die neuen Mitarbeitenden bestätigt werden. (BSI, 2025a, S. 13)

2. Zugriffskontrollen und Rechtevergabe

Hier ist ein für den Wechsel oder das Ausscheiden von Mitarbeitenden ein geregelter Prozess zu etablieren, der das Zurückgeben von Assets (Schlüssel, Geräte, Ausweise) und das unverzügliche Entziehen oder Löschen von Zugriffsrechten beinhaltet. Dies ist in der ISO 27001 im Annex unter Punkt A.6.5, sowie der BSI Grundschutzbausteinen ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden und ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen geregelt. (BSI, 2023b, S. 14)

3. Zugriffskontrolle (Logisch und Physisch)

Ein wirksames IAM (Identitäts- und Berechtigungsmanagement) bildet den Kern der zweiten Subkategorie. Die Rechtevergabe an die Mitarbeitenden sollte stehts rollenbasiert erfolgen und sich an den aktuellen Standards orientieren. Dazu zählen unter anderem das Need-to-know-Prinzip (Kenntnis, nur wenn nötig) und das Least-Privilege-Prinzip (geringste, erforderliche Rechte). Die Angemessenheit der Rechte sollte dabei regelmäßig für alle Nutzenden geprüft werden. Dies wird in der ISO 27001 im Annex unter A.8.2 und A.8.3, sowie mehreren IT-Grundschutz-Bausteinen geregelt. Der wichtigste Baustein zur Orientierung für alle Unternehmen ist der ORP.4 Identitäts- und Berechtigungsmanagement. (BSI, 2023b, S. 21)

Der Gebrauch und Umgang mit Passwörtern, sowie deren Komplexität muss ebenfalls geregelt werden. Hier legt besonders der Baustein ORP.4.A23 Regelung für passwortverarbeitende Anwendungen und IT-Systeme die Vorgaben für IT-Systeme fest. (Förster et al., 2023, S. 126)

Um die physische Sicherheit zu gewährleisten, werden für schützenswerte Infrastrukturen weitere Maßnahmen in der ISO 27001 im Annex A.7.1 – A.7.5 und den dazu gemappten Bausteinen im IT-Grundschutz ausführlich geregelt. Diese sind in der Ergebnisdatei entsprechend für die Mindestanforderungen operationalisiert. (BSI, 2023b, S. 15 ff.)

4. Sichere Authentisierung, Authentifizierung und Autorisierung des Personals:

Als Grundlage hierfür muss ein Konzept für die Authentisierung erstellt werden, welches die Zugriffe auf alle IT-Systeme und Dienste durch einen angemessene Identifikation und

Authentisierung zugreifender Nutzender, Diensten, oder IT-Systeme regelt. Hier sollte auch die Authentisierung an OT-Komponenten berücksichtigt werden. Dies wird in der ISO 27001 im Annex unter A.8.2 und in mehreren BSI-Grundschutz Bausteinen geregelt. (BSI, 2023b, S. 21)

Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung:

Bei der Analyse des letzten Clusters ergeben sich die Anforderungen an MFA (Multi-Faktor-Authentifizierung) und die Übertragung der Kommunikation im Notfall und innerhalb der Unternehmen. Die Anforderungen an MFA überschneiden sich hier teilweise mit bereits ausgeführten Clustern, da diese zum einen als Grundlage ein Konzept benötigen und technisch umgesetzt werden müssen. Die mehreren Faktoren bei der Authentifizierung müssen vor allem bei privilegierten Konten angewendet werden. Wichtig ist bei der Implementierung, dass zwingend mindestens zwei verschiedene Faktoren verwendet werden. Dabei unterscheidet die Literatur zwischen verschiedenen Kategorien, wie Wissen (z.B. Passwort), Besitz (z.B. Hardwaretoken) oder Inhärenz (Biometrie). Dies wird zum einen in der ISO 27001 im Annex unter A.8.5 als auch in dem BSI Baustein SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung gefordert. (BSI, 2023b, S. 22) Ergänzend dazu wird die Nutzung von Lösungen zur kontinuierlichen Authentifizierung empfohlen, um die Identität während einer laufenden Sitzung permanent zu verifizieren.

Die Ergebnisse für den Teil „gesicherte Sprach-, Video- und Textkommunikation“ basieren maßgeblich auf dem Baustein APP.5.4 Unified Communications und Collaboration (UCC), der diese Anforderungen bündelt. Zunächst wird dort die Planung und Konzeption, über Implementierung in der Netzplanung zu den Tests beschrieben. Der Baustein APP.5.4.A6 Verschlüsselung von UCC-Daten beschreibt schließlich die Implementierung der Verschlüsselung der Kommunikationswege. (BSI, 2025a, S. 459)

Die gesicherte Notfallkommunikation ist Teil des BSI Standards 200-4 (BCM). Dort wird gefordert, dass sichergestellt werden muss, wie die Notfallkommunikation während eines Ausfalls bewerkstelligt werden kann. Es sollten Kommunikationskanäle eingehalten werden, die unabhängig von der organisationsinternen IT funktionieren, um auch bei einem Netzwerkausfall funktionierende Meldewege zu haben. (BSI, 2023a, S. 104)

Die gesicherte Notfallkommunikation muss einem dokumentierten Prozess folgen und regelmäßig im Rahmen von Krisenübungen auf ihre Wirksamkeit geprüft werden.

3.3.2 Unterschiede

Die Analyse der Experteninterviews in Kombination mit den verfügbaren B3S des BSI verdeutlicht, dass für viele Branchen bereits hoch spezifizierte Anforderungen existieren, während in anderen Sektoren noch erhebliche Orientierungslücken vorhanden und regulatorische Unklarheiten bestehen. Der „Stand der Technik“ wird hier stark maßgeblich von allgemeinen Standards, wie der ISO 27001 und dem BSI-IT-Grundschutz geprägt, während andere Branchen diesen durch vorhandene Standards schärfen müssen. Ein essenzielles Merkmal, das mit dem BSIG n.F. einhergeht, ist, dass die Sektoren, die bereits von einer Regulatorik betroffen waren, nun den Scope auf das gesamte Unternehmen erweitern müssen. Ein Fokus auf einzig den Kernbereich der Einrichtungen ist damit nicht mehr möglich.
Basierend auf den Auswertungen aus der Tabelle 3.2.2 lassen sich für die betroffenen Sektoren folgende Spezifika und geltende Standards festhalten, an denen sich die KMU orientieren müssen:

Energie:
Aufgrund der spezifischen Standards ergeben sich für Energieversorgungsunternehmen (EVU) und Stadtwerke wesentliche Zusatzanforderungen, die über die BSIG n.F. Umsetzung hinausgehen. Eine der massivsten Änderungen durch das BSIG ist, dass die bisher oft auf die reine Netzleittechnik beschränkte Zertifizierung nun auf die gesamte Organisation inklusive der Verwaltungs-IT ausgeweitet werden muss.
Während für viele Sektoren keine fester Nachweiszyklus vorgegeben wird, müssen Energieversorger gemäß dem ITSIK oft bereits alle zwei Jahre ein Audit-Ergebnis vorlegen. Bei der Lieferantensicherheit müssen die Betreiber in ihren Lieferantenvereinbarungen spezifische Klauseln zu Auditrechten und Sicherheitsnachweisen enthalten, da EVU für die Sicherheit ihrer kritischen Komponenten gegenüber der BNetzA (Bundesnetzagentur) haften. Für die physische Resilienz und Notfallvorsorge müssen für die Erfüllung des „Stands der Technik“ zwingend regelmäßige Notstromtests durchgeführt und die die Erstellung von Notfallhandbüchern für jeden einzelnen kritischen Prozesse erfüllt werden.
Bei der Meldepflicht muss dieser Sektor oft parallel die Meldung bei der BNetzA einreichen.

Finanzwesen / Versicherung:
Zur Vermeidung von Doppelregulierungen sind diese Sektoren laut § 28 Abs. 6 BSIG n.F. von den allgemeinen Risikomanagement-, Melde- und Nachweispflichten laut §§ 30, 31, 32, 35, 36, 38 und 39 weitgehend ausgenommen, sofern sie gleichwertige Anforderungen erfüllen. Dennoch bleibt die Kooperation zwischen dem BSI und der BaFin für den Informationsaustausch zwingend vorgeschrieben. Die DORA fordert zusätzlich tiefergehende Schulungen für Geschäftsleitung, die auch die „letztliche Verantwortung“ für das Management von IKT Risiken trägt. Für das

Lieferantenmanagement gelten strenge Vorgaben für die Überwachung von IKT-Drittdienstleistern. Verträge müssen spezifische Mindestbestandteile enthalten, wie uneingeschränkte Auditrechte, klare Ausstiegsstrategien und präzise Leistungsbeschreibungen (SLAs).

Maschinenbau:

Der Sektor Maschinenbau und insbesondere der Sondermaschinenbau sind bereits stark reguliert. Diese Branche ist durch eine starke Verflechtung aus klassischer IT und OT und ergänzende EU-Verordnungen geprägt. Für diese Einrichtungen ist die NIS-2-Richtlinie nicht die einzige maßgebliche Richtlinie, vielmehr müssen die unterschiedlichsten Rechtsnormen zusammengeführt werden. Die geltenden Normen unterliegen meist auch einem klassischen ISMS Aufbau nach etwa der ISO 27001. Die IEC 62443 ist eine entscheidende Norm für die Absicherung von industriellen Kommunikationsnetzen und der OT-Sicherheit. Die NIS2 fordert hier eine Erweiterung des Scopes des ISMS auf das gesamte Unternehmen – somit reicht eine reine Betrachtung des Maschinenbausektors nicht mehr aus.

Zusätzlich können die Unternehmen in dieser Branche unter die Maschinenverordnung (MVO), den CRA für Produkte mit digitalen Elementen sowie den EU AI-Act fallen. Durch eine indirekte Betroffenheit als Zulieferer für KRITIS Unternehmen unterliegen sie zusätzlich den Anforderungen der KRITIS-Verordnung. Der Stand der Technik definiert sich hier vielmehr über die OT-Sicherheit, ein vollumfängliches MFA für z.B. Fernwartungen der Maschinen, wie eine Netzwerksegmentierung für die Maschinen.

Laut den Interviews ist in dieser Branche oftmals die Awareness noch nicht vollständig vorhanden, da der Fokus der Geschäftsleitung vielmehr auf der Produktion der Maschinen, als auf der IT-Security liegt – diese wird eher als „notwendiges Übel“ angesehen. Die neuen Verordnungen sollten dazu führen, dass die betroffenen KMU sich nun deutlich mehr mit der Sicherheit ihres gesamten Unternehmens beschäftigen müssen.

Gesundheit & Pharma:

Die Sektoren Gesundheit und Pharma unterliegen aufgrund der hohen Sensibilität der verarbeitenden Daten und der kritischen Bedeutung für die Patientenversorgung einem besonders strengen regulatorischen Rahmen, der durch spezialisierte Branchenstandards und gesetzliche Vorgaben konkretisiert wird. Gemäß der Anlage 1 des BSIG n.F. umfasst dieser Bereich nicht nur die Erbringung von Gesundheitsdienstleistungen durch Krankenhäuser, sondern auch Labore sowie Unternehmen, die Arzneimittel erforschen, entwickeln oder pharmazeutische Erzeugnisse herstellen. Es können auch häusliche Krankenpfleger betroffen sein, die zu pflegenden Personen Medizin verabreichen, selbiges gilt für Pflegeheime.

Aus diesem Grund lassen sich hier zunächst mehrere B3S zuordnen, wie B3S Krankenhaus, B3S Pharma und B3S Laboratoriumsdiagnostik. Deshalb ist es für die betroffenen Unternehmen notwendig, die für sie passenden und geltenden B3S mit in die Gesamtkonzeption des ISMS mit einzubeziehen.

Darüber hinaus sind in der pharmazeutischen Industrie spezialisierte Richtlinien wie GAMP 5 (Good Automated Manufacturing Practice) sowie GXP-Anforderungen für die Validierung computergestützter Systeme von zentraler Bedeutung.

Die Experten aus den Interviews betonen, dass im Gesundheitswesen die Schutzobjekte adressiert werden müssen, die über einen Standard-ISMS hinausgehen. Zu diesen zählen unter anderem, dass Krankenhäuser und Labore spezialisierte Zutrittssysteme benötigen, die über den allgemeinen Gebäudezutritt hinausgehen. Dies betrifft insbesondere die Absicherung von Laboren und Medikamentenlagern, in denen wertvolle Bestände vor Missbrauch oder Diebstahl geschützt werden müssen. Des Weiteren müssen sich die Schutzziele auf die Datenintegrität und Patientenschutz konzentrieren. Die Systeme müssen sich dahingehend auf die Schutzziele Integrität und Verfügbarkeit dieser Informationen konzentrieren. Eine Manipulation der Systeme können zu unmittelbaren lebensbedrohlichen Folgen führen, weshalb beispielsweise industrielle Steuerungssysteme (ICS) in der Produktion oder Medizintechnik einen extrem hohen Schutzbedarf aufweisen.

Sonderregelung für Nachweise: Für zugelassene Krankenhäuser sieht das Gesetz eine längere Frist vor: Während andere Einrichtungen meist nach drei Jahren Nachweise erbringen müssen, kann das BSI diese von Krankenhäusern erst nach fünf Jahren verlangen, sofern keine andere Rechtsverordnung einen früheren Zeitpunkt bestimmt. Weitere Herausforderungen stellen die Legacy-Systeme und das Medizinproduktegesetz (MPG) dar. Eine der größten praktischen Schwierigkeiten liegt in der Integration veralteter Medizintechnik in moderne Sicherheitsarchitekturen. Das Medizinproduktegesetz (MPG) begrenzt zudem die Veränderbarkeit zertifizierter Medizinprodukte erheblich. Da selbst geringfügige Änderungen die Zulassung des Geräts gefährden können, lassen sich sicherheitskritische Updates oder Patches häufig nicht ohne weiteres einspielen. Hinzu kommt, dass die Experten in den Interviews den Einsatz veralteter Betriebssysteme bemängeln. Etwa bei Medizingeräten, die noch auf Windows XP oder ähnlich alten Plattformen basieren. Da eine Aktualisierung oft technisch oder regulatorisch nicht möglich ist, müssen solche Systeme konsequent segmentiert werden, etwa durch strikte Netz- oder Mikrosegmentierung und sie somit vom übrigen Kliniknetz isolieren, um Sicherheitsrisiken zu minimieren. Insgesamt entsteht im Bereich Gesundheit und Pharmazie durch das Zusammenspiel von B3S-Konkretisierungen, strengen Qualitäts- und Zulassungsanforderungen sowie den technischen Restriktionen des MPG eine hochkomplexe Ausgangslage für die praktische Umsetzung der NIS2-Anforderungen.

Transport und Verkehr:

Für die Regulatorik und Standards greifen in dieser Branche mehrere fachspezifische Gesetzte wie das Luftsicherheitsgesetz sowie IT-Grundschutz-Profil für kleine und mittlere Flughäfen. Für die weitere Konkretisierung für den Straßentransport dienen die B3S Bundesautobahn und B3S kommunaler Straßenverkehr. Das Kernziel dieser Branche ist die größtmögliche Verfügbarkeit, da ohne IT die Warenströme nicht gesteuert werden können. Hinzu kommt die Vernetzung der Lieferkette, die ein Hauptproblem darstellen kann, wenn einer der zahlreichen Partner aufgrund der unterschiedlichen Sicherheitsniveaus ausfällt und Alarmierungsketten, sowie Wiederanlaufpläne nicht einhalten kann.

Zu den Spezifika des Luftverkehrs zählt unter anderem die Bodeninfrastruktur (Groundhandling), da diese die Grundlage für einen funktionierenden Verkehr darstellt. Die physischen Schnittstellen erfordern hier zusätzliche Maßnahmen.

Für Transportdienstleister mit Automotive-Bezug (z. B. Transport von Prototypen) ist der TISAX-Standard oft eine zwingende Anforderung der Hersteller, der durch die Lieferkette greifen kann.

Ernährung (Lebensmittel):

Die Branche Ernährung wird in der NIS2 im Vergleich zur NIS1 breiter betrachtet und es können somit auch die Lebensmittelhändler davon betroffen sein. Als bereits geltende Standards können hier die B3S Lebensmittelhandel und die B3S Ernährungsindustrie herangezogen werden, um den Stand der Technik zu ermitteln. Laut den Experten sind diese Branchen bereits gut reguliert und erfüllen damit einen hohen Reifegrad. Dazu zählen die geltenden Qualitätsstandards IFS (International Food Standard) und HACCP, welche bereits Prüfungen in Form von Audits vorsehen. Aufgrund der strengen Auflagen ist bereits eine Chargenrückverfolgung Standard und kann auf die Zulieferer von IT-Systemen adaptiert werden. Die meisten dieser Prozesse sind bereits elektronisch abgebildet und aufgrund der Vorgaben dokumentiert, was eine gute Basis für eine ISMS bilden kann. Der hohe Reifegrad und die etablierten Controls müssen in geeigneter Form des PDCA Zyklus abgebildet werden. In der Regel gibt es bereits Qualitätsmanagementbeauftragten (QMB), die mit diesen Prozessen vertraut und in der Lage sind, bei der ISMS Einführung sowie dem Betrieb zu unterstützen. Dies ist besonders sinnvoll, da diese Personen bereits mit der Einhaltung von Richtlinien vertraut sind. Der Zusatzaufwand wird daher in dieser Branche im Vergleich zu weniger vorregulierten KMU als besonders gering eingeschätzt. Die größte Herausforderung ist auch hier laut den Experten der Faktor Mensch, da man nun die IT-Systeme zusätzlich betrachten muss und dies zu Veränderungen in den gelebten Prozessen führen kann.

Digitale Infrastrukturen (MSP / Cloud)

Diese Sektoren übernehmen als direkt betroffene Branchen und als kritische Dienstleister in der Lieferkette eine besondere Doppelrolle ein. Zunächst muss einmal die direkte Betroffenheit rechtssicher geklärt werden und im zweiten Schritt die Betroffenheit durch die Lieferkette. Als branchenspezifische Standards sollten die B3S für Housing, Hosting und CDN herangezogen werden. Da für viele Teildienste dieses Sektors (z. B. Cloud-Anbieter oder MSPs) Durchführungsrechtsakte der Europäischen Kommission zur Festlegung technischer Anforderungen Vorrang haben, müssen betroffene Unternehmen diese internationalen Vorgaben zwingend mit nationalen Standards wie dem BSI C5-Katalog oder dem BSI IT-Grundschutz harmonisieren. Besonders die Betriebskontinuität und Redundanz müssen von den Betreibern als Schutzziele betrachtet werden. Dazu zählt unter anderem auch, dass ein umfassendes BCM inklusive Backup-Management und Wiederherstellungsplänen vorgehalten wird und diese regelmäßig auf ihre Wirksamkeit getestet werden. Zusätzlich müssen die Betreiber starke technische Maßnahmen ergreifen, um die Risiken für ihre Systeme zu minimieren.
Sollten die Anbieter zusätzlich digitale Produkte vertreiben, muss der CRA eingehalten werden und das Risikomanagement vollumfänglich für diese Produkte angewendet werden.

Siedlungsabfallentsorgung:

Diese Branche ist aktuell kaum reguliert und daher wird hier ein besonders hoher Aufwand erwartet. Zur Orientierung gibt es hier die B3S Siedlungsabfallentsorgung, an denen sich orientiert werden soll. Für die betroffenen KMU müssen zunächst die Grundlagen für ein ISMS geschaffen werden.

4 Fazit

4.1 Unklarheiten für KMU

Die Umsetzung der NIS-2-Richtlinie in nationales Recht durch das BSIG n.F. stellt viele Unternehmen in Deutschland vor erhebliche regulatorische Unklarheiten. Eine der zentralen Unklarheiten liegt bereits in der Einstufung der Betroffenheit, da die Einrichtungen nicht über die eigene Betroffenheit informiert werden. Diese müssen eigenständig anhand der Kriterien wie Branche, Mitarbeiteranzahl und Umsatz prüfen, ob sie betroffen sind und wenn ja, ob als „wichtige“ oder „besonders wichtige“ Einrichtung. Dies ist ohne spezialisiertes Fachwissen oder eine Rechtsberatung oftmals nicht möglich und führt zu ungenauen Ergebnissen.

Zudem erweist sich der für die Risikomanagement maßgebliche „Stand der Technik“ als unbestimmter Rechtsbegriff, der in der Gesetzgebung nicht weiter präzisiert wurde. So haben die Unternehmen nach der Prüfung der Betroffenheit im nächsten Schritt die Herausforderung, passende Maßnahmen für ihre Bedürfnisse zu definieren. Eine rechtssichere Bewertung der technischen und organisatorischen Maßnahmen auf deren Angemessenheit und Verhältnismäßigkeit ist eine zusätzliche Herausforderung. Die Heterogenität zwischen den verschiedenen Branchen erschwert die Vereinheitlichung auf passende Sicherheitsstandards.

Für bereits regulierte Branchen bringt die potenzielle Doppelregulierung ein weiteres Konfliktfeld mit sich, da es teilweise Überschneidungen in den einzelnen Anforderungen gibt. Diese Umsetzung der Anforderungen müssen dann pro Regulierung geprüft und bei Bedarf geschärft werden. Diese Überschneidungen führen in der Praxis zu redundantem Aufwand und Unklarheiten darüber, welche spezifischen Melde- und Nachweispflichten vorrangig zu erfüllen sind.

Aufgrund der Lieferkettensicherheit herrscht bei nicht direkt betroffenen Unternehmen eine weitere Unklarheit. Diese werden oftmals von regulierten Branchen zur Erfüllung von komplexen Sicherheitsstandards aufgefordert. Dies führt zu einer problematischen Haftungsverschiebung innerhalb der Lieferkette auf KMU. Die Erfüllung der

Sicherheitsanforderungen, sowie die Beantwortung der Fragebögen überfordert diese Unternehmen administrativ und finanziell.

Schließlich bestehen weitere Unklarheiten bei den Schulungspflichten für die Geschäftsleitung. Der Gesetzgeber schreibt zwar regelmäßige Schulungen vor, macht aber keine konkreten Vorgaben zu deren exakter Dauer oder den verbindlichen Inhalten. Bisher existieren hierzu lediglich vorläufige Handreichungen des BSI, was die rechtsverbindliche Ausgestaltung dieser Pflichten für die betroffenen Führungskräfte erschwert.

4.2 Vorteile der NIS-2-Richtlinie

Durch die Einführung von einheitlichen Richtlinien in der europäischen Union bieten sich für KMU trotz des initialen administrativen Aufwands bedeutende strategische und operative Vorteile, die über eine reine Erfüllung der Gesetzgebung hinausgehen. Ein zentraler Vorteil liegt in der nachhaltigen Steigerung der digitalen Resilienz, da sich nun viele Unternehmen in der EU mit Cybersecurity als strategische Führungsaufgabe beschäftigen müssen. Ein wesentlicher ökonomischer Faktor kann dabei die Präventionswirkung sein. Die Ergebnisse der Arbeit unterstreichen, dass Investitionen in die Sicherheit rentabel sind, da sie die Präventionskosten die Reaktionskosten auf Sicherheitsvorfälle massiv reduzieren. Die Implementierung der Risikomanagementmaßnahmen dient dabei als Grundgerüst für die gesamte europäische Lieferkette, indem Ausfälle reduziert und das Wiederanlaufen nach Ausfällen verbessert wird.

Die Compliance eines KMU sichert darüber hinaus eine stabile Position und Wettbewerbsvorteile innerhalb der Lieferkette. Durch die Erfüllung der Vorgaben und den Nachweis der Einhaltung von Standards können die Unternehmen den Verlust von Aufträgen verhindern. Das ergaben vor allem die Gespräche mit den Experten, die vor einem enormen Umsatzverlust bei Nicht-Compliance warnen. Durch die Erfüllung der Schulungsmaßnahmen wird zudem dazu beigetragen, dass bestehende „digitale Kompetenzdefizite“ abgebaut und Führungskräfte befähigt werden, risikobasierte Investitionsentscheidungen zu treffen.

Nicht zuletzt profitieren KMU von einer verbesserten Informationslage und staatlicher Unterstützung, da die neuen Meldewege und -systeme eine schnelle Koordination ermöglichen. Die zentralen Stellen des Bundes dienen in diesem Kontext auch als Anlaufstellen für Unternehmen und stellen die frühzeitige Warnung vor akuten Bedrohungen sicher. Durch die Orientierung am „Stand der Technik“ wird sichergestellt, dass über die gesamte Lieferkette hinaus

angemessene Sicherheitsmaßnahmen ergriffen werden, um die Resilienz vor Ausfällen und Angriffen zu stärken. Dies bietet bei Ausfällen anderer Unternehmen einen zusätzlichen Schutz für die eigene Einrichtung. Dies schützt KMU langfristig und trägt zur Wettbewerbsfähigkeit in einem digitalen Ökosystem bei.

4.3 Beantwortung der Forschungsfrage

Cybersicherheit für KMU nach NIS2 – welche Anforderungen ergeben sich unter Berücksichtigung des ‚Stands der Technik' in den betroffenen Branchen, welche Unterschiede bestehen zwischen ihnen und welche Gemeinsamkeiten lassen sich feststellen?

Die Beantwortung der Forschungsfrage nach den Anforderungen der NIS-2-Richtlinie und der Umsetzung im BSIG n.F. für kleine und mittlere Unternehmen (KMU) lässt sich in drei Kernbereiche unterteilen:

4.3.1 Der „Stand der Technik als Maßstab"

Der „Stand der Technik" fungiert als zentraler unbestimmter Rechtsbegriff für die Angemessenheit der geforderten Risikomanagementmaßnahmen gemäß § 30 BSIG n.F. Er beschreibt den Entwicklungsstand fortschrittlicher Verfahren für Einrichtungen und Betriebsweisen, sowie deren praktische Eignung zum Schutz der Funktionsfähigkeit von IT-Systemen von Beeinträchtigungen nach herrschender Auffassung führender Fachleute und Praktiken. Im Gegensatz zu den anerkannten „Regeln der Technik", die auch Laien bekannt sind, setzt dieser Maßstab Expertenwissen voraus, muss sich aber im Gegenzug zum „Stand der Wissenschaft" bereits in der Praxis bewährt oder zumindest erfolgreich erprobt haben. Der Begriff ist nicht abschließend definiert, sondern als dynamischer und offener Rechtsbegriff angelegt. Für KMU stellt sich daher insbesondere die Frage, wie dieser Maßstab im betrieblichen Alltag konkret zu verstehen und umzusetzen ist.

Die Operationalisierung des Stands der Technik erfolgt dabei primär durch etablierte internationale Frameworks wie die ISO 27001 oder den BSI IT-Grundschutz, die hier konkrete Strukturvorgaben und Maßnahmenkataloge für die Umsetzung bereitstellen. Da der Stand der Technik sich in keiner starren Checkliste abbilden lässt, sondern vielmehr einen kontinuierlichen Prozess darstellt, bildet eine individuelle Strukturanalyse und Schutzbedarfsfeststellung die zwingende Grundlage, um die Verhältnismäßigkeit der umzusetzenden Maßnahmen abzuleiten.

Aus den Interviews geht hervor, dass viele KMU ohne vorherige Berührungspunkte mit Informationssicherheit Schwierigkeiten haben, diesen Maßstab auszulegen. In solchen Fällen wird häufig auf niedrigschwellige Unterstützungsangebote zurückgegriffen - insbesondere der FitNIS2-Navigator wurde mehrfach als hilfreich genannt.

Der Maßstab ist dabei immer im Verhältnis zum Schutzbedarf, zur Kritikalität der IT-Systeme und zu den verfügbaren Ressourcen des Unternehmens zu sehen. Die Experten betonen hier ebenfalls, dass der „Stand der Technik" nicht als Checkliste zu verstehen ist, sondern als Prozess - der regelmäßig überprüft, angepasst und dokumentiert werden muss.

4.3.2 Sektorübergreifende Gemeinsamkeiten

Unabhängig vom jeweiligen Sektor zeigen sich mehrere grundlegende Anforderungen, die für alle betroffenen KMU im Rahmen der NIS-2-Richtlinie gelten. Grundlage ist in allen Fällen ein strukturiertes Informationssicherheitsmanagementsystem (ISMS), das als kontinuierlicher Zyklus nach dem Plan-Do-Check-Act-Prinzip aufgebaut ist. Die Schutzbedarfsfeststellung, Risikoanalyse und Ableitung technischer und organisatorischer Maßnahmen erfolgen darin in festgelegten, wiederkehrenden Prozessen.

Technisch gesehen sind nur wenige Maßnahmen explizit vorgeschrieben, wie unter anderem Backup-Management, Zugangskontrollen (z.B. durch Multi-Faktor-Authentifizierung) und Kryptographie. Die konkrete Auswahl weiterer Maßnahmen ergibt sich aus der individuellen Risikobewertung. Die Interviews zeigen, dass sich in der Praxis ein Konsens über eine Reihe von „Grundschutzmaßnahmen" gebildet hat, die unabhängig von der Branche angewendet werden, z.B. Netzwerksegmentierung, Logging, regelmäßige Patches oder Notfallpläne.

Organisatorisch spielt insbesondere die strategische Einbindung der Geschäftsführung eine zentrale Rolle. Mehrere Experten betonen, dass ein rein technischer Ansatz ohne Managementunterstützung nicht tragfähig sei. Schulungen, Verantwortlichkeitsregelungen, interne Richtlinien und etablierte Meldewege gehören daher zum Pflichtprogramm. Auch die Anbindung an das Risikomanagement des Unternehmens wird als wesentlich eingestuft. Im Ergebnis zeigt sich, dass ein Großteil der Anforderungen branchenübergreifend ist.

4.3.3 Sektorübergreifende Unterschiede

Obwohl der rechtliche Rahmen mit der NIS-2-Richtlinie grundsätzlich einheitlich ist, bestehen in der praktischen Umsetzung erhebliche Unterschiede zwischen den einzelnen Branchen. Diese

lassen sich im Wesentlichen den folgenden drei Bereichen zuordnen: bestehende Regulierungslandschaft, Priorisierung nach den Risiken und Prüfungstiefe.

Branchen wie Energie, Gesundheit und Telekommunikation verfügen meist über bestehende IT-Sicherheitsanforderungen, sei es durch KRITIS-Verordnungen, branchenspezifische Regelwerke oder gesetzlich geregelte Aufsichtspflichten. In diesen Sektoren ist die Umsetzungstiefe deutlich höher, da Unternehmen auf vorhandene Managementsysteme und Prüfungserfahrung zurückgreifen können. Für andere Branchen, wie insbesondere KMU im verarbeitenden Gewerbe oder in der Logistik, stellt die NIS2-Regulierung dagegen eine neue Herausforderung dar. Dort fehlt es oft an Erfahrung, aber auch an strukturellen Grundlagen für ein ISMS.

Ein weiterer wesentlicher Unterschied betrifft die Priorisierung der Schutzziele. Während etwa im Gesundheitsbereich die Vertraulichkeit im Vordergrund steht, hat im Energiesektor die Verfügbarkeit der Systeme höchste Priorität. Dies hat unmittelbare Auswirkungen auf die Ausgestaltung der Sicherheitsmaßnahmen und deren technische Umsetzung.

Auch die Prüf- und Aufsichtsdichte variiert stark. Unternehmen mit bestehender Prüfungserfahrung erwarten eine engmaschige Kontrolle, während weniger regulierte KMU eher mit punktuellen Prüfungen rechnen. Diese Erwartung beeinflusst nicht nur die Motivation zur Umsetzung, sondern auch den Ressourceneinsatz.

Die Interviews machen deutlich, dass viele KMU eine gewisse Unsicherheit im Umgang mit regulatorischen Überschneidungen empfinden. Besonders bei Unternehmen, die bereits anderen Sicherheitsvorgaben unterliegen (z.B. aus der DSGVO oder branchenspezifischen Standards), stellt sich die Frage nach der Abgrenzung und Kompatibilität. Hier besteht ein hoher Bedarf an klarer behördlicher Kommunikation und an praxisnahen Hilfsmitteln zur Harmonisierung bestehender Systeme mit neuen Anforderungen.

5 Ausblick

Da die Definition der Risikomanagementmaßnahmen sich an der Angemessenheit und dem „Stand der Technik“ orientiert und diesen Maßnahmen somit einen dynamischer Begriff zugrunde liegt, der durch den technologischen Fortschritt und aktuelle Bedrohungen kontinuierlich vorangetrieben wird, müssen die Unternehmen ihre Cybersecurity-Strategie regelmäßig neu bewerten.

Die regulatorische Landschaft innerhalb der EU wird sich weiter verdichten. Zukünftige Untersuchungen sollten sich daher inhaltlich stärker mit der Wechselwirkung mit neuen Verordnungen wie dem C wie dem Cyber Resilience Act (CRA), dem AI Act oder dem Data beschäftigen. Hier sollte weiter der Fokus auf einer einheitlichen Anwendbarkeit und Operabilität der Maßnahmen für die KMU liegen. Ohne eine Vereinheitlichung und einer rein theoretischen Richtlinie wird es für Unternehmen eine enorme Herausforderung, alle Rechtsakte erfolgreich umzusetzen.

Besonders für KMU wird im verarbeitenden Gewerbe die Absicherung vernetzter Produkte über den gesamten Lebenszyklus hinweg eine zentrale Herausforderung bleiben. Ein weiterer kritischer Faktor bleibt die Bewältigung des Fachkräftemangels in den Unternehmen im Bereich der Cybersecurity. Zukünftige Forschung sollte Untersuchen, inwieweit Managed Security Service Provide (MSSP) oder automatisierte KI-gestützte Sicherheitssysteme die personellen Engpässe in KMU effektiv kompensieren können, ohne zu große Abhängigkeiten innerhalb der eigenen Lieferkette zu schaffen.

Bei der persönlichen Haftung für die Geschäftsleitungen bleibt abzuwarten, wie sich das auf die Unternehmenskultur auswirken wird. Hier können zukünftige Studien untersuchen, ob die verpflichtenden Schulungen tatsächlich zu einer nachhaltigen Reduzierung digitaler Kompetenzdefizite führen oder ob die Umsetzung ein weiterer primär formeller bürokratischer Akt bleibt.

Die im Rahmen dieser erarbeiteten Controls bilden eine fundierte Basis für die Weiterentwicklung des FitNIS2-Navigators. Die formulierten Maßnahmen können Unternehmen kostenfrei nutzen, um ein besseres Verständnis für die umzusetzenden Maßnahmen zu bekommen. Die verständlich formulierten Handlungsmaßnahmen liefern zusätzliche Informationen für betroffene KMU.