ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Entwicklung eines praxisnahen ISMS-Frameworks für KMUs im Einklang mit der NIS2-Richtlinie

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieurin

eingereicht von

Cornelia Mayer, BSc

is221802

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: Dipl.-Ing. Lukas König, BSc

Mitwirkung: -

Ehrenwörtliche Erklärung

Titel: Entwicklung eines praxisnahen ISMS-Frameworks für KMUs im Einklang mit der NIS2-Richtlinie

Art der Arbeit: Diplomarbeit

Autor: Cornelia Mayer, BSc

Matrikelnummer: is221802

Ich versichere, dass

- ich diese Arbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich das Thema dieser Arbeit bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Ich erkläre hiermit, dass

☒ ich ein Large Language Model (LLM) verwendet habe, um die Arbeit Korrektur zu lesen.

☐ ich ein Large Language Model (LLM) verwendet habe, um Teile des Inhalts der Arbeit zu erstellen. Ich versichere, dass ich jeden generierten Satz/Absatz mit der Originalquelle zitiert habe. Das genutzte LLM ist an entsprechenden Stellen durch eine Fußnote ausgewiesen.

☐ im Zuge dieser Arbeit kein Large Language Model (LLM) zum Einsatz gekommen ist.

Ort, Datum *Unterschrift*

Kurzfassung

Mit der NIS2-Richtlinie der Europäischen Union sowie dem in Österreich geplanten Netz- und Informationssystemsicherheitsgesetz 2024 ("NISG 2024") werden erstmals auch kleine und mittlere Unternehmen (KMUs) in kritischen oder wirtschaftlich relevanten Sektoren dazu verpflichtet, ein Mindestniveau an Cybersicherheit umzusetzen. KMUs verfügen häufig weder über eigene IT-Sicherheitsabteilungen noch über systematische Managementprozesse. Die 13 Themenbereiche des NISG 2024 benennen Handlungsfelder, enthalten jedoch keine konkreten Anforderungen. Viele KMUs wissen daher nicht, wie sie die Vorgaben strukturiert umsetzen können.

Im Rahmen dieser Arbeit wurde ein praxisorientiertes Rahmenwerk für ein Informationssicherheitsmanagementsystem (ISMS) entwickelt, das auf die Bedürfnisse österreichischer KMUs zugeschnitten ist. Ziel war es, ein Framework zu entwerfen, das sowohl die gesetzlichen Anforderungen aus Art. 21 Abs. 2 der NIS2-Richtlinie als auch die thematischen Vorgaben der nationalen Gesetzgebung abdeckt. Zu diesem Zweck wurde der aktuelle Reifegrad der Cybersicherheit von KMUs in der EU und in Österreich untersucht. Anhand der 13 Themenbereiche des NISG 2024 wurde eine Struktur erstellt und die Anforderungen der NIS2-Durchführungsverordnung sowie der NIS2-Richtlinie analysiert, verglichen und systematisch einander zugeordnet. Mithilfe eines methodischen Vorgehens wurden auf Basis des Anforderungsmappings konkrete Maßnahmen und beispielhafte Nachweise abgeleitet, Fragestellungen für eine Gap-Analyse definiert sowie die Entwicklung von Umsetzungshilfen, Vorlagen und einer beispielhaften Roadmap für die priorisierte Umsetzung der Maßnahmen erarbeitet.

Die Praxistauglichkeit des entwickelten Frameworks wurde im Rahmen einer qualitativen Validierung durch zwei Fachpersonen aus verschiedenen Bereichen der Informationssicherheit überprüft. Dabei zeigte sich, dass der Aufbau, die klare Strukturierung entlang der NISG 2024 Themenbereiche sowie die praxisnahen Umsetzungshilfen als besonders hilfreich bewertet wurden. Durch die Ergebnisse dieser Arbeit liegt ein konkreter Ansatz vor, wie KMUs die gesetzlichen Anforderungen aus NIS2 und NISG 2024 schrittweise umsetzen können, ohne dabei überfordert zu werden. Gleichzeitig trägt das entwickelte Framework dazu bei, das Sicherheitsniveau der KMUs nachhaltig zu erhöhen und ihre organisatorische Resilienz gegenüber Cyberrisiken zu stärken.

Abstract

With the introduction of the EU Directive 2022/2555 (“NIS2”) and the forthcoming Austrian Network and Information System Security Act 2024 (“NISG 2024”), small and medium-sized enterprises (SMEs) operating in critical or economically relevant sectors will, for the first time, be required to implement a minimum level of cybersecurity. Many SMEs, however, lack dedicated IT security departments and established management processes. While the 13 thematic areas defined in Annex 3 of the NISG 2024 outline general areas of action, they do not provide specific implementation requirements. As a result, many SMEs are uncertain about how to translate these obligations into practical measures.

This thesis develops a practice-oriented framework for an Information Security Management System (ISMS) tailored to the needs of Austrian SMEs. The aim was to create a framework that addresses both the legal obligations outlined in Article 21(2) of the NIS2 Directive and the thematic structure of the national legislation. To this end, the current cybersecurity maturity level of SMEs in Austria and the EU was examined, and the sector-specific challenges they face were identified. A structured ISMS framework was designed based on the 13 thematic areas of the NISG 2024. The regulatory requirements from the NIS2 Directive and the corresponding implementing regulation were analysed, compared and systematically mapped. Using a structured methodological approach, concrete security measures and sample evidence were derived, questions for a gap analysis were formulated, and practical tools such as implementation templates and a prioritised roadmap were developed.

The applicability of the framework was assessed through a qualitative validation involving two subject matter experts from the field of information security. The results indicate that the modular structure, the alignment with the 13 NISG 2024 areas, and the practical implementation aids were considered particularly helpful. This work provides a concrete approach to support SMEs in gradually fulfilling their legal obligations under NIS2 and NISG 2024. In doing so, the proposed framework contributes to raising the overall cybersecurity level of SMEs and strengthening their organisational resilience against cyber risks.

Inhaltsverzeichnis

1 Einleitung

Die fortschreitende Digitalisierung durchdringt zunehmend auch traditionell IT-ferne Branchen. Parallel dazu nimmt die Zahl gezielter Cyberangriffe auf kleine und mittlere Unternehmen (KMUs) deutlich zu. Diese Unternehmen verfügen häufig nicht über ausreichendes Fachpersonal, Budget oder strukturierte Sicherheitsprozesse, um adäquat auf Bedrohungen zu reagieren. Eine ENISA-Erhebung [1, p. 3] zeigt, dass rund 80% der befragten KMUs einen schwerwiegenden Cybervorfall binnen einer Woche als existenzbedrohend einstufen und dabei ihr tatsächliches Risiko signifikant unterschätzen.

Mit der Richtlinie (EU) 2022/2555 („NIS2“) führt die Europäische Union erstmals ein harmonisiertes und sanktionsbewehrtes Mindestniveau für Cybersicherheit ein. Der Geltungsbereich umfasst nun auch zahlreiche KMUs in kritischen oder wirtschaftlich relevanten Sektoren. Für wesentliche Einrichtungen drohen Bußgelder bis zu 10 Millionen Euro bzw. 2% des Jahresumsatzes; für wichtige Einrichtungen bis zu 7 Millionen Euro bzw. 1,4% des Umsatzes. [2, p. 60] In Österreich erfolgt die nationale Umsetzung durch das Netz- und Informationssystemsicherheitsgesetz 2024 („NISG 2024“), das sich derzeit im Gesetzgebungsverfahren befindet. Der aktuelle Entwurf konkretisiert die Anforderungen jedoch lediglich durch thematische Oberbegriffe in Anlage 3, ohne verbindliche Detailvorgaben.

1.1 Motivation und Problemstellung

Österreichische KMUs stehen damit vor einem regulatorischen Wandel, dessen konkrete Anforderungen zwar absehbar, in der Umsetzung jedoch vielfach unklar bleiben. Das NISG 2024 verpflichtet die oberste Leitungsebene zur Umsetzung geeigneter und verhältnismäßiger Sicherheitsmaßnahmen sowie zur Einhaltung eines dreistufigen Meldeverfahrens. Gleichzeitig nennt die Gesetzesvorlage keine operationalisierbaren Mindeststandards. Die EU-weite Umsetzungsfrist endete am 17. Oktober 2024, ein nationaler Beschluss steht derzeit noch aus. [3] Vor diesem Hintergrund ergibt sich für österreichische KMUs ein doppeltes Dilemma, da sie einerseits den regulatorischen Anforderungen nachkommen müssen, deren Ausgestaltung noch nicht abschließend definiert ist und andererseits verfügen viele dieser Unternehmen über nur begrenzte

Ressourcen. Ein vereinfachtes und praxisnahes Informationssicherheitsmanagementsystem (ISMS) wird daher nicht nur zur Erfüllung der gesetzlichen Vorgaben, sondern auch zur Absicherung der eigenen Resilienz im digitalen Raum unternehmerischen Notwendigkeit.

1.2 Zielsetzung und Forschungsfrage

Ziel dieser Arbeit ist die Entwicklung eines praxisnahen ISMS-Frameworks, welches sich an den Anforderungen der NIS2-Richtlinie orientiert und explizit auf die Bedürfnisse österreichischer KMUs zugeschnitten ist. Das Framework soll auf den 13 Themenbereichen der Anlage 3 des geplanten NISG 2024 basieren und dabei sämtliche in Artikel 21 Absatz 2 der NIS2-Richtlinie definierten Mindestanforderungen abdecken. [2, p. 48], [4]

Die zentrale Forschungsfrage dieser Arbeit lautet daher:
„Wie kann ein auf den 13 Themenbereichen der Anlage 3 NISG 2024 basierendes ISMS-Framework für österreichische KMUs gestaltet werden, sodass es sämtliche in Artikel 21 Absatz 2 der NIS2-Richtlinie genannten Mindestanforderungen abdeckt?“

Zur Beantwortung dieser Frage werden regulatorische Vorgaben analysiert, bestehende ISMS-Ansätze bewertet und ein methodisch fundiertes Framework entwickelt, welches durch praktische Umsetzungshilfen wie Vorlagen, Gap-Analyse und einen priorisierten Fahrplan ergänzt wird.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in acht Kapitel, die systematisch aufeinander aufbauen und den gesamten Forschungsprozess von der Problemstellung bis zur Evaluation des entwickelten Frameworks abdecken. Die Struktur ermöglicht es, das Thema umfassend zu analysieren und praxisnahe Lösungen zu präsentieren.

- **Einleitung**: Die Einleitung (referenziert als Kapitel 1) gibt einen Überblick über das Thema ISMS-Framework für KMUs mit Fokus auf NIS2, die Motivation und Problemstellung, die Zielsetzung und Forschungsfrage sowie den Umfang der Arbeit.
- **Grundlagen**: Dieses Kapitel (referenziert als Kapitel 2) stellt die rechtlichen Grundlagen (NIS2, NISG 2024, NIS2-Durchführungsverordnung) sowie Hintergrundinformationen zu einem ISMS dar. Zudem werden auch die aktuellen Reifegrade sowie Herausforderungen von KMUs in der EU sowie in Österreich untersucht und thematisiert.

- **Stand der Forschung**: In diesem Teil (referenziert als Kapitel 3) werden ähnliche Arbeiten sowie bestehende Forschungen und Literatur zu ISMS-Frameworks für KMUs vorgestellt.
- **Methodisches Vorgehen**: Dieses Kapitel (referenziert als Kapitel 4) beschreibt das methodische Vorgehen, insbesondere das Anforderungs-Mapping, die Maßnahmenermittlung, die Gap-Analyse und die Entwicklung der Vorlagen.
- **Inhalt und Ausarbeitung des Frameworks**: In diesem Abschnitt (referenziert als Kapitel 5) wird das fertige Framework strukturiert anhand der 13 Themenbereiche des NISG 2024 inklusive Umsetzungen, Vorlagen und einem holistischen Fahrplan zur priorisierten Umsetzung präsentiert.
- **Validierung des entwickelten Frameworks**: Dieser Abschnitt (referenziert als Kapitel 6) zeigt die Ergebnisse der Validierung des entwickelten Frameworks der externen Fachpersonen.
- **Diskussion**: Dieses Kapitel (referenziert als Kapitel 7) dokumentiert die Erkenntnisse der Validierung sowie Selbstreflexion, ordnet diese kritisch ein und identifiziert Verbesserungspotenziale.
- **Conclusio**: Zum Schluss wird das Fazit gezogen, die Forschungsfrage beantwortet und ein Ausblick auf künftige Arbeiten gegeben. (referenziert als Kapitel 8)

1.4 Abgrenzung der Arbeit

Diese Arbeit fokussiert sich auf die Entwicklung eines ISMS-Frameworks mit Fokus auf NIS2 für KMUs in Österreich. Um die Zielsetzung der Arbeit klar abzugrenzen, werden jedoch einige Bereiche bewusst nicht im Detail behandelt:

- **Geografischer Fokus**: Die Analyse beschränkt sich auf das österreichische NISG 2024 und dessen Bezüge zur NIS2-Richtlinie. Andere nationale Umsetzungen bleiben unberücksichtigt.
- **Zielgruppe**: Betrachtet werden ausschließlich KMUs gemäß Empfehlung 2003/361/EG mit höchstens 250 Mitarbeitenden. [5, p. 4]
- **Normativer Umfang**: Es werden nur die in Art. 21 Abs. 2 NIS2 genannten Mindestmaßnahmen sowie die Anforderungen gemäß NIS2-Durchührungsverordnung behandelt.
- **Technische Tiefe**: Die Arbeit liefert organisatorische und prozessuale Leitlinien. Tiefgreifende Implementierungsdetails einzelner Sicherheitstechnologien werden nicht ausgearbeitet.
- **Zeitlicher Rahmen**: Rechtsentwicklungen nach dem 7. Mai 2025 werden nicht mehr berücksichtigt.
- **Regulatorische Konformität**: Es handelt sich bei dieser Arbeit um eine wissenschaftliche Ausarbeitung ohne Rechtsverbindlichkeit und ersetzt somit keine juristische Beratung.
- **Dokumentenbasis**: Ein ausgewählter Satz relevanter Vorlagen- und Beispieldokumenten wird im

Rahmen der Arbeit ausgearbeitet und decken einen Teil der potenzielle erforderlichen Nachweise ab. Die Dokumente dienen lediglich als Basis und müssen an die individuellen Gegebenheiten des jeweiligen KMUs angepasst werden.

2 Grundlagen

Die zunehmende Digitalisierung wirtschaftlicher Prozesse sowie die wachsende Bedrohungslage im Cyberraum führen dazu, dass Informationssicherheit nicht länger als optionales Randthema betrachtet werden kann. Insbesondere KMUs rücken hierbei zunehmend in den Fokus regulatorischer Vorgaben. Um den Anforderungen aus NIS2 und deren nationaler Umsetzung wirksam begegnen zu können, bedarf es eines fundierten Verständnisses der zugrunde liegenden rechtlichen, normativen und methodischen Rahmenbedingungen. Ziel dieses Kapitels ist es daher, die regulatorischen Anforderungen, welche sich aus der NIS2-Richtlinie und ihrer Umsetzung in Österreich ergeben, sowie die grundlegenden Konzepte und Standards eines ISMS systematisch darzustellen. Diese Elemente bilden die fachliche Grundlage für die spätere Entwicklung eines ISMS-Frameworks, welches den spezifischen Herausforderungen und Ressourcenlagen von KMUs gerecht werden soll.

2.1 Regulatorischer Rahmen

Die regulatorischen Entwicklungen im Bereich der Cybersicherheit bilden das Fundament für unternehmensinterne Maßnahmen. Für Organisationen und insbesondere KMUs ergeben sich daraus neue rechtliche Verpflichtungen, die strukturiert und nachhaltig erfüllt werden müssen. Ziel dieses Abschnitts ist es, die zentralen Elemente der NIS2-Richtlinie sowie deren nationale Umsetzung in Österreich darzustellen, um im Anschluss die Ableitung konkreter Anforderungen für ein ISMS vornehmen zu können.

2.1.1 EU-Vorgaben: Die NIS2-Richtlinie im Überblick

Die NIS2-Richtlinie verfolgt das Ziel, das Cybersicherheitsniveau innerhalb der Europäischen Union durch eine stärkere Vereinheitlichung nationaler Vorschriften sowie eine Ausweitung des Geltungsbereichs zu verbessern. [2]

Strukturell gliedert sich die Richtlinie [2] in:

- **Nationale Strategien (Art. 7)**: Die Mitgliedstaaten sind verpflichtet, umfassende Cybersicherheitspläne zu entwickeln, die auch grenzüberschreitende Aspekte berücksichtigen.
- **Institutionelle Architektur (Art. 8-10)**: Hierzu zählen der Aufbau von Computer-Notfallteams (CERTs), zentrale Kontaktstellen sowie zuständige Aufsichtsbehörden.
- **Risikomanagementpflichten (Art. 21)**: Betroffene Einrichtungen müssen konkrete technische und organisatorische Schutzmaßnahmen umsetzen.
- **Meldeverfahren (Art. 23)**: Die Richtlinie definiert Fristen für die Meldung von Sicherheitsvorfällen, eine erste Meldung binnen 24 Stunden, eine vollständige nach spätestens 72 Stunden.

Ein wesentlicher Unterschied zur vorherigen NIS1-Richtlinie (2016/1148/EU) [6] besteht in der neuen Kategorisierung betroffener Organisationen. Die detaillierten Unterschiede zwischen NIS1 und NIS2 hinsichtlich des Geltungsbereichs, der Meldepflichten und des Sanktionsrahmens sind in der nachfolgenden Tabelle 2.1 zusammengestellt.

Kriterium	**NIS1 [6]**	**NIS2 [2]**
Sektoren / Geltungsbereich	7 kritische Sektoren + digitale Dienstanbieter (Cloud, Online-Marktplatz, Suchmaschine).	Zwei Kategorien von Einrichtungen: • Wesentliche (Annex I: Energie, Transport, Bankwesen etc.) • Wichtige (Annex II: Post, Abfall, Lebensmittel, Chemie, Raumfahrt, Manufacturing)
Meldefristen für Sicherheitsvorfälle	Pflicht zur Meldung ohne unangemessene Verzögerung; keine EU-weit definierte Stundenfrist.	Dreistufiges Meldeschema: • Frühwarnung $\leq$ 24 h (Initial) • Incident Notification $\leq$ 72 h (Intermediate) • Finaler Bericht $\leq$ 1 Monat (Final)

Kriterium	NIS1 [6]	NIS2 [2]
Sanktionen / Bußgelder	Von Mitgliedstaaten festgelegt. Beispiel Österreich (NISG 2018): max. 50.000 €	Harmonisiertes Bußgeldregime: • Wesentliche Einrichtungen: bis 10 Mio. € oder 2% des weltweiten Jahresumsatzes • Wichtige Einrichtungen: bis 7 Mio. € oder 1,4% des Umsatzes

Tabelle 2.1: Vergleich der Anforderungen nach NIS1 und NIS2

Ein weiteres zentrales Element ist die Absenkung der Größenanforderungen: Künftig werden auch KMUs erfasst, sofern sie in sicherheitskritischen oder wirtschaftlich bedeutenden Bereichen tätig sind. Damit soll die zunehmende systemische Abhängigkeit von KMUs in digitalen Lieferketten berücksichtigt und deren Schutzstandard erhöht werden. [7]

Die NIS2 unterscheidet zwei Aufsichtskategorien, die sich primär aus Sektorzugehörigkeit (Annex I bzw. II) und Unternehmensgröße, mindestens mittleres Unternehmen nach Empfehlung 2003/361/EG, ergeben. Ein Unternehmen gilt als mittleres Unternehmen, wenn mindestens 50 Mitarbeitende dort beschäftigt sind oder ein Jahresumsatz von über zehn Millionen Euro erzielt wird und sich die Jahresbilanzsumme auf über zehn Millionen Euro beläuft. [8] Abhängig von den Sektoren wird dann bestimmt, ob es sich um wesentliche oder wichtige Einrichtungen handelt. Um die abstrakten Einstufungskriterien greifbar zu machen, illustriert Tabelle 2.2 anhand je eines österreichischen KMU die praktische Zuordnung zu „wesentlichen“ bzw. „wichtigen“ Einrichtungen.

Kategorie	Definition nach NIS2	Beispiel KMU	Begründung
Wesentliche Einrichtung	Mittlere oder Große Unternehmen in einem Annex-I-Sektor (Energie, Transport, Gesundheit, ...); unterliegt präventiver und nachträglicher Aufsicht (Art. 32 NIS2). [2, pp. 56-58]	Regionale Trinkwasser Versorgungs GmbH mit 85 MA und 15 Mio. € Umsatz	• Sektor „Trinkwasser“ ist Annex I, Nr. 6. [2, pp. 64-67] • Unternehmensgröße $\geq$ 50 MA & $\geq$ 10 Mio. € Umsatz $\rightarrow$ Mittleres Unternehmen. • Versorgungskritische Dienstleistung $\rightarrow$ hohe Systemrelevanz.
Wichtige Einrichtung	Mittlere oder Große Unternehmen in einem Annex-II-Sektor (Post & Kurier, Abfall, Lebensmittel, Chemie, Manufacturing, ...); unterliegt nur nachträglicher Aufsicht (Art. 33 NIS2). [2, pp. 58-60]	Molkerei Genossenschaft Alpenfrisch eGen mit 120 MA und 28 Mio. € Umsatz	• Sektor „Produktion, Verarbeitung und Vertrieb von Lebensmitteln“ ist Annex II, Nr. 4. [2, pp. 69-70] • Größenschwelle erfüllt • Lebensmittelverarbeitung trägt zur „örtlichen Grundversorgung“ bei, jedoch ohne kritische Infrastrukturmerkmale $\rightarrow$ Kategorie „wichtig“.

Tabelle 2.2: Definition wesentliche und wichtige Einrichtung

Daraus ergibt sich die Implikation: Beide Unternehmen müssen sämtliche Sicherheitsmaßnahmen des Art. 21 erfüllen; jedoch unterliegen nur „wesentliche Einrichtungen“ der präventiven Audit-Aufsicht und können mit höheren Bußgeldobergrenzen belegt werden (bis 10 Mio. € / 2 % Umsatz).

2.1.2 Nationale Umsetzung in Österreich: Das NISG 2024

Die Implementierung der NIS2-Richtlinie in Österreich erfolgt durch das geplante Netz- und Informationssystemsicherheitsgesetz 2024 („NISG 2024“). Derzeit befindet sich dieses im Gesetzgebungsverfahren. Ein erster Entwurf wurde dem Nationalrat vorgelegt, erreichte jedoch nicht die erforderliche Zweidrittelmehrheit. Ein Inkrafttreten wird daher frühestens im Laufe des Jahres 2025 erwartet. [3] Die ursprüngliche Umsetzungsfrist auf EU-Ebene endete bereits am 17. Oktober 2024. [2, p. 63] Der österreichische Gesetzesentwurf lehnt sich eng an die Vorgaben der EU-Richtlinie an und übernimmt deren wesentliche Anforderungen. Die zuständige Aufsichtsbehörde soll gemäß §4 das Bundesministerium für Inneres sein. Die Einstufung erfolgt unter Berücksichtigung von Unternehmensgröße (§§ 25, 26) sowie Zugehörigkeit zu bestimmten Sektoren gemäß Anlagen 1 und 2. [9]

Gemäß § 29 haben betroffene Einrichtungen in Österreich binnen drei Monaten nach Inkrafttreten des NISG 2024 eine Registrierung vorzunehmen. In Bezug auf die Steuerung sehen § 31 und § 32 vor, dass Leitungsorgane aktiv für die Umsetzung von Sicherheitsmaßnahmen verantwortlich sind, an Schulungen teilnehmen müssen und für die Weiterbildung der Mitarbeitenden Sorge zu tragen haben. Ein zweistufiger Nachweis der Umsetzung ist in § 33 geregelt: Zunächst erfolgt eine Selbstdeklaration innerhalb von sechs Monaten nach Aufforderung durch die Behörde; bei wesentlichen Einrichtungen ist zusätzlich eine regelmäßige externe Prüfung durch unabhängige Stellen vorgesehen (alle drei Jahre). Sicherheitsvorfälle sind nach § 34 über ein dreistufiges Meldeverfahren zu berichten: eine Frühwarnung binnen 24 Stunden, eine detaillierte Meldung innerhalb von 72 Stunden sowie ein Abschlussbericht innerhalb eines Monats. Zur Durchsetzung sieht § 45 hohe Bußgelder vor: Für wichtige Einrichtungen sind Sanktionen bis zu 7 Mio. € oder 1,4% des Jahresumsatzes möglich; bei wesentlichen Einrichtungen kann die Strafe bis zu 10 Mio. € oder 2% des Umsatzes betragen. [9, p. 30]

Eine tatsächliche Auflistung von geforderten Anforderungen zu Sicherheitsmaßnahmen ist im österreichischen Gesetzesentwurf nicht zu finden. Es wird laut §32 (1) darauf verwiesen, dass Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen in den Bereichen der Anlage 3 [4] umzusetzen haben. Anlage 3 listet 13 Bereiche auf, darunter befinden sich unter anderem folgende:

- 1.a. Rollen und Verantwortlichkeiten der Leitungsorgane
- 2.a. Sicherheitsleitlinien
- 3.a. Risikomanagementrichtlinie und -prozess

- 7.b. Lieferantenverzeichnis

2.1.3 NIS2-Durchführungsverordnung (EU)

Die Durchführungsverordnung (EU) 2024/2690 [10] wurde am 17. Oktober 2024 angenommen und am 18. Oktober 2024 im Amtsblatt veröffentlicht. Sie gilt seit 7. November 2024 unmittelbar in allen Mitgliedstaaten für folgende Einrichtungen:

- DNS-Diensteanbieter
- TLD-Namenregister
- Anbieter von Cloud-Computing-Diensten
- Anbieter von Rechenzentrumsdiensten
- Betreiber von Inhaltszustellnetzen
- Anbieter verwalteter Dienste
- Anbieter verwalteter Sicherheitsdienste
- Anbieter von Online-Marktplätzen
- Online-Suchmaschinen
- Plattformen für Dienste sozialer Netzwerke
- Vertrauensdiensteanbieter

Ihr Zweck ist die Festlegung der technischen und methodischen Anforderungen zu den in Art. 21 Abs. 2 NIS2 aufgeführten Risikomanagement-Maßnahmen sowie die Präzisierung, wann ein Vorfall als „signifikant“ gilt. [2, pp. 49-51] Der Annex 1 der Verordnung spiegelt die 13 Buchstabenpunkte des Art. 21 Abs. 2 der NIS2-Richtlinie wider. Jedes Kapitel enthält konkrete Vorgaben, welche beispielhaft in der folgenden Tabelle 2.3 inklusive der Zuordnung zu NIS2 dargestellt sind.

Kapitel im Anhang der Verordnung	**Referenz zu NIS2-Richtlinie**	**Domäne**	**Auszug aus den Vorgaben**
5	7 Artikel 21 Abs. 2 (d)	Lieferkettensicherheit	Verfahren zur Bewertung der Kritikalität von Drittanbietern in Bezug auf die sicherheitsrelevanten Auswirkungen.

Kapitel im Anhang der Verordnung	Referenz zu NIS2-Richtlinie	Domäne	Auszug aus den Vorgaben
11	Artikel 21 Abs. 2 (d)	Zugriffsmanagement	Multi-Faktor-Authentifizierung je nach Schutzbedarf der sicherheitsrelevanten Assets.
12	7 Artikel 21 Abs. 2 (i)	Asset-Management	Vollständiges, versionsgeführtes Inventar aller sicherheitsrelevanten Assets.

Tabelle 2.3: Auszugsweise Zuordnung der Kapitel der Durchführungsverordnung zur NIS2-Richtlinie

Damit liefert die Verordnung einen prüfbaren Maßnahmenkatalog für Unternehmen, welcher vergleichbar mit Annex A der ISO/IEC 27001 ist. Obwohl die NIS2-Durchführungsverordnung nicht für KMUs gilt, ist es ratsam, sich bis zur Veröffentlichung des NISG 2024 an den Anforderungen der Durchführungsverordnung zu orientieren. So kann sichergestellt werden, dass die erstmalige Erstellung oder Erweiterung von Sicherheitsmaßnahmen in die richtige Richtung geht. In den Erwägungsgründen der Verordnung wird unter (4) [10, p. 1] in Bezug auf Proportionalität zudem klargestellt, dass betroffene Einrichtungen bei Ressourcenknappheit äquivalente Kompensationsmaßnahmen wählen dürfen, sofern die Schutzwirkung vergleichbar ist (z.B. Management-Oversight statt strikter Funktionstrennung in Kleinstunternehmen). Dies eröffnet KMUs einen legitimen Spielraum für maßgeschneiderte Sicherheitsmaßnahmen.

2.1.4 ENISA-Implementation Leitfaden zur NIS2-Durchführungsverordnung (EU)

Die Europäische Union-Agentur für Cybersicherheit (ENISA) hat parallel zur Durchführungsverordnung (EU) 2024/2690 den Entwurf „Implementation Guidance on Security Measures“ [11] im Oktober 2024 vorgelegt. Der finale Leitfaden wir im Laufe des dritten Quartals 2025 erwartet. Das Dokument verfolgt das Ziel, die im Annex der Durchführungsverordnung beschriebenen 13 Risikomanagement-Bereiche in handlungsorientierte Empfehlungen zu überführen und damit sowohl Aufsichtsbehörden als auch betroffenen Einrichtungen eine praxistaugliche Auslegungshilfe zu bieten.

Obwohl der Leitfaden keine Rechtsverbindlichkeit besitzt, stuft die NIS-Kooperationsgruppe sie im Vorwort als „common baseline for supervisory activities“ ein. Damit könnte sie faktisch als Audit-Leitfaden für

die Aufsichtsbehörden der Mitgliedstaaten verwendet werden. Unternehmen, welche ihre Maßnahmen an diesem Leitfaden ausrichten, können plausibel darlegen, dass sie den „Stand der Technik“ (Art. 21 Abs. 1 NIS2) erfüllen.

Jedes Kapitel folgt einer dreistufigen Struktur:

- **„Requirement“-Kurztext** (wörtliche Übernahme aus der Verordnung)
- **„Guidance“** erläuternde Umsetzungstipps (z.B. Frequenz der Maßnahme, Tools, etc.)
- **„Example of Evidence“** konkret akzeptierte Nachweise (z.B. Change-Log des Firewall-Rule-Sets, Protokolle zu Management-Freigaben, etc.)

Diese Systematik übersetzt hiermit für betroffene Unternehmen abstrakte Pflichten der NIS2 sowie der Verordnung in prüfbare Kontrollpunkte. Zusätzlich stellt ENISA zu jedem Annex-Bereich eine Mapping-Tabelle bereit, welche unter anderem ISO/IEC 27001 Annex A, NIST CSF sowie branchenspezifische und nationale Rahmenwerke in Bezug auf Informationssicherheit abbildet. Der ENISA-Leitfaden dient im Rahmen dieser Arbeit als zentrale Interpretationshilfe (siehe Kapitel 4.1). Insbesondere die Guidance sowie die beispielhaften Nachweise wurden hierbei berücksichtigt, um die abstrakten Anforderungen aus der Verordnung in konkretere und einfachere Maßnahmen für KMUs zu überführen.

2.2 Informationssicherheitsmanagementsystem (ISMS) als methodischer Rahmen

Die zuvor dargestellten regulatorischen Anforderungen, insbesondere im Kontext der NIS2-Richtlinie und ihrer nationalen Umsetzung durch das NISG 2024, setzen ein strukturiertes und nachvollziehbares Vorgehen zur Absicherung informationstechnologischer Systeme voraus. Um diesen Anforderungen systematisch begegnen zu können, bedarf es eines methodischen Rahmens, der die Informationssicherheit in den betrieblichen Alltag integriert, kontinuierlich überprüft und fortlaufend verbessert. Ein ISMS stellt dabei das zentrale Instrument dar, um die organisatorischen, technischen und rechtlichen Vorgaben wirksam umzusetzen. Es bildet die Grundlage dafür, Risiken systematisch zu identifizieren, angemessen zu bewerten und durch geeignete Maßnahmen zu beherrschen. Darüber hinaus ermöglicht ein ISMS die nachhaltige Verankerung von Sicherheitskultur und Verantwortungsbewusstsein auf allen Ebenen der Organisation. Im Folgenden werden die Grundprinzipien, Ziele sowie internationale Standards eines ISMS näher erläutert, um die Rolle des ISMS als zentrales Element der operativen Umsetzung von Cybersicherheitsanforderungen herauszuarbei-

ten.

2.2.1 Definition und Ziel eines ISMS

Ein Informationssicherheitsmanagementsystem oder englisch „Information Security Management System“ ist ein Satz von Richtlinien, Verfahren und Methoden, die von der Leitung einer Organisation verwendet werden, um die Informationssicherheit in den täglichen Aktivitäten zu schützen. Die Implementierung eines ISMS basiert auf einer umfassenden Risikobewertung sowie der Festlegung akzeptabler Risikoniveaus, um Bedrohungen und Schwachstellen zu verwalten. Das Hauptziel eines ISMS besteht darin, die Vertraulichkeit, Integrität und Verfügbarkeit („CIA-Triade“) der Daten vor unbefugtem Zugriff zu schützen. Die Relevanz eines ISMS variiert je nach Organisationstyp. Nach Hamdi et al. [12, pp. 2-3] wird es als wesentlicher Bestandteil jeder Organisation angesehen, da es die Sicherheit und das Vertrauen der interessierten Parteien gewährleistet, auch wenn die Motivation zur Implementierung zwischen den Branchen unterschiedlich ist.

Die ISO/IEC 27001:2022 [13] definiert die internationalen Anforderungen an ein ISMS. Sie beschreibt, wie ein ISMS geplant, eingeführt, betrieben, überwacht, überprüft, aufrechterhalten und kontinuierlich verbessert werden sollte. Dabei wird betont, dass ein ISMS nicht isoliert als technisches System betrachtet werden darf, sondern integraler Bestandteil der gesamten Organisationsprozesse sein muss. Die Norm hebt hervor, dass das ISMS an die spezifischen Bedürfnisse, Ziele und Rahmenbedingungen der Organisation angepasst werden sollte, um effektiv zu sein. [13, pp. 3-4]

2.2.2 Die Grundprinzipien eines ISMS

Die Umsetzung eines ISMS folgt bewährten Prinzipien und etablierten Modellen. Im Kern basiert ein ISMS auf dem Plan-Do-Check-Act (PDCA)-Zyklus [12, pp. 2-3], der vier Phasen umfasst:

1. **Plan (Planung):** Analyse der Rahmenbedingungen, Festlegung der Sicherheitsziele und Entwicklung einer Sicherheitsstrategie.
2. **Do (Umsetzung):** Implementierung der Sicherheitsmaßnahmen gemäß der entwickelten Strategie.
3. **Check (Überprüfung):** Überwachung und Bewertung der Wirksamkeit der umgesetzten Maßnahmen.
4. **Act (Verbesserung):** Beseitigung erkannter Schwachstellen, Anpassung und Optimierung der Maßnahmen.

Dieses zyklische Modell verdeutlicht, dass Informationssicherheit ein kontinuierlicher Prozess ist, der regelmäßige Anpassungen an neue interne und externe Herausforderungen erfordert. Dies kann technologische Fortschritte, gesetzliche Änderungen oder die Entwicklung neuer Bedrohungen umfassen. Zusätzlich zu diesem allgemeinen Rahmen identifiziert der BSI-Standard 200-1 [14] die folgenden zentralen Komponenten eines ISMS:

- **Managementprinzipien:** Die Leitungsebene trägt die Verantwortung für die Entwicklung und Umsetzung einer Sicherheitsstrategie, die sich an den Geschäftszielen orientiert.
- **Ressourcen und Mitarbeiter:** Der Aufbau eines kompetenten und verantwortungsbewussten Teams ist essenziell. Dies umfasst Schulungen, klare Zuweisung von Rollen und Verantwortlichkeiten sowie die Bereitstellung notwendiger Ressourcen.
- **Sicherheitsprozess:** Dazu gehören Sicherheitsleitlinien, ein Sicherheitskonzept und eine Sicherheitsorganisation, die klare Strukturen und Zuständigkeiten schaffen.

Die Sicherheitsstrategie bildet das Herzstück eines ISMS und wird in der Sicherheitsleitlinie dokumentiert. Diese Leitlinie spiegelt das Engagement der Leitungsebene wider und definiert die strategischen Ziele der Organisation im Bereich Informationssicherheit. Sie dient als Grundlage für die Umsetzung der Sicherheitsmaßnahmen und die Etablierung eines einheitlichen Sicherheitsniveaus.

Das Lebenszyklusmodell, das im BSI-Standard 200-1 [14, pp. 15-18] beschrieben wird, zeigt, dass Informationssicherheit niemals als statisch betrachtet werden darf. Veränderungen in Geschäftsprozessen, der technologischen Landschaft oder gesetzlichen Vorgaben erfordern eine regelmäßige Überprüfung und Anpassung der Sicherheitsmaßnahmen. Der Lebenszyklus eines ISMS umfasst dabei nicht nur die Einführung neuer Systeme, sondern auch die sichere Stilllegung oder den Austausch von Komponenten.

2.2.3 Gängige ISMS-Standards und -Frameworks

Die Umsetzung eines ISMS kann grundsätzlich auf verschiedenen anerkannten Standards und Rahmenwerken basieren. Diese unterscheiden sich hinsichtlich ihrer Zielgruppen, Komplexität, Struktur und regulatorischen Anschlussfähigkeit. Im Folgenden wird eine kompakte Übersicht zentraler ISMS-Standards und -Frameworks dargestellt. Ziel ist es, eine Orientierung darüber zu geben, welche Referenzwerke beim Aufbau eines ISMS prinzipiell herangezogen werden können. Für jedes der aufgeführten Frameworks werden die Zielsetzung, die grundsätzliche Eignung und typische Einsatzbereiche knapp skizziert.

ISO/IEC 27001: Der Standard ISO/IEC 27001 [13] ist einer der am weitesten verbreiteten und anerkannten Standards für ISMS. Er bietet einen systematischen Ansatz zur Verwaltung der Informationssicherheit, indem er Organisationen bei der Identifizierung, Bewertung und Behandlung von Risiken unterstützt. ISO/IEC 27001 konzentriert sich auf die Implementierung des PDCA-Zyklus, um kontinuierliche Verbesserungen sicherzustellen. Der Standard umfasst auch eine Reihe von Sicherheitskontrollen, die im Annex A spezifiziert sind. [12, pp. 2-3]

BSI IT-Grundschutz: Das deutsche Pendant zur ISO/IEC 27000-Reihe ist der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene IT-Grundschutz. [15, p. 7] Dieser besteht aus vier zentralen Standards: [16]

- BSI 200-1 definiert allgemeine Anforderungen an ein ISMS, kompatibel zu ISO/IEC 27001.
- BSI 200-2 beschreibt drei Umsetzungsansätze (Basis-, Standard-, Kern-Absicherung) zur Einführung eines ISMS.
- BSI 200-3 bündelt risikobezogene Schritte zur effizienten Durchführung von Risikoanalysen.
- BSI 200-4 ergänzt den Grundschutz um ein systematisches Business Continuity Management (BCMS).

NIST Cyber Security Framework (CSF): Das Cybersecurity Framework des US-amerikanischen National Institute of Standards and Technology (NIST) bietet einen risikobasierten, modularen Ansatz zur Bewertung und Verbesserung von Cybersicherheitsmaßnahmen. Die fünf Kernfunktionen „Identify“, „Protect“, „Detect“, „Respond“ und „Recover“ strukturieren die Sicherheitsprozesse eines Unternehmens. [17, pp. 15-27]

2.3 Informationssicherheit in KMUs

Nachdem nun die regulatorischen Anforderungen sowie der Rahmen zur systematischen Umsetzung thematisiert wurden, werden in diesem Kapitel der wirtschaftliche Wert sowie die Herausforderungen von KMUs näher betrachtet. Für KMUs stellen die regulatorischen Vorgaben in vielfacher Hinsicht eine erhebliche Herausforderung dar: begrenzte personelle Ressourcen, fehlendes Fachwissen sowie ein oft reaktiver Zugang zur Informationssicherheit erschweren die systematische Umsetzung. [1], [18] Gerade im Zuge der NIS2-Richtlinie und deren nationaler Umsetzung erfahren KMUs jedoch eine neue regulatorische Sichtbarkeit. Viele Unternehmen, die bislang nicht unter die Regelungssysteme fielen, sind künftig zur Einhaltung umfassender Sicherheitsvorgaben verpflichtet. Dies wirft die Frage auf, inwiefern KMUs aktuell in der Lage

sind, diesen Anforderungen gerecht zu werden, sowohl organisatorisch als auch wirtschaftlich. Ziel dieses Kapitels ist es daher, die spezifische Ausgangslage von KMUs im Hinblick auf ihre Rolle in der Wirtschaft, ihre besondere Verwundbarkeit sowie den aktuellen Stand ihrer Cyber-Resilienz zu analysieren. Damit soll die Grundlage geschaffen werden, um in den folgenden Kapiteln ein praxistaugliches ISMS-Framework zu entwickeln, welches diesen Rahmenbedingungen gerecht wird.

2.3.1 Wirtschaftliche und regulatorische Relevanz

KMUs machen 99,8% aller nicht-finanziellen Unternehmen in der EU aus, stellen 64% der Arbeitsplätze und erwirtschaften gut 52% der Bruttowertschöpfung. [19] Ihre Rolle als Zuliefernde und Dienstleistende in digitalisierten Wertschöpfungsketten macht sie zugleich zum Einfallstor für Angriffe auf größere Ökosysteme. [1, p. 8] Mit NIS2 rücken sie erstmals systematisch ins Zentrum der Cybersicherheitsregulierung. Die in Kapitel 2.1 beschriebenen regulatorischen Neuerungen (NIS2, NISG 2024) erhöhen somit nicht nur die rechtliche, sondern auch die betriebswirtschaftliche Relevanz von Informationssicherheit für KMUs.

2.3.2 Aktueller Stand und Reifegrad der KMUs

Obwohl der Schwerpunkt dieser Arbeit auf österreichischen KMUs liegt, werden im Folgenden auch Studienergebnisse aus Deutschland, der Schweiz und Italien herangezogen. Der Grund dafür ist die derzeit eingeschränkte Datenverfügbarkeit zu sicherheitsrelevanten Reifegraden in österreichischen KMUs. Gleichzeitig besteht aufgrund ähnlicher Unternehmensstrukturen, Digitalisierungsthemen und regulatorischer Rahmenbedingungen eine hohe Vergleichbarkeit im mitteleuropäischen Raum. Die ausgewählten Studien sind daher inhaltlich anschlussfähig und tragen dazu bei, ein umfassenderes Bild der Ausgangslage zu zeichnen.

Eine breit angelegte ENISA-Studie [1, p. 3] aus dem Jahr 2021 mit 249 KMUs ergab, dass viele Unternehmen in der EU zwar auf das Thema Digitalisierung (z.B. Cloud-Dienste, Home-Office, etc.) angewiesen sind, jedoch Schwachpunkte im Bereich Awareness, Budget, IT-Fachkräften sowie geeigneten Leitfäden haben. So gaben über 80% der befragten KMUs an, dass ein Cybervorfall binnen einer Woche gravierende Folgen für sie hätte und 57% fürchten hierbei sogar Insolvenz. Trotzdem schätzen KMUs ihr eigenes Risiko als relativ niedrig ein. Auch eine aktuelle empirische Studie [20, p. 56, 70] aus dem Jahr 2024 zeigt, dass KMUs in Deutschland ihre Eintrittswahrscheinlichkeit für Cyberangriffe systematisch unterschätzen: Über 52% der Befragten schätzen ihr Risiko niedriger ein als das von vergleichbaren Unternehmen und das trotz steigender Bedrohungslage. Diese Verzerrung ist ein typischer Indikator für den sogenannten Optimismus-Bias in der Risikowahrnehmung. Auch in Italien fanden Neri et al. (2022) [21, p. 2] mit einer Befragung von

KMUs heraus, dass organisatorische Cyber-Readiness auf einem sehr niedrigen Niveau ist und viele „noch viele weitere Maßnahmen ergreifen müssen."

In Deutschland beschreibt das BSI im Lagebericht des Jahres 2024 [22, pp. 68-69], dass etwa 3,1 Millionen KMUs existieren und somit 99,4% aller Unternehmen ausmachen. Insbesondere Kleinst- (unter 10 Mitarbeitenden) sowie kleine Unternehmen (unter 50 Mitarbeitenden) verfügen häufig nicht über eigenes Personal für IT-Sicherheit. Stattdessen wird im Rahmen des klassischen „Make or Buy"-Entscheidungsprozesses oft der Ansatz gewählt, „das bekommen wir schon irgendwie selbst hin", was zu strukturellen Schwächen in der Sicherheitsorganisation führt. Der Lagebericht [22, pp. 6-9] bestätigt zudem die zunehmende Bedrohungslage, da Ransomware und Access-Broker zu den dominierenden Angriffsvektoren zählen, wobei Opfer zumeist KMUs sind. Angreifer:innen wählen gezielt „den Weg des geringsten Widerstandes", denn je schwächer die Schutzmaßnahmen, desto höher die Erfolgswahrscheinlichkeit.

In der Schweiz zeigt die Cyberstudie 2024 [23, pp. 8-12] Ähnliches. 4% der befragten Schweizer KMUs waren in den letzten drei Jahren Opfer eines schweren Cyberangriffs, wobei bei 73% ein hoher finanzieller Schaden entstand. Trotz einer allgemein hohen Wahrnehmung der Bedrohungen, schätzen über 50% der KMUs ihr eigenes Risiko als „gering" ein, was in einem falschen Sicherheitsgefühl und somit potenziellen gravierenden Folgen resultieren kann. Zudem besitzen fast die Hälfte der KMUs keinerlei Notfallplan oder Kontinuitätsstrategie im Falle eines Angriffes. IT-Dienstleister:innen fordern daher deutlich mehr Sensibilisierung und Schulung der Mitarbeitenden. Bemerkenswert ist auch die Zurückhaltung bei modernen Sicherheitstechnologien, da nur wenige Schweizer KMUs etwa Passwortmanager oder Multi-Faktor-Authentifizierung verwenden. Außerdem werden organisatorische Maßnahmen wie Sicherheitsrichtlinien sowie Audits oft vernachlässigt.

Der Reifegrad in österreichischen KMUs zeigt sich sehr heterogen. Eine aktuelle Studie [24, pp.257-258] mit 30 mittelständischen Unternehmen aus Deutschland und Österreich ergab, dass im Mittel nur etwa 28% der abgefragten Sicherheitsmaßnahmen vollständig umgesetzt sind, 42% teils umgesetzt und 30% kaum oder gar nicht. Diese Einschätzung wird durch den CyberGuide 2024 [25, pp. 31-34] für österreichische KMUs bestätigt. Laut dessen Ergebnissen führen Kleinst- und kleine Unternehmen seltener Risikoanalysen durch und verfügen häufig nicht über klar definierte Zuständigkeiten für IT-Sicherheit. Demgegenüber haben mittlere Unternehmen bereits regelmäßige Sicherheitsupdates, Passwortkonzepte und Berechtigungssysteme etabliert. Dennoch investiert insgesamt nur etwa ein Fünftel der KMUs gezielt in Cybersicherheit,

was ein strukturelles Umsetzungshemmnis darstellt.

Parallel zeigt das Allianz Risk Barometer 2025 [26, p. 5, 12], dass Cyber-Vorfälle mit 38% weltweit das größte Geschäftsrisiko darstellen. Damit belegte das Thema Cyber bereits das vierte Jahr in Folge den ersten Platz der globalen Risiko-Rangliste. Diese Ergebnisse spiegeln die gestiegene Risiko-Wahrnehmung in der Wirtschaft wider.

2.3.3 Größte Herausforderungen im Bereich Cybersicherheit für KMUs

Die Analyse des aktuellen Reifegrads hat gezeigt, dass viele KMUs weder organisatorisch noch technisch ausreichend auf aktuelle Cyberbedrohungen vorbereitet sind. Im Folgenden werden die zentralen Herausforderungen der KMUs in Bezug auf Informationssicherheit dargestellt:

- **Unterfinanzierung:** Finanzielle Ressourcen gelten weiterhin als zentrales Umsetzungshemmnis für Cybersicherheitsmaßnahmen in KMUs. Laut dem CyberGuide 2024 [25, p. 5, 49, 51] geben 54% der Unternehmen an, dass hohe Investitionskosten die Umsetzung geeigneter Sicherheitsmaßnahmen erheblich erschweren. Cybersicherheit wird vielfach nicht als unmittelbar geschäftskritisch wahrgenommen, wodurch geplante Investitionen zugunsten anderer operativer Ausgaben zurückgestellt werden. In der Praxis verbleibt damit ein strukturelles Finanzierungsdefizit, das besonders bei der Einführung systematischer Schutzkonzepte wie eines ISMS wirksam adressiert werden muss.
- **Mangel an Personal und Expertise:** Laut ENISA [1, p. 7] verfügen nur etwa 28% der KMUs in der EU überhaupt über eine dedizierte Rolle für Informationssicherheit, wodurch systematische Risikoanalysen und strukturierte Schutzmaßnahmen erschwert werden. 38% der österreichischen KMUs geben an, nicht über ausreichende interne Expertise zu verfügen, um Cybersicherheitsmaßnahmen eigenständig umzusetzen. Besonders Kleinstunternehmen sind auf externe Dienstleistende angewiesen, denen oft strategische Steuerungskompetenz fehlt. Dies verstärkt die Abhängigkeit von punktuellen Lösungen, ohne nachhaltige Verankerung im Unternehmen. [25, p. 5, 51]
- **Kostenrisiko durch Ransomware:** Lösegeldforderungen bei Angriffen erreichen regelmäßig bis zu 850.000 US-Dollar pro Vorfall. Für KMUs kann ein einzelner Vorfall mit Produktionsstillstand existenzbedrohend sein. [22]
- **Kulturelle Barrieren:** Informationssicherheit wird in vielen Betrieben als „notwendiges Übel“ wahrgenommen. Führungskräfte unterschätzen häufig ihre Verantwortung nach NIS2, während Mitarbeitende Sicherheitsmaßnahmen als zusätzliche Belastung erleben, was deren Akzeptanz reduziert. [25, p. 35]

Die dokumentierten Schwächen und Bedürfnisse, wie sie sowohl in EU-weiten ENISA-Erhebungen als auch im österreichischen CyberGuide 2024 identifiziert wurden, unterstreichen die Notwendigkeit eines zielgerichteten, schlanken ISMS-Frameworks für KMUs, welches regulatorische Anforderungen mit realistischen Umsetzungsfähigkeiten in Einklang bringt.

3 Stand der Forschung

Die Entwicklung eines praxisnahen ISMS-Frameworks für KMUs erfordert eine fundierte Auseinandersetzung mit dem aktuellen Stand der Wissenschaft und bestehenden Implementierungsansätzen. Insbesondere im Hinblick auf die bevorstehenden Anforderungen der NIS2-Richtlinie stellt sich die Frage, inwieweit bestehende Standards und Modelle sowohl regulatorischen als auch unternehmensspezifischen Anforderungen gerecht werden. Dieses Kapitel verfolgt das Ziel, relevante theoretische und praxisorientierte Quellen zu identifizieren, systematisch zu analysieren und hinsichtlich ihrer Eignung für KMUs zu bewerten. Dabei liegt ein besonderer Fokus auf der Umsetzbarkeit, Skalierbarkeit und NIS2-Konformität bestehender ISMS. Vor dem Hintergrund der noch jungen Regulierungslandschaft rund um NIS2 zeigt sich bereits in der Recherchephase ein begrenzter wissenschaftlicher Diskurs zur konkreten Umsetzung in KMUs. Diese Forschungslücke wird im Verlauf dieses Kapitels sichtbar gemacht und dient als Argumentationsbasis für die Eigenständigkeit und Relevanz des in dieser Arbeit entwickelten Frameworks.

3.1 Ziel und Methodik der Literaturrecherche

Die Recherche fokussiert sich auf wissenschaftliche und praxisorientierte Veröffentlichungen, die sich mit bestehenden ISMS im Kontext von KMUs sowie mit den regulatorischen Anforderungen der NIS2-Richtlinie befassen. Die Recherche erfolgte primär in wissenschaftlichen Datenbanken wie IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar sowie in branchenspezifischen Quellen wie BSI-Publikationen, ENISA-Leitlinien. Die verwendeten Suchbegriffe kombinierten unter anderem:

- „ISMS + KMU“
- „Informationssicherheit + kleine und mittlere Unternehmen“
- „NIS2 + Umsetzung“
- „ISO 27001 + KMU“
- „Cybersecurity Frameworks + SMEs“
- „ISMS Framework + SMEs“
- NIS2 Directive + SMEs“

- Information Security + small and medium enterprises”

Zur Eingrenzung wurden Publikationen ab dem Jahr 2016 berücksichtigt, um die Relevanz im Hinblick auf aktuelle Herausforderungen und regulatorische Entwicklungen sicherzustellen. Dokumente wurden unter anderem nach den folgenden Auswahlkriterien gefiltert:

- direkter Bezug zur praktischen Umsetzung von ISMS in KMUs
- Anwendbarkeit auf europäische Rechtskontexte (insbesondere NIS2)
- strukturelle oder methodische Ansätze zur Informationssicherheitsgovernance
- Praxisnähe und Skalierbarkeit der Konzepte

Die Auswertung wurde inhaltsanalytisch vorgenommen, wobei der Fokus auf der Identifikation von Stärken, Schwächen und potenziellen Lücken bestehender Ansätze lag. Erkenntnisse aus der Analyse bilden die Grundlage für die Entwicklung des in dieser Arbeit vorgeschlagenen ISMS-Frameworks.

3.2 Überblick bestehender ISMS-Ansätze für KMUs

KMUs stehen bei der Einführung und dem Betrieb eines ISMS vor besonderen Herausforderungen. Während ISO/IEC 27001, IT-Grundschutz sowie NIST CSF primär für mittlere bis große Organisationen mit dedizierten Security-Ressourcen konzipiert sind, adressieren die nachfolgend dargestellten Ansätze typische KMU-Restriktionen wie limitiertes Budget, begrenztes Fachpersonal und minimaler Overhead. Sie vereinfachen die Implementierung eines ISMS unter anderem durch folgende Punkte:

- **Modularisierung:** klare Phasen-Pakete, welche Schritt für Schritt eingeführt werden können
- **Reduzierter Kontrollumfang:** Konzentration auf risikoadäquate Mindestanforderungen
- **Branchen- bzw. Unternehmensgrößen-spezifische Benchmarks:** passgenaue Leitplanken statt „One-size-fits-all“

3.2.1 Modularisierte ISMS-Ansätze für KMUs

Einige Modelle und Leitfäden wurden explizit für KMUs entwickelt oder erweitert, um eine schrittweise und ressourcenschonende Einführung von Informationssicherheitsprozessen zu ermöglichen.

Die „VdS 10000:2025“ [27] ist ein solcher Ansatz. Sie wurde gemeinsam mit mittelständischen Unternehmen überarbeitet und enthält klar formulierte, praxisnahe Anforderungen, welche insbesondere für Orga-

nisationen ohne tiefgehende Informationssicherheitskenntnisse verständlich sind. Neu in der Version 2025 sind unter anderem verbindlich geregelte Rollen (z.B. Informationssicherheitsbeauftragte:r), verpflichtende Multi-Faktor-Authentifizierung bei Fernzugriffen, ein vereinfachtes Sicherheitsvorfallsmanagement sowie ein modernisiertes Risikomanagement. Besonders relevant ist, dass die VdS 10000 als Grundlage für die kommende „VdS 10100“ dient, welche die Anforderungen der NIS2-Richtlinie in nationales deutsches Recht übertragen wird. Diese Norm ersetzt den Annex A der ISO/IEC 27001 durch 32 vorvalidierte Maßnahmen, wodurch der Dokumentationsaufwand ein Vielfaches für KMUs sinkt.

Ein weiteres Beispiel ist das Framework „CISIS12“ [28], welches insbesondere in Bayern und im kommunalen Umfeld Verbreitung findet. Es basiert methodisch auf ISO/IEC 27001, reduziert jedoch die Komplexität durch einen 12-stufigen, klar strukturierten Prozess. CISIS12 ist modular aufgebaut, leicht auditierbar und ebenfalls auf KMUs mit geringen Ressourcen zugeschnitten.

Die „ISO/IEC 27001-HBK:2024“ [29] bietet als offizielles Handbuch zur Anwendung von ISO/IEC 27001 in KMUs eine praxisnahe Interpretation und Anwendungshilfen und priorisiert lediglich 35 Kern-Maßnahmen (statt 93). Es adressiert Organisationen ohne spezifisches Fachpersonal oder umfangreiche finanzielle Mittel und reduziert die Einstiegshürden erheblich.

International hervorzuheben ist zudem der “NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide”. [30] Dieser basiert auf den fünf bekannten Funktionen des NIST CSF „Identify“, „Protect“, „Detect“, „Respond“ und „Recover“ und bietet speziell für KMUs einfache Schritt-für-Schritt-Einstiege mit klaren Priorisierungen und Checklisten.

3.2.2 Reifegradmodelle und vereinfachte Einstiegskonzepte

Neben modularisierten Frameworks gibt es auch einige Konzepte, welche auf Reifegradmodellen oder Mindestanforderungen basieren und KMUs einen gestaffelten Einstieg in die Informationssicherheit bieten.

Ein Beispiel ist das „CHOISS-Modell“ von Mijnhardt et al. [31], welches auf einer empirischen Untersuchung basiert. Es identifiziert 47 Einflussfaktoren aus den Bereichen Organisation, Technologie und Management, welche in ihrer Gesamtheit die ISMS-Reife eines Unternehmens bestimmen. Dieses Modell kann sowohl zur Initialbewertung als auch zur Fortschrittskontrolle eingesetzt werden.

Das „LCCI-Framework“ (Least Controls for Cybersecurity Implementation) verfolgt einen pragmatischen Bottom-up-Ansatz und leitet aus der Analyse von 115 KMUs ein Minimum an effektiven Sicherheitskontrollen ab. Ziel ist es, mit geringstmöglichem Aufwand eine grundlegende Sicherheitsbasis zu schaffen. [32, pp. 3-5]

Ergänzend dazu bietet der „SBS SME Guide“ [33] eine stark vereinfachte Umsetzungshilfe für ISO/IEC 27001 in KMUs, die mit praxisorientierten Erläuterungen und Musterdokumenten arbeitet. Der Fokus liegt auf Anwendbarkeit, nicht auf formaler Vollständigkeit.

3.2.3 Beratungserfahrungen und Umsetzungsrealitäten

Studien zur Beratungspraxis und empirische Analysen zur NIS2-Umsetzung zeigen, dass trotz zunehmender Verfügbarkeit vereinfachter ISMS-Modelle strukturelle Hindernisse in KMUs weiterhin bestehen. Eine qualitative Untersuchung von Khan et al. [18, pp. 6-11] beschreibt, dass viele Unternehmen selbst einfache Handlungsempfehlungen nicht umsetzen können. Ursachen sind unzureichende Awareness, fehlende Kapazitäten sowie Unsicherheiten hinsichtlich Zuständigkeiten und Priorisierung. Diese Erkenntnisse werden durch die umfassende empirische Analyse von Joswig und Kurz [34] bestätigt, welche sich mit der NIS2-Implementierung in deutschen KMUs in KRITIS-Sektoren befasst. Die Studie belegt, dass insbesondere kleinere Organisationen mit bis zu 50 Mitarbeitenden erhebliche Compliance-Probleme, insbesondere hinsichtlich Vorfalls-Meldung, Risikomanagement und Lieferkettensicherheit, aufweisen. Hauptursachen sind finanzielle Engpässe, fehlende Fachkompetenz und die hohe Komplexität der regulatorischen Anforderungen. Die Autoren fordern unter anderem die Entwicklung vereinfachter, skalierbarer ISMS-Frameworks sowie staatlich geförderter Beratungslösungen, um die Lücke zwischen Regulierung und Umsetzung zu schließen. Es wird ebenso auf die Notwendigkeit technischer Hilfsmittel (z.B. KI-gestützte Compliance-Werkzeuge) und branchenspezifischer Guidelines hingewiesen.

3.3 Analyse und Identifikation von Lücken

Die Analyse der einschlägigen KMU-Leitfäden zeigt drei wiederkehrende Erfolgsfaktoren:

- **Schlanke Governance und klare Verantwortlichkeiten:** Viele der Modelle setzen auf ein minimalistisches Rollenmodell, welches KMUs organisatorisch nicht überfordert
- **Risikobasierte Modularität:** Die Modelle und Leitfäden priorisieren Maßnahmen strikt nach Geschäftsauswirkung (z.B. Red-/Amber-/Green-Kontrollen bei VdS 10000 oder „Least Controls“ im

LCCI) Dadurch können KMUs exakt dort investieren, wo der höchste Wertbeitrag zur Risikominderung entsteht

- **Hands-on-Umsetzungshilfen:** Checklisten, Vorlagendokumente, Beispielprozesse und Reifegrad-Self-Assessments vereinfachen die operative Einführung wesentlich

Trotz der beschriebenen Vielzahl von praxisorientierten ISMS-Ansätzen für KMUs zeigen sich eine Reihe von strukturellen, methodischen und regulatorischen Defiziten, welche KMUs eine praxisnahe und einfache Umsetzung erschweren. Diese Defizite betreffen sowohl die Inhalte der bestehenden Frameworks als auch deren Anschlussfähigkeit an regulatorische Vorgaben, insbesondere im Hinblick auf die Anforderungen der NIS2-Richtlinie.

3.3.1 Fehlende Integration der regulatorischen Anforderungen

Ein wesentlicher Aspekt, welcher in der durchgeführten Analyse zur Kenntnis genommen wurde, ist die unzureichende Berücksichtigung aktueller europäischer Regulierungen. Keines der untersuchten Modelle hat die Anforderungen der NIS2-Richtlinie in operationalisierbarer Form abgebildet. Obwohl VdS die Entwicklung der VdS 10100 als NIS2-konformes Pendant angekündigt hat [27], liegt aktuell noch kein integriertes ISMS-Framework mit explizitem NIS2-Bezug für KMUs vor.

3.3.2 Methodische Fragmentierung und eingeschränkte Praxistauglichkeit

Viele bestehende Modelle beschränken sich auf technische oder organisatorische Einzelmaßnahmen, ohne ein konsistentes und gesamtes Managementsystem zu etablieren. Insbesondere fehlt oft eine ganzheitliche Integration der Bereiche Governance, Risikoanalyse, Schulung, Auditierung und kontinuierliche Verbesserung, welche zentrale Elemente eines ISMS gemäß ISO/IEC 27001 sind und auch in Hinblick auf die NIS2 wichtig sind. Der Einsatz eines ISMS eignet sich gerade dazu, diese Einzelmaßnahmen systematisch und risikobasiert umzusetzen sowie Synergien für die Ressourceneffizienz zu nutzen. Zudem ist die Praxistauglichkeit der Maßnahmenumsetzung in vielen Frameworks nicht ausreichend gewährleistet. Zwar bieten Formate wie VdS 10000 oder CISIS12 strukturierte Vorgaben, jedoch bleibt die konkrete Beschreibung von Maßnahmen, Zuständigkeiten und Umsetzungsschritten oftmals zu abstrakt für KMUs ohne tiefgreifende Fachexpertise im Bereich Cybersicherheit. Die Beschreibung bleibt vielfach auf Managementebene und vernachlässigt die operative Umsetzbarkeit für kleine Organisationseinheiten, welche nicht über spezialisiertes Fachpersonal verfügen. In der Studie von Joswig und Kurz [34, pp. 1-14] wird explizit gefordert, dass Maßnahmen stärker durch Beispiele, Szenarien und branchenspezifische Kontexte veranschaulicht werden

sollten.

4 Methodisches Vorgehen

Das folgende Kapitel beschreibt die Vorgehensweise zur Erstellung eines schlanken und praxisorientierten ISMS-Frameworks für KMUs, welches gezielt auf die regulatorischen Anforderungen der NIS2-Richtlinie eingeht. Als „schlank“ wird das Framework bezeichnet, da es sich ausschließlich auf die in Art. 21 Abs. 2 der NIS2-Richtlinie geforderten Mindestanforderungen sowie die 13 Themenbereiche der Anlage 3 des NISG 2024 konzentriert und bewusst auf optionalen Overhead („Gold Plating“) verzichtet. Der praxisorientierte Ansatz ergibt sich unter anderem aus der Verwendung vorhandener Best Practices (z.B. BSI-Guidelines) für Umsetzungshilfen, einen modularen Aufbau mit einer beginnenden vereinfachten Gap Analyse zur Evaluierung der Lücken, anpassbare Dokumentenvorlagen sowie einem holistischen Fahrplan, welcher KMUs bei der priorisierten Umsetzung der Maßnahmen helfen soll.

4.1 Arbeitsgrundlagen

Die Entwicklung des ISMS-Frameworks basiert auf folgenden Quellen und Inputs:

Input	**Quelle**
Rechtsdokumente	• NIS2-Richtlinie • NIS2 Durchführungsverordnung • Österreichischer Gesetzesentwurf NISG 2024
Best Practice	• ISO/IEC 27001:2022 Annex A (Kontrollen) • ENISA „NIS2 Implementation Guidance“ • BSI-Standards des IT-Grundschutzes • BSI-Umsetzungshinweise der IT-Grundschutz-Bausteine • WKO „IT-Sicherheitshandbuch für KMU“ der WKO

Input	Quelle
Praxis-Know-how	• Persönliche Projekterfahrungen aus der Unternehmensberatung hinsichtlich NIS2-, ISMS- sowie KMU-Thematiken

Tabelle 4.1: Arbeitsgrundlagen für die Entwicklung des ISMS-Frameworks

Diese Quellenkombination stellt sicher, dass die entwickelte Lösung sowohl regulatorisch korrekt als auch direkt praxisrelevant ist.

4.2 Vorgehensschritte

Das Framework wurde durch eine klar strukturierte Abfolge pragmatischer Schritte entwickelt, um KMUs ein effizientes Vorgehen bei der Implementierung zu ermöglichen.

4.2.1 Mapping der Anforderungen

Alle regulatorischen Anforderungen der NIS2-Richtlinie, der Durchführungsverordnung sowie des österreichischen Gesetzesentwurfs (Anlage 3) wurden zunächst systematisch analysiert und anschließend thematisch in einem Excel-Dokument zusammengeführt. Das Ergebnis ist ein übersichtliches Mapping, welches die regulatorischen Vorgaben konkret den einzelnen Themenbereichen der Anlage des Gesetzesentwurfs (1. Leitungsorgane, 1a. Rollen und Verantwortlichkeiten der Leitungsorgane, 2. Sicherheitsrichtlinien, etc.) zuordnet.

In der folgenden Abbildung 4.1 ist ein exemplarischer Auszug dieses Mappings dargestellt. Am Beispiel der Themenbereiche „Risikomanagement“ (Punkt 3) sowie „Verwaltung von Vermögenswerten“ (Punkt 4) wird ersichtlich, wie die Anforderungen aus den verschiedenen Normquellen miteinander verknüpft wurden:

- Die Spalte „NISG 2024 (Anlage 3)“ bildet die nationale Umsetzungsebene in Österreich ab (siehe Kapitel 2.1.2). Sie verweist auf die aufgelisteten Themen des NISG 2024 der Anlage 3 (z.B. „Risikomanagementrichtlinie und -prozess“, „Inventarisierung von Vermögenswerten“).
- Die Spalte „NIS2-Durchführungsverordnung (Anhang)“ zeigt die korrespondierenden Kapitel aus dem EU-Umsetzungsdokument (siehe Kapitel 2.1.3), welches die konkreten Sicherheitsanforderungen weiter operationalisiert.

- Die Spalte „NIS2-Richtlinie (EU)“ referenziert auf die zugrunde liegenden Artikel der NIS2-Richtlinie (insbesondere Artikel 21 Abs. 2), in welchen die jeweiligen Anforderungen rechtlich normiert sind (siehe Kapitel 2.1.1).

NISG 2024 (Anlage 3)		NIS2-Durchführungsverordnung (Anhang)	NIS2-Richtlinie (EU)
Nr.	Thema	Kapitel	Artikel
		[...]	
3.	Risikomanagement	2, 7	-
3a.	Risikomanagementrichtlinie und -prozess	2.1	Article 21(2) point (a)
		[...]	
4.	Verwaltung von Vermögenswerten	12	
4a.	Inventarisierung von Vermögenswerten	12.4	Article 21(2) point (i)
		[...]	

Abbildung 4.1: Mapping der NIS2-Anforderungen

Durch diese strukturierte Zuordnung wird die rechtliche Grundlage für jeden Themenbereich nachvollziehbar dokumentiert. Zudem dient das Mapping als Basis für die Ableitung spezifischer Maßnahmen und Kontrollen im Rahmen des zu entwickelnden ISMS-Frameworks.

4.2.2 Ableitung konkreter Maßnahmen und Nachweise

Für jeden Themenbereich der Anlage 3 des NISG 2024 wurden auf Basis des zuvor erstellten Mappings sowie unter Heranziehung etablierter Arbeitsgrundlagen 4.1 konkrete, niederschwellige Maßnahmen abgeleitet. Dies bedeutet, dass die Maßnahmen so formuliert wurden, dass sie ohne tiefgreifendes Fachwissen einfacher interpretierbar sind. Indem die Anforderungen der NIS2 durch konkrete Handlungsschritte beschrieben werden, was konkret zu machen ist, wird bewusst eine abstrakte Formulierung vermieden. Jede Maßnahme enthält zudem im Kapitel 5 konkrete Umsetzungshilfen mit praxisnahen Beispielen inklusive Dokumentenvorlagen (siehe Kapitel 4.2.4), welche sich unter anderem, wie in den Arbeitsgrundlagen erwähnt, aus der Praxiserfahrung sowie Best Practices sowie Leitfäden ableiten. Zusätzlich wurde zu jeder Maßnahme ein entsprechender, möglichst standardisierter Nachweis definiert, der sowohl im internen ISMS-Betrieb als auch im Rahmen externer Prüfungen (z.B. durch Aufsichtsbehörden oder Auditoren) als prüfrelevantes Dokument dient.

In der nachfolgenden Abbildung 4.2 ist ein exemplarischer Auszug dargestellt. Dieser zeigt für den Themenbereich „Risikomanagement“ konkrete Maßnahmen sowie zugehörige Nachweise:

- Für das Thema „Risikomanagementrichtlinie und -prozess“ wurde als Maßnahme unter anderem die Erstellung eines Risikomanagement-Handbuches sowie die Einführung eines standardisierten Risiko-

bewertungsprozesses definiert. Als Nachweise dienen beispielsweise das Handbuch selbst, durchgeführte und dokumentierte Risikoanalysen oder Protokolle.

NISG 2024 (Anlage 3)			
Nr.	**Thema**	**Abgeleitete Maßnahmenempfehlungen**	**Generelle Empfehlungen und Beispiele für Nachweise**
3.	**Risikomanagement**		
3a.	**Risikomanagementrichtlinie und -prozess**	- Erstellung und Einführung eines IS-Risikomanagement-Handbuchs zur Identifizierung, Bewertung und Behandlung von IS-Risiken inkl. Ziele, Risikotoleranz und -kriterien, Verantwortlichkeiten und Methodologie - Regelmäßige (mindestens jährlich) Durchführung von Risikoanalysen und Dokumentation in ein zentrales Risikoregister - Ableitung von Maßnahmen, Zuweisen von Maßnahmenverantwortlichen und Dokumentation in einem Risikobehandlungsplan - Regelmäßige Präsentation der kritischsten Risiken an die oberste Führungsebene	- Risikomanagement-Handbuch - Risikoregister - Risikobehandlungsplan

Abbildung 4.2: Ableitung von Maßnahmen und Nachweisen

Diese strukturierte Herangehensweise bildet das methodische Fundament für die weitere Framework-Entwicklung und ermöglicht eine nachvollziehbare Umsetzung der NIS2-Vorgaben in der betrieblichen Praxis.

4.2.3 Gap-Analyse-Checkliste

Die zuvor abgeleiteten Maßnahmen und zugehörigen Nachweise wurden durch eine integrierte Gap-Analyse-Checkliste ergänzt. Diese besteht aus spezifischen, prägnant formulierten Fragen im Ja/Nein/Teilweise-Format und ermöglicht eine strukturierte Selbsteinschätzung des aktuellen Umsetzungsstands im Unternehmen. Ziel dieser Checkliste ist es, insbesondere KMUs eine niederschwellige Möglichkeit zu bieten, bestehende Sicherheitsmaßnahmen im Kontext der NIS2-Anforderungen systematisch zu überprüfen. Die Ergebnisse der Analyse machen Handlungsbedarfe schnell sichtbar und können direkt in die Maßnahmenplanung überführt werden.

In der nachfolgenden Abbildung 4.3 ist ein exemplarischer Auszug der Fragen dargestellt. Für die Themenbereiche „Risikomanagementrichtlinie und -prozess“ und „Inventarisierung von Vermögenswerten“ wurden dabei konkrete Kontrollfragen hinterlegt, beispielsweise:

- Gibt es ein dokumentiertes Risikomanagement-Handbuch welches unter anderem Verantwortlichkeiten, Risikotoleranz bzw. -Kriterien und die Methodik enthält?
- Erfassen Sie alle Assets (z.B. Server, Endgeräte, Netzwerksysteme, Software, Cloud-Dienste) in einem zentralen Asset-Register?

NISG 2024 (Anlage 3)		
Nr.	**Thema**	**Gap-Analyse-Fragen**
3.	**Risikomanagement**	
3a.	**Risikomanagementrichtlinie und -prozess**	- Gibt es ein dokumentiertes Risikomanagement-Handbuch welches unter anderem Verantwortlichkeiten, Risikotoleranz bzw- kriterien und die Methodik enthält? - Sind die Risikotoleranz und -kriterien von der obersten Führungsebene freigegeben? - Wird mindestens jährlich eine Risikoanalyse durchgeführt und dokumentiert? - Gibt es einen Risikobehandlungsplan mit Verantwortlichkeiten und Fristen? - Werden kritische Risiken regelmäßig der Geschäftsleitung präsentiert?
		[...]
4.	**Verwaltung von Vermögenswerten**	
4a.	**Inventarisierung von Vermögenswerten**	- Erfassen Sie alle Assets (z. B. Server, Endgeräte, Netzwerksysteme, Software, Cloud-Dienste) in einem zentralen Asset-Register? - Werden jedem Asset eine Beschreibung, Standort und Schutzbedarf zugewiesen? - Wird das Asset-Register regelmäßig überprüft und aktualisiert?

Abbildung 4.3: Gap-Analyse-Checkliste

Diese Gap-Analyse ist ein zentrales Werkzeug im Rahmen des entwickelten ISMS-Frameworks und unterstützt sowohl die initiale Bewertung des Ist-Stands als auch die fortlaufende Wirksamkeitskontrolle im Sinne der kontinuierlichen Verbesserung gemäß PDCA-Zyklus.

4.2.4 Erstellung eines Vorlagen-Toolkits

Da KMUs, wie bereits in Kapitel 2.3.2 beschrieben, häufig mit eingeschränkten personellen Kapazitäten und begrenztem Fachwissen im Bereich Informationssicherheit konfrontiert sind, wurde ergänzend ein praxisorientiertes Toolkit in Form editierbarer Vorlagen und Beispieldokumente entwickelt. Dieses Toolkit soll die Umsetzung der im Rahmen dieser Arbeit definierten Maßnahmen und Nachweise gezielt erleichtern. Die Vorlagen wurden im Excel bei den jeweiligen Themenbereichen der Anlage 3 dokumentiert und orientieren sich sowohl an den regulatorischen Anforderungen der NIS2-Richtlinie und des NISG 2024 als auch an bewährten Standards wie ISO/IEC 27001, BSI IT-Grundschutz und NIST CSF. Darüber hinaus flossen Erkenntnisse aus der operativen Beratungspraxis ein, um insbesondere typische KMU-Herausforderungen zu adressieren (z.B. Dokumentationslast, fehlende Struktur, etc.).

In der nachfolgenden Abbildung 4.4 ist ein exemplarischer Auszug der Vorlagen pro Themenbereich dargestellt.

NISG 2024 (Anlage 3)		
Nr.	**Thema**	**Erstellte Vorlagendokumente**
1.	**Leitungsorgane**	
1a.	**Rollen und Verantwortlichkeiten der Leitungsorgane**	Informationssicherheitsleitlinie ("Sicherheitsrichtlinie") (Word) IS-Organisationsstruktur (PP) Cybersecurity-Lagebericht_VORLAGE (PP)
2.	**Sicherheitsrichtlinien**	
2a.	**Sicherheitsrichtlinien**	Informationssicherheitsleitlinie ("Sicherheitsrichtlinie") (Word) ISMS_Dokumentenlenkung (Excel) Kennzahlen und KPIs (Excel) Cybersecurity-Lagebericht_VORLAGE (PP)
		[...]
3.	**Risikomanagement**	
3a.	**Risikomanagementrichtlinie und -prozess**	IS-Risikomanagement_Handbuch (Word) Risikoregister und -behandlungsplan (Excel) Ergebnisse_Business Impact Analyse (Excel)

Abbildung 4.4: Auszug aus dem Vorlagen-Toolkit

Die Vorlagen sind so gestaltet, dass sie individuell anpassbar und unabhängig von einem bestimmten Branchenkontext einsetzbar sind. Sie stellen ein zentrales Anwendungsinstrument des entwickelten ISMS-Frameworks für KMUs dar.

4.2.5 Entwicklung eines holistischen Fahrplans zur Umsetzung

Zur strukturierten Einführung eines praxisnahen ISMS in KMUs mit Fokus auf NIS2 wurde ein Fahrplan auf einer hohen Detailgrad-Ebene entwickelt, welcher sich methodisch am etablierten PDCA-Zyklus orientiert (siehe Kapitel 2.2.2). Ziel ist es, eine kontinuierliche und schrittweise Verbesserung zu gewährleisten und gleichzeitig eine pragmatische, ressourcenschonende Umsetzung zu ermöglichen. Der vollständige Fahrplan einschließlich des inhaltlichen Mappings auf die relevanten Kapitel und Themenbereiche ist im Kapitel 5.14 dieser Arbeit dokumentiert und bildet die Umsetzungsgrundlage für das entwickelte Framework.

4.2.6 Validierung

Zur Überprüfung der Verständlichkeit, Umsetzbarkeit und regulatorischen Passfähigkeit des entwickelten ISMS-Frameworks wurde eine qualitative Validierung durchgeführt. Ziel war es, potenzielle Schwächen in der Struktur und Formulierung des Frameworks zu identifizieren sowie praxisbezogene Optimierungspotenziale aufzudecken. Die Validierung orientierte sich methodisch an der Vorgehensweise „Vali-Quali“ von Torlig et al. [35], welche sich zur Bewertung von qualitativen, praxisorientierten Forschungsprodukten bewährt hat. Im Zentrum der Validierung stand eine strukturierte qualitative Rückmeldung durch zwei Expert:innen mit einschlägiger Erfahrung im Bereich Informationssicherheitsmanagement in KMUs:

- Ein Informationssicherheitsbeauftragte:r eines KMUs
- Ein Unternehmensberater:in mit langjähriger Projekterfahrung im Aufbau von ISMS und in der NIS2-

Beratung

Die Auswahl der Expert:innen erfolgte gezielt auf Basis ihrer Expertise im relevanten Anwendungskontext. Beide Expert:innen wurden mithilfe eines standardisierten Interviewleitfadens befragt, welcher auf den Kernkomponenten des entwickelten Frameworks basierte. Die Fragen zielten darauf ab, die vier zentralen Validierungsattribute gemäß Torlig et al. [35, pp. 12-14] abzubilden:

- **Zielausrichtung**: Entspricht das Framework dem intendierten Anwendungszweck?
- **Konstruktadäquanz:** Spiegelt es die Anforderungen und Begriffe der NIS2-Richtlinie korrekt wider?
- **Explizitheit:** Sind Inhalte klar und verständlich formuliert?
- **Qualitative Erkenntniserwartung:** Lässt sich auf Basis der Rückmeldungen weiterführender Erkenntnisgewinn generieren?

Die Interviews wurden als strukturierte Kurzgespräche durchgeführt und protokollarisch dokumentiert. Die Befragung erfolgte entlang von sieben offenen Leitfragen, welche inklusive der Ergebnisse in Kapitel 6 zu finden sind.

5 Inhalt und Ausarbeitung des Frameworks

Dieses Kapitel stellt die inhaltliche Ausarbeitung des entwickelten ISMS-Frameworks vor. Die Struktur folgt den 13 Themenbereichen der Anlage 3 des NISG 2024, wobei die jeweiligen Anforderungen der NIS2-Durchführungsverordnung (siehe Kapitel 4.2.1) die inhaltliche Grundlage bilden. Ziel ist es, eine praxisnahe und prüfbare Umsetzungshilfe zu schaffen, welche den spezifischen Rahmenbedingungen von KMUs gerecht wird. Für jeden Themenbereich werden die regulatorischen Vorgaben kompakt zusammengefasst, greifbar interpretiert und durch konkrete Umsetzungsempfehlungen sowie anpassbare Vorlagen ergänzt. Durch den Abgleich der Interpretationen der Anforderungen der NIS2 mit dem ENISA „Implementation Guidance on Security Measures“ [11] sowie der Praxiserfahrung wird sichergestellt, dass die erarbeiteten Umsetzungshilfen fachlich fundiert sind.

5.1 Leitungsorgane

Im Themenbereich der Leitungsorgane stehen insbesondere die Verantwortlichkeiten der obersten Leitungsebene (z.B. Geschäftsführung, Vorstand, etc.) im Kontext der Informationssicherheit im Fokus. Hierbei geht es nicht nur um formale Zuständigkeiten, sondern auch um die konkrete Verpflichtung zur aktiven Steuerung und Überwachung sicherheitsrelevanter Maßnahmen. Diese Klarstellung ist vor allem im Hinblick auf die persönliche Haftung gemäß NIS2 Artikel 20 Absatz 1 sowie Erwägungsgrund (137) der obersten Leitungsebene von zentraler Bedeutung. [2]

5.1.1 Rollen und Verantwortlichkeiten der Leitungsorgane

Mapping - NIS2 Durchführungsverordnung (Punkt 1.1.1. d - g): Die NIS2 Durchführungsverordnung fordert die Existenz eines „Konzepts zur Sicherheit von Netz- und Informationssystemen“, welches explizit die Verantwortlichkeiten der obersten Leitungsebene definiert. Dieses Konzept muss formell durch die Leitungsorgane genehmigt werden und unterstreicht deren zentrale Rolle unter anderem bei der kontinuierlichen Verbesserung der Sicherheitsmaßnahmen sowie bei der Bereitstellung der erforderlichen Ressourcen.

Interpretation dieser Anforderungen: Das „Konzept zur Sicherheit von Netz- und Informationssystemen“ ist das zentrale strategische Dokument eines ISMS gemäß den Anforderungen der NIS2-Richtlinie. Es dient als übergeordnete Leitlinie, in welcher die grundlegenden Ziele, Prinzipien und Zuständigkeiten zur Gewährleistung der Informationssicherheit innerhalb einer Organisation festgelegt sind. Inhaltlich entspricht es der klassischen Informationssicherheitsleitlinie und bildet die Basis für alle darauf aufbauenden, themenspezifischen Richtlinien und Prozesse. Dieses Dokument hat eine besondere Bedeutung für die Rollen und Verantwortlichkeiten der obersten Leitung: Durch seine formale Verabschiedung und regelmäßige Überprüfung unterstreicht die Unternehmensführung die strategische Relevanz der Informationssicherheit. Damit wird Informationssicherheit nicht als isoliertes IT-Thema behandelt, sondern als integraler Bestandteil einer verantwortungsbewussten und zukunftsorientierten Unternehmensführung verankert.

Umsetzung im NIS2-ISMS-Framework: Das Konzept zur Sicherheit von Netz- und Informationssystemen, als zentrale Leitlinie des ISMS, sollte pragmatisch, jedoch vollständig ausgestaltet sein. Ein besonderer Fokus von Punkt 1.a. Rollen und Verantwortlichkeiten der Leitungsorgane der Anlage 3 des österreichischen NIS2 Gesetzesentwurfs liegt hierbei auf den Verantwortlichkeiten der obersten Leitungsebene. Die Durchführungsverordnung verlangt ausdrücklich, dass sich die Leitungsorgane zur kontinuierlichen Verbesserung der Sicherheitsmaßnahmen verpflichten (Punkt 1.1.1 d), die notwendigen personellen, finanziellen und technischen Ressourcen bereitstellen (Punkt 1.1.1 e) und für eine klare Definition sowie Zuweisung von Rollen und Zuständigkeiten im Sicherheitsmanagement sorgen (Punkt 1.1.1 g).

In der Praxis bedeutet dies, dass KMUs ein kompaktes, aber strategisch fundiertes Dokument entwickeln sollten (z.B. 5 bis 10 Seiten), das nicht nur als formale Leitlinie dient, sondern als strukturierende Grundlage für alle weiteren ISMS-Komponenten fungiert. Dieses Dokument sollte durch die oberste Leitungsebene ausdrücklich genehmigt und mindestens einmal jährlich überprüft werden, beispielsweise im Rahmen eines Management-Reviews.

Zur Unterstützung dieser Umsetzung wurde im Rahmen dieser Arbeit für KMUs eine Muster-Vorlage für ein Konzept erstellt, die insbesondere auf die Anforderungen der Punkte 1.1.1 (d), (e) und (g) eingeht. Diese Vorlage bietet KMUs eine strukturierte Orientierungshilfe, ersetzt jedoch nicht die individuelle Auseinandersetzung mit den eigenen betrieblichen Anforderungen. Eine organisationsspezifische Anpassung ist unerlässlich, um sowohl den rechtlichen Vorgaben als auch den tatsächlichen Gegebenheiten im Unternehmen gerecht zu werden. Eine vertiefende Betrachtung zur inhaltlichen Ausgestaltung, Pflege und Dokumenten-

struktur der Leitlinie erfolgt im nachfolgenden Kapitel 5.2.

Wie in Kapitel 2.3.2 schon thematisiert, fehlt es in KMUs oft an finanziellen Ressourcen für das Thema Informationssicherheit. In Österreich stehen hierfür verschiedene Förderprogramme direkt für KMUs zur Verfügung, um Maßnahmen im Bereich Cybersicherheit und zur Umsetzung der NIS2-Richtlinie finanziell zu unterstützen. [36] Beispielsweise gab es seitens der österreichischen Forschungsförderungsgesellschaft (FFG) den sogenannten „Cyber Security Scheck“, welcher insbesondere an KMUs mit Sitz in Österreich gerichtet war, welche unter die NIS2-Richtlinie fallen. Pro Unternehmen konnte hierbei ein Scheck im Wert von maximal 10.000 € beziehungsweise maximal 40% der förderbaren Projektkosten vor Projektbeginn beantragt werden, wobei die Förderung sich für technologische Investitionen und Beratungsleistungen zur Umsetzung technischer Sicherheitsmaßnahmen richtete. [37] Auch Austria Wirtschaftsservice (aws) bietet KMUs mit Sitz in Österreich seit April 2022 die Förderung „KMU.Cybersecurity“ für bis zu 50% der förderbaren Kosten beziehungsweise Projektkosten zwischen 2.000 € und 50.000 € an. Hierbei ist zu beachten, dass die Projekte innerhalb von 18 Monaten ab Antragstellung umgesetzt werden müssen und maximal nur ein Projekt pro Unternehmen gefördert wird. Hierbei richtet sich die Förderung an Investitionen in IT-Sicherheitslösungen und damit verbundenen externen Dienstleistungen. [38] Mit dem Förderprogramm „KMU.DIGITAL“, welches eine Initiative des Bundesministeriums für Arbeit und Wirtschaft ist, wurden österreichischen KMUs neben Beratungsleistungen und Investitionen in digitalen Projekten je nach Modul auch Förderungen für den Bereich Cybersicherheit angeboten. Die Förderungskosten gehen bis zu 50% der förderbaren Kosten, wobei die genauen Beträge je nach Modul variieren. [39] Zusätzlich gibt es auch beispielsweise in den einzelnen Bundesländern in Österreich Förderungen angeboten. So können neben Kleinstunternehmen auch KMUs mit Betriebsstandort in Kärnten die Förderung „Digitalisierung.IMPULS“ des Kärntner Wirtschaftsförderung Fonds (KWF) beantragen. Die Förderhöhe beträgt hier bis zu 50% der förderbaren Kosten beziehungsweise 5.000 € bis 25.000 € der Projektkosten. Die Förderung richtet sich ähnlich wie bei „KMU.DIGITAL“ an Digitalisierungsprojekte sowie auch im Bereich Cybersicherheit. [40]

Mapping - NIS2 Durchführungsverordnung (Punkt 1.2.1, Punkt 1.2.3., Punkt 1.2.6): Im Abschnitt 1.2 der NIS2-Durchführungsverordnung werden mehrere Anforderungen definiert, die sich unmittelbar auf die Verantwortlichkeiten der obersten Leitungsebene beziehen. Besonders relevant ist Punkt 1.2.3, der explizit vorschreibt, dass mindestens eine Person direkt gegenüber den Leitungsorganen für Fragen der Informationssicherheit zuständig sein muss. Diese Berichtslinie ist essenziell, um sicherzustellen, dass Sicherheitsbelange regelmäßig auf strategischer Ebene adressiert werden können. Darüber hinaus verpflichtet Punkt 1.2.6

die Leitungsorgane dazu, Rollen, Verantwortlichkeiten und Weisungsbefugnisse regelmäßig zu überprüfen und anzupassen. Dies soll sicherstellen, dass die Organisation auch bei Veränderungen in der Bedrohungslage oder in betrieblichen Strukturen angemessen aufgestellt bleibt. Ergänzend ergibt sich aus Punkt 1.2.1 eine Informationspflicht gegenüber der obersten Leitungsebene, sodass diese über die interne Zuweisung sicherheitsrelevanter Zuständigkeiten informiert sind und entsprechend steuernd eingreifen können.

Interpretation der Anforderungen: Die Anforderungen aus Abschnitt 1.2 der NIS2-Durchführungsverordnung verdeutlichen, dass die oberste Leitungsebene nicht nur für die strategische Genehmigung des Konzepts verantwortlich ist, sondern auch eine aktive Rolle in der organisatorischen Steuerung und Überwachung der Netz- und Informationssicherheit übernehmen muss. Insbesondere durch Punkt 1.2.3 wird eine strukturelle Voraussetzung geschaffen, nach der mindestens eine Person direkt an die Geschäftsleitung über Sicherheitsfragen berichtet. Darüber hinaus verpflichtet Punkt 1.2.6 die Leitungsorgane dazu, regelmäßig zu überprüfen, ob die Zuweisung von Rollen, Verantwortlichkeiten und Weisungsbefugnissen noch den aktuellen Gegebenheiten entspricht. Damit wird Informationssicherheit als kontinuierlicher Führungsprozess verstanden, nicht als einmalige Maßnahme. Durch die Informationspflicht gemäß 1.2.1 wird zudem sichergestellt, dass die Geschäftsleitung über relevante Struktur- und Zuständigkeitsänderungen informiert ist und steuernd eingreifen kann.

Umsetzung im NIS2-ISMS-Framework: Für KMUs bedeutet die Umsetzung der NIS2-Anforderungen, dass sie klare, dokumentierte Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit unter aktiver Einbindung der obersten Leitungsebene etablieren müssen. Eine zentrale Maßnahme ist die Benennung einer verantwortlichen Person, idealerweise eines:einer Informationssicherheitsbeauftragten (ISB), die unmittelbar der obersten Leitungsebene unterstellt ist. Die Rolle kann beispielsweise bei Ressourcenmangel auch in Teilzeit ausgeübt werden, sofern keine Interessenskonflikte bestehen. Die IT-Leitung ist zum Beispiel hierfür in der Regel nicht geeignet, da operative Verantwortung und Kontrollfunktion nicht in einer Person vereint sein sollten. Alternativ können externe Dienstleistende als ISB eingesetzt werden. Wichtig ist in jedem Fall eine klare Zuweisung der Aufgaben und eine feste Anbindung an die oberste Leitungsebene.

Darüber hinaus sollte ein strukturierter Berichtskanal etwa in Form eines regelmäßigen „Management-Review“ eingerichtet werden. In diesem Rahmen wird die oberste Leitungsebene durch die zuvor festgelegte verantwortliche Person (ISB) mindestens einmal jährlich und zusätzlich anlassbezogen (z.B. bei Sicherheitsvorfällen) über zentrale Themen informiert: Sicherheitslage, Rollenverteilung, aktuelle Risiken, Maß-

nahmenumsetzung und NIS2-Compliance. Ziel ist es, fundierte Entscheidungen zu ermöglichen, Verantwortung nachvollziehbar zu dokumentieren und die kontinuierliche Verbesserung zu fördern. Zur Unterstützung der praktischen Umsetzung wurden im Rahmen dieser Arbeit mehrere Vorlagen für KMUs entwickelt. Dazu zählt eine strukturierte Vorlage für die Informationssicherheitsorganisation und -Governance-Struktur in Form einer aufbereiteten anpassbaren Power-Point-Vorlage, welche die zentralen Rollen, Berichtslinien und Zuständigkeiten im Bereich der Netz- und Informationssicherheit grafisch abbildet.

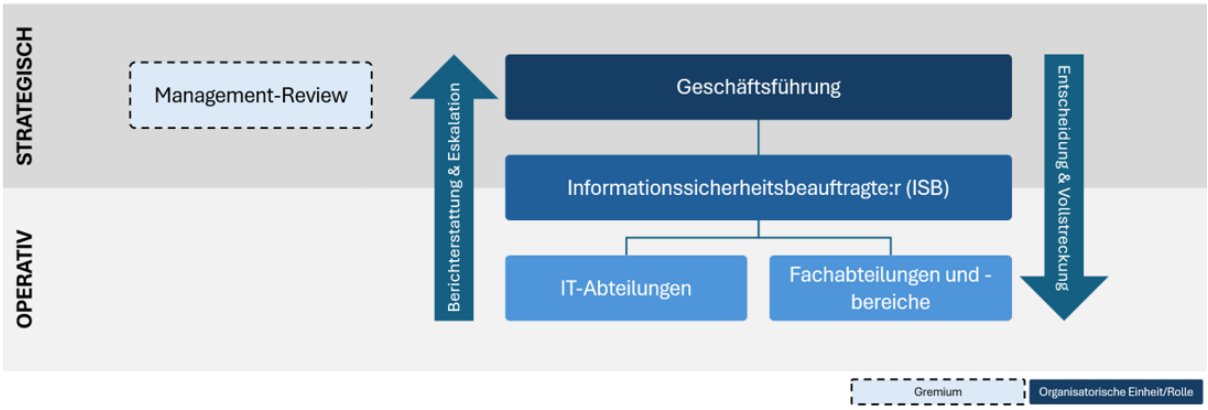

Abbildung 5.1: Beispielhafte Informationssicherheitsorganisation

Die dargestellte Struktur bildet eine Idealorganisation zur Veranschaulichung der Governance-Logik ab, insbesondere im Sinne der Trennung zwischen operativer Umsetzung und strategischer Verantwortung. Der:die ISB koordiniert operativ die Umsetzung sicherheitsrelevanter Maßnahmen in den IT- und Fachabteilungen und berichtet direkt an die Geschäftsführung als oberste Leitungsebene. Diese ist auf strategischer Ebene für Grundsatzentscheidungen, Prioritätensetzung und Ressourcenvergabe verantwortlich und wird im Rahmen des Management-Reviews (Gremiums) regelmäßig eingebunden. Die Trennung zwischen operativer (Umsetzung) und strategischer (Steuerung und Verantwortung) Ebene unterstützt eine klare Steuerung und macht Verantwortungs- sowie Berichtslinien nachvollziehbar und prüfbar. In der praktischen Realität von KMUs kann die Umsetzung vereinfacht erfolgen, wobei hier wie schon zuvor erwähnt Interessenkonflikte berücksichtigt werden müssen.

Ergänzend wurden die in der Organisationsstruktur definierten Rollen (insbesondere der obersten Leitungsebene sowie des:der ISB), Gremien sowie organisatorischen Einheiten samt Beschreibung und Hauptverantwortlichkeiten in der zuvor erwähnten Informationssicherheitsleitlinie schriftlich definiert und damit formell verankert (nähere Informationen zu Rollen und Verantwortlichkeiten werden im Kapitel zu 5.2.2 behandelt). Ein weiteres zentrales Instrument stellt die entwickelte Berichtsvorlage im Präsentationsformat dar, welche

es erlaubt, die in der Durchführungsverordnung geforderten Themen, etwa zur Umsetzung von Sicherheitsmaßnahmen, den Risikoanalysen, Sicherheitsvorfällen oder Compliance-Status, mindestens einmal jährlich strukturiert an die oberste Leitungsebene zu berichten. Die Vorlage orientiert sich inhaltlich an den Vorgaben der Verordnung und stellt eine praktikable Arbeitsgrundlage für Informationssicherheitsverantwortliche (z.B. ISB) dar. Die Inhalte der Berichtsvorlage können auf Basis, der in Kapitel 5.3.2 erstellen Key Performance Indicators (KPIs) erstellt werden. Alle Vorlagen sind bewusst anpassbar gestaltet, sodass KMUs sie an ihre spezifischen Anforderungen, ihre Größe und ihre bestehende Organisationsstruktur angleichen können.

5.2 Sicherheitsrichtlinien

Dieser Themenbereich behandelt spezifischer die zentralen Anforderungen im Zusammenhang mit dem Konzept für die Sicherheit von Netz- und Informationssystemen (Informationssicherheitsleitlinie) sowie ergänzender themenspezifischer Richtlinien. Darüber hinaus werden die Definition und Zuweisung von Rollen und Verantwortlichkeiten innerhalb der Informationssicherheitsorganisation näher thematisiert.

5.2.1 Sicherheitsrichtlinien

Mapping - NIS2 Durchführungsverordnung (Punkt 1.1.): Es wird gefordert, dass ein „Konzept für die Sicherheit von Netz- und Informationssystemen“ vorhanden sein muss, welches

- den Ansatz für das Management der Informationssicherheit darlegt (1.1.1. a),
- die Sicherheitsziele definiert (1.1.1. c),
- einen Bezug zur Geschäftsstrategie hat (1.1.1. b),
- die kontinuierliche Verbesserung beschreibt (1.1.1. d),
- die Bereitstellung von Ressourcen sicherstellt (1.1.1. e),
- die Verantwortlichkeiten regelt (1.1.1. g),
- die Dokumentationspflichten beschreibt (1.1.1. h),
- die themenspezifischen Richtlinien benennt (1.1.1. i),
- die Metriken und Key Point Indicators (KPIs) definiert (1.1.1. j),
- allen Mitarbeiter:innen sowie relevanten Parteien mitgeteilt wird (1.1.1. f),
- und die Genehmigung durch die Unternehmensleitung beinhaltet (1.1.1. k).

Außerdem muss das Konzept mindestens einmal jährlich und zusätzlich anlassbezogen (z.B. bei Sicher-

heitsvorfällen) geprüft und gegebenenfalls aktualisiert werden, wobei die Änderungen dokumentiert werden müssen und die Ergebnisse der Leitungsebene berichtet werden müssen.

Interpretation der Anforderungen: Während Kapitel 5.1 die strategische Rolle der Leitungsorgane im Kontext der Informationssicherheit in den Fokus stellte, befasst sich dieser Punkt der Verordnung mit der konkreten inhaltlichen Ausarbeitung und fortlaufenden Pflege der zentralen Informationssicherheitsleitlinie sowie der dazugehörigen themenspezifischen Richtlinien. Die Informationssicherheitsleitlinie fungiert, wie bereits erwähnt, als zentrales Steuerungsinstrument auf operativer und strategischer Ebene. Sie formuliert nicht nur übergeordnete Sicherheitsziele und Grundsätze, sondern verweist auch auf sämtliche relevanten themenspezifischen Richtlinien, etwa im Bereich der Zugangssteuerung, Kryptographie oder der Sicherheit von Lieferketten. Zielsetzung dieser Anforderung ist die Etablierung eines flexiblen, dokumentierten Regelwerks, welches einerseits als Orientierungshilfe für Mitarbeitende dient und andererseits eine konsistente Umsetzung technischer wie organisatorischer Maßnahmen gewährleistet.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt es sich, die Informationssicherheitsleitlinie als kompaktes, verständliches Dokument zu gestalten, das den Einstieg in ein strukturiertes ISMS ermöglicht. Ein Umfang von fünf bis zehn Seiten ist ausreichend, um Relevanz, Lesbarkeit und Umsetzbarkeit sicherzustellen, insbesondere mit begrenzten Ressourcen. Die Informationssicherheitsleitlinie selbst muss abgestimmt mit der Unternehmensstrategie und -ziele sein und unter anderem folgende Elemente enthalten:

- Geltungsbereich und Zielsetzung
- Sicherheitsziele und Grundprinzipien (Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität) → z.B. orientieren an IT-Grundschutzziele als Basis
- Verweis auf themenspezifische Richtlinien
- Rollen und Verantwortlichkeiten
- Verpflichtung zur kontinuierlichen Verbesserung und Bereitstellung notwendiger Ressourcen
- Dokumentationsanforderungen, Kennzahlen zur Erfolgsmessung
- Datum und Freigabe durch die Geschäftsleitung

Die Inhalte dieser Informationssicherheitsleitlinie orientieren sich an den Anforderungen der NIS2-Durchführungsverordnung und sind in der in Kapitel 5.1 erwähnten Muster-Vorlage bereits strukturiert abgebildet. Sie muss durch die KMUs individuell angepasst und kann als Arbeitsgrundlage genutzt werden. Nach interner Abstimmung sollte die Informationssicherheitsleitlinie formell durch die oberste Leitung (z.B. im Zuge

eines Management-Reviews) freigegeben und anschließend organisationsweit bzw. an relevante Stakeholder (z.B. Dienstleister) kommuniziert werden. Dies idealerweise begleitet durch Schulungs- und Awareness-Maßnahmen. Die in der Vorlage enthaltene Änderungshistorie dokumentiert alle Überarbeitungen inklusive Datum, Änderungsgrund und verantwortlicher Person, und trägt zur Revisionssicherheit bei. Die in Kapitel 5.1 der Vorlage für die Informationssicherheitsleitlinie dargestellte ISMS-Dokumentenstruktur (siehe Abbildung 5.2) zeigt die Verbindung zwischen der Leitlinie, themenspezifischen Richtlinien, Prozessen und Nachweisdokumenten und dient als Orientierung für den weiteren Aufbau. Die zu erstellenden themenspezifischen Richtlinien ergeben sich anhand der Anforderungen der NIS2, insbesondere bei jenen, wo ein Konzept gefordert wird.

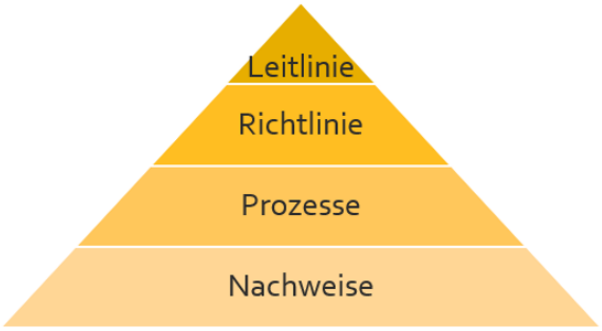

Abbildung 5.2: Beispielhafte ISMS-Dokumentenstruktur

Um die Pflege und Steuerung dieser Dokumente effizient umzusetzen, wurde eine Excel-Vorlage zur Dokumentenlenkung entwickelt, mit der KMUs Zuständigkeiten, Prüffristen und Freigaben übersichtlich verwalten können. Sie unterstützt sowohl die regelmäßige Überprüfung (mindestens jährlich und zusätzlich anlassbezogen) als auch die Einhaltung der formalen Anforderungen der NIS2.

5.2.2 Funktionen, Aufgaben und Verantwortlichkeiten

Mapping - NIS2 Durchführungsverordnung (Punkt 1.2): Im Abschnitt 1.2 der NIS2-Durchführungsverordnung wird gefordert, dass Einrichtungen ihre Verantwortlichkeiten und Weisungsbefugnisse im Bereich der Netz- und Informationssystemsicherheit klar definieren und diesen konkreten Rollen zuordnen (1.2.1). Diese Aufgabenverteilung muss dem Bedarf und der Struktur der jeweiligen Organisation entsprechen und soll auch den Leitungsorganen bekannt gemacht werden. Zudem ist sicherzustellen, dass alle Mitarbeitenden sowie Dritte, die Zugriff auf Netz- und Informationssysteme haben oder diese nutzen, zur Einhaltung der festgelegten Sicherheitskonzepte, Richtlinien und Verfahren verpflichtet werden (1.2.2). Die Sicherheitsaufgaben können, abhängig von der Unternehmensgröße, durch dedizierte Rollen oder im Rahmen bestehender

Rollen wahrgenommen werden (1.2.4). Dabei sind widersprüchliche oder konfliktträchtige Verantwortlichkeiten möglichst zu vermeiden (1.2.5), um eine wirksame Sicherheitsorganisation sicherzustellen.

Interpretation der Anforderungen: Die Anforderungen verfolgen das Ziel, Sicherheitsverantwortlichkeiten im Unternehmensalltag auf eine praxisnahe und organisatorisch umsetzbare Weise zu etablieren. Anders als die strategisch ausgerichteten Steuerungsaufgaben der Leitungsebene, wie sie in Kapitel 5.1 beschrieben wurden, steht hier die konkrete Umsetzung im operativen Bereich im Vordergrund. Es geht dabei insbesondere darum, wer innerhalb der Organisation für bestimmte sicherheitsrelevante Aufgaben zuständig ist und mit welchen Mechanismen die Einhaltung dieser Zuständigkeiten abgesichert werden kann. Dabei gilt, dass Sämtliche Mitarbeitende sowie gegebenenfalls externe Dienstleistende klar über ihre sicherheitsrelevanten Pflichten informiert und zur Einhaltung verpflichtet werden müssen. Verantwortlichkeiten dürfen sich nicht überschneiden oder widersprüchlich sein (z.B. keine gleichzeitige Kontrolle und Ausführung sicherheitsrelevanter Tätigkeiten).

Umsetzung im NIS2-ISMS-Framework: Für KMUs bedeutet die Umsetzung der Anforderungen aus Abschnitt 1.2, dass sie eine klare, dokumentierte Aufgaben- und Rollenzuordnung für die Informationssicherheit schaffen müssen. Während Aspekte wie die Benennung einer verantwortlichen Person, Berichtslinien zur Geschäftsleitung und regelmäßige Überprüfung der Struktur bereits in Kapitel 5.1 behandelt wurden (siehe Anforderungen 1.2.1, 1.2.3 und 1.2.6 der Verordnung), liegt der Fokus hier auf der praktischen Umsetzung im Unternehmensalltag.

Zentral ist die detaillierte Definition der Funktionen und Zuständigkeiten für alle sicherheitsrelevanten Aufgaben insbesondere im IT-Betrieb, in den Fachabteilungen und bei ausgelagerten Dienstleistungen. Zur Unterstützung wurde im Rahmen dieser Arbeit eine strukturierte Vorlage zur Informationssicherheitsorganisation entwickelt. Sie bildet die zentralen Rollen, Gremien und Berichtslinien grafisch ab und unterstützt KMUs dabei, ihre Sicherheitsorganisation nachvollziehbar und prüfbar zu strukturieren. In Ergänzung dazu wurden die beschriebenen Rollen und Zuständigkeiten auch in der Informationssicherheitsleitlinie schriftlich dokumentiert. Dort sind die wichtigsten organisatorischen Funktionen, insbesondere auf operativer Ebene, benannt, kurz beschrieben und formal verankert. Schließlich müssen auch alle Mitarbeitenden sowie relevante externe Partner zur Einhaltung der Verantwortlichkeiten und Sicherheitsvorgaben verpflichtet werden (siehe Anforderung 1.2.2 der Durchführungsverordnung). Dies kann pragmatisch über Regelungen in Arbeitsverträgen, Schulungsunterlagen oder durch regelmäßige Awareness-Maßnahmen erfolgen.

5.3 Risikomanagement

Das Risikomanagement bildet das Rückgrat eines jeden ISMS und steht im Zentrum der NIS2-Anforderungen. Es dient nicht nur der systematischen Identifikation, Analyse, Bewertung und Behandlung von Risiken, sondern stellt auch die Basis für viele weitere Maßnahmen wie Vorfallsmanagement oder Schulungsplanung dar. In diesem Kapitel werden die Anforderungen an einen NIS2-Risikomanagementprozess dargestellt und praxisgerecht für KMUs aufbereitet.

5.3.1 Risikomanagementrichtlinie und -prozess

Mapping - NIS2 Durchführungsverordnung (Punkt 2.1): Einrichtungen müssen ein angemessenes Rahmenwerk zum Risikomanagement etablieren und aufrechterhalten, um Risiken für die Sicherheit der Netz- und Informationssysteme zu identifizieren und zu adressieren (2.1.1). Hierzu gehört die Durchführung und Dokumentation von Risikoanalysen sowie die Ableitung, Umsetzung und Überwachung eines Risikobehandlungsplans. Ergebnisse und Restrisiken sind von der Geschäftsleitung oder risikoverantwortlichen Personen formell zu akzeptieren. Ein definierter Risikomanagementprozess muss Verfahren zur Identifikation, Analyse, Bewertung und Behandlung von Risiken beinhalten (2.1.2). Dieser Prozess soll Teil des allgemeinen Risikomanagementsystems sein und unter anderem folgende Anforderungen erfüllen:

- Anwendung einer Risikomanagementmethodik (2.1.2 a)
- Festlegung von Risikotoleranz und Risikokriterien (2.1.2 b-c)
- Gefahrenübergreifender Ansatz zur Risikodokumentation inklusive Drittparteien, Schwachstellen und Single Points of Failure (2.1.2 d)
- Risikoanalyse inklusive Bedrohung, Eintrittswahrscheinlichkeit, Auswirkung und Gesamtrisiko (2.1.2 e)
- Risikobewertung und Auswahl geeigneter Maßnahmen (2.1.2 f-g)
- Monitoring, Verantwortlichkeitszuweisung und Dokumentation in einem Risikobehandlungsplan (2.1.2 h-j)

Zusätzlich sind wirtschaftliche Aspekte, Effektivitätsbewertungen, Asset-Klassifikation und Business-Impact-Analysen bei der Auswahl der Maßnahmen zu berücksichtigen (2.1.3). Eine regelmäßige, mindestens jährliche Überprüfung der Risikoergebnisse und Behandlungspläne ist erforderlich (2.1.4). [10]

Interpretation der Anforderungen: Der dokumentierte Risikomanagementprozess stellt eine zentrale Säu-

le eines NIS2-ISMS dar. Er bildet nicht nur die Grundlage für eine strukturierte Identifikation, Analyse und Bewertung von Informationssicherheitsrisiken, sondern ist zugleich eng mit einer Vielzahl weiterer Themenbereiche der NIS2-Anforderungen verknüpft. Ziel dieses Prozesses ist es, auf systematischer und nachvollziehbarer Basis zu erfassen, welche Bedrohungen und Schwachstellen für die Assets einer Organisation bestehen, wie wahrscheinlich deren Eintreten ist und welche Auswirkungen dies auf die Sicherheit und Funktionsfähigkeit der Organisation hätte. Die daraus abgeleiteten Bewertungen und Priorisierungen dienen als Entscheidungsgrundlage für die Auswahl geeigneter Maßnahmen. Der Prozess ist nicht als einmalige Maßnahme zu verstehen, sondern muss zyklisch wie auch anlassbezogen durchgeführt, dokumentiert und aktualisiert werden. Nur so lässt sich sicherstellen, dass aktuelle Risikolagen, neue Bedrohungen sowie Veränderungen in der Systemlandschaft angemessen berücksichtigt werden. Damit wird der Risikomanagementprozess zum verbindenden Element und Steuerungsinstrument innerhalb des gesamten ISMS und ermöglicht eine risikoorientierte Umsetzung und kontinuierliche Verbesserung.

Umsetzung im NIS2-ISMS-Framework: Im Rahmen dieser Arbeit wurde ein pragmatischer, schlank gehaltener Umsetzungsansatz entwickelt, der auf typische Rahmenbedingungen von KMUs zugeschnitten ist. Zentraler Bestandteil ist das entwickelte IS-Risikomanagement-Handbuch, welches die methodische Vorgehensweise inklusive vordefinierter Risikokriterien, Verantwortlichkeiten und Prozessschritte beschreibt. Ergänzt wird dieses durch die Excel-Vorlage des Risikoregister und -behandlungsplans. Beide Vorlagen wurden so konzipiert, dass sie leicht verständlich sind und an die Bedürfnisse des Unternehmens angepasst werden müssen.

Der definierte Ansatz im Handbuch definiert folgende Phasen, welche aufeinander aufbauen:

1. **Vorbereitung und Grundvoraussetzungen:** Aufbau eines Asset-Inventars (siehe Kapitel 5.4), Definition der Risikokriterien (Eintrittswahrscheinlichkeit, Schadensausmaß, Risikolevel), formale Freigabe einer Risikoakzeptanzgrenze durch die oberste Leitungsebene sowie Vorbereitung einer praxistauglichen Bedrohungsliste für die Risikoanalyse. Ein besonderer wichtiger Unterpunkt ist die Durchführung der Business Impact Analyse, in welcher der Schutzbedarf, die RTO (maximale Wiederanlaufzeit) und die RPO (maximal tolerierter Datenverlust) der Assets identifiziert werden. Das genaue Vorgehen ist im IS-Risikomanagement-Handbuch detaillierter erklärt. Die Ergebnisse können in der vorbereiteten Vorlage der Business Impact Analyse eingetragen werden.
2. **Risikoanalyse:** Betrachtung der Assets mit hohem Schutzbedarf sowie anlassbezogener Risiken (z.B. aus Penetrationstests, Audits). Risiken werden als Kombination aus Asset bzw. dem konkreten Kon-

text, einer Bedrohung sowie einer ausnutzbaren Schwachstelle beschrieben. Eintrittswahrscheinlichkeiten werden mithilfe der definierten Kriterien bewertet. Das Schadensausmaß ergibt sich in der Regel aus der vorab durchgeführten Schutzbedarfsanalyse des Assets. Für nicht-assetbezogene (z.B. organisatorische) Risiken erfolgt eine manuelle Bewertung durch den:die ISB und Fachverantwortliche.

3. **Risikoevaluierung:** Die bewerteten Risiken werden einem Risiko-Level gemäß der Risiko-Matrix zugewiesen. Bewertungsergebnisse werden mit der definierten Risikoakzeptanzgrenze abgeglichen.
4. Risikobehandlung: Nicht akzeptable oder freiwillig zu behandelnde Risiken werden mit Maßnahmen adressiert. Entscheidungswege, etwa bei Behandlung trotz mittlerem Risiko, werden dokumentiert. Die Umsetzung wird überwacht, das Restrisiko bewertet und bei Bedarf durch die Geschäftsleitung genehmigt.
5. **Überwachung und Berichterstattung:** Alle Ergebnisse und Maßnahmen werden zentral im Risikoregister und -behandlungsplan dokumentiert. Das Excel fungiert als zentrales Arbeitsinstrument für Nachvollziehbarkeit, Steuerung und kontinuierliche Verbesserung. Der gesamte Prozess wird jährlich sowie anlassbezogen (z.B. bei neuen Bedrohungslagen oder Vorfällen) durch den:die ISB überprüft.

Zusätzlich ist auch das Reporting ein wichtiger Bestandteil im Rahmen des Risikomanagements. Die regelmäßig durchgeführten Risikoanalysen, Bewertungen und Behandlungsmaßnahmen werden durch den:die ISB in einem strukturierten Format an die oberste Leitungsebene kommuniziert. Hierfür wurde im Rahmen dieser Arbeit die Präsentationsvorlage entwickelt (siehe Kapitel 5.1.1).

5.3.2 Beurteilung der Effektivität von Risikomanagementmaßnahmen

Mapping - NIS2 Durchführungsverordnung (Punkt 7.): Gemäß Abschnitt 7 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, ein dokumentiertes Konzept sowie entsprechende Verfahren zu etablieren, um die Wirksamkeit ihrer umgesetzten Risikomanagementmaßnahmen im Bereich der Cybersicherheit systematisch zu bewerten (7.1). Dieses Konzept muss sich dabei auf die Ergebnisse der vorangegangenen Risikoanalysen (siehe Punkt 2.1 der Verordnung) sowie auf Erkenntnisse aus relevanten Sicherheitsvorfällen stützen (7.2). Inhaltlich wird gefordert, dass die Einrichtungen definieren, welche konkreten Maßnahmen, Verfahren und Kontrollen regelmäßig überwacht bzw. gemessen werden sollen (7.2 a). Dabei sind geeignete Methoden zur Durchführung der Überwachung, Messung, Analyse und Bewertung zu bestimmen, um die Gültigkeit und Aussagekraft der Ergebnisse sicherzustellen (7.2 b). Ebenso ist festzulegen, in welchen Intervallen diese Aktivitäten durchzuführen sind (7.2 c) und wer für die operative Umsetzung,

Auswertung und Bewertung verantwortlich ist (7.2 d-f). Zusätzlich sieht die Durchführungsverordnung vor, dass dieses Bewertungsverfahren regelmäßig sowie bei erheblichen Vorfällen oder wesentlichen Änderungen im Betrieb oder Risikoumfeld überprüft und angepasst wird (7.3).

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt es sich, die Wirksamkeit von Sicherheitsmaßnahmen auf pragmatische, aber strukturierte Weise zu bewerten. Grundlage dafür ist ein Konzept für KPIs und Metriken, das zentrale Kennzahlen definiert, welche regelmäßig erhoben, analysiert und bewertet werden. Im Sinne der Anforderungen wurde im Rahmen dieser Arbeit ein simples, anwendungsfertiges und anpassbares KPI-Vorlagendokument entwickelt, das eine strukturierte Bewertung der Wirksamkeit umgesetzter Sicherheitsmaßnahmen ermöglicht. Die Vorlage deckt zentrale Themenbereiche der Cybersicherheit, insbesondere solche, die laut Durchführungsverordnung kontinuierlich überwacht, gemessen und analysiert werden müssen, ab. Für jeden Themenbereich (z.B. Risikomanagement, Cybersicherheitsvorfälle, Notfallmanagement) werden spezifische KPIs definiert, die folgende Elemente beinhalten:

- **Kennzahl / KPI:** z.B. Anzahl offener Risiken oder Phishing-Klickrate
- **Definition / Messgröße:** beschreibt, was konkret erfasst wird
- **Einheit:** z.B. Anzahl, Prozent
- **Zielwert / Toleranzgrenze:** definiert den akzeptablen Bereich der Wirksamkeit
- **Trend:** dient der langfristigen Bewertung der Entwicklung
- **Beispielhafte KPIs sind etwa:**
  - „Anzahl der Risiken über definierter Akzeptanzgrenze“ (Ziel: 0)
  - „Phishing-Klickrate bei Tests“ (Ziel: $< 10\%$)
  - „Lessons-Learned-Quote nach Vorfällen“ (Ziel: $\geq 90\%$)
  - „Beteiligung der Leitungsebene am Management-Review“ (Ziel: mind. 1x p.a.)

Die Bewertung der Kennzahlen erfolgt in regelmäßigen Intervallen, Best-Practice mäßig mindestens einmal jährlich, und wird von dem:der ISB aggregiert und im Rahmen des Management-Reviews der obersten Leitungsebene präsentiert. Die definierten KPIs stellen bewusst eine beispielhafte Auswahl dar. Jedes KMU muss individuell beurteilen, welche Kennzahlen sinnvoll, relevant und mit vertretbarem Aufwand messbar sind. Entscheidend ist nicht die Anzahl der KPIs, sondern deren Aussagekraft für die tatsächliche Wirksamkeit der Sicherheitsmaßnahmen.

5.3.3 Überwachung der Einhaltung von Vorgaben

Mapping - NIS2 Durchführungsverordnung (Punkt 2.2.): Gemäß Abschnitt 2.2 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, regelmäßig die Einhaltung ihrer sicherheitsbezogenen Konzepte, themenspezifischen Richtlinien sowie relevanter Vorschriften und Normen zu überprüfen (2.2.1). Diese Überprüfungen müssen in ein geeignetes Berichtsformat überführt werden, das den Leitungsorganen einen fundierten Überblick über den Stand der Informationssicherheit sowie die Umsetzung des Risikomanagements vermittelt (2.2.2). Das Berichtssystem muss dabei auf den jeweiligen Unternehmenskontext, insbesondere den organisatorischen Strukturen, dem Betriebsumfeld und der aktuellen Bedrohungslage, angepasst sein. Darüber hinaus verlangt Punkt 2.2.3, dass die Überwachungsmaßnahmen nicht nur in geplanten Intervallen, sondern auch anlassbezogen, etwa bei sicherheitsrelevanten Vorfällen oder wesentlichen organisatorischen und technischen Veränderungen, durchgeführt werden.

Interpretation der Anforderung: Diese Anforderung verpflichtet Organisationen dazu, die Einhaltung ihrer eigenen Konzepte, Richtlinien und Verfahren regelmäßig zu prüfen. Für KMUs bedeutet dies in der Praxis, dass der:die ISB gezielte Stichproben z.B. an sicherheitsrelevanten Kontrollpunkten wie in Projekten, im Änderungsmanagement oder bei der Einführung neuer Systeme durchführt. Dabei liegt der Fokus auf der Überprüfung der Umsetzung interner Vorgaben, insbesondere der themenspezifischen Richtlinien. Ziel ist es, den Umsetzungsgrad zu ermitteln, Schwachstellen frühzeitig zu erkennen und gezielt Verbesserungen bzw. Sicherheitsmaßnahmen abzuleiten.

Umsetzung im NIS2-ISMS-Framework: Es empfiehlt sich ein pragmatischer, fokussierter Ansatz, bei dem die Einhaltung der wichtigsten themenspezifischen Richtlinien (z.B. Zugriffsmanagement, Vorfallmanagement, Backup, Patchmanagement) in regelmäßigen Stichproben durch den:die ISB überprüft wird. Die Überprüfung erfolgt risikoorientiert, also an Stellen mit hohem Schutzbedarf oder Relevanz für kritische Geschäftsprozesse/Dienstleistungen.

Ziel ist es, konkrete Aussagen darüber treffen zu können:

- Ob die dokumentierten Vorgaben tatsächlich im operativen Betrieb umgesetzt werden,
- Ob Schwachstellen oder Abweichungen bestehen,
- Und ob daraus Verbesserungsmaßnahmen abgeleitet werden müssen.

Die Ergebnisse dieser Einhaltungskontrollen sind eng mit dem Risikomanagementprozess verknüpft: Fest-

gestellte Abweichungen oder Schwachstellen stellen potenzielle Risiken dar und fließen, sofern relevant, in die Risikoanalyse ein. Geplant werden diese Überwachungen/Prüfungen im Rahmen eines Prüfungsprogramms, welches im Normalfall alle Prüfungen (auch unabhängige sowie technische; siehe Kapitel 5.9.4) für die nächste drei Jahre plant. Für jede konkrete Prüfung innerhalb Programms muss jährlich im Rahmen eines Prüfungsplans die Prüfung detaillierter geplant werden (Umfang, Verantwortlichkeiten, Zeitraum, Methode, etc.). Nähere Informationen zum Programm und Plan sind im nächsten Kapitel 5.3.4 zu finden.

Zur strukturierten Durchführung der einzelnen stichprobeartigen Prüfungen kann eine einfache Checkliste eingesetzt werden, welche je nach Umfang der Prüfung angepasst werden muss. Im Rahmen dieser Arbeit wurde eine entsprechende Vorlage entwickelt, welche folgende Elemente abbildet:

- Richtlinie / Themenbereich (z.B. „Zugriffsmanagement“),
- Kontrollpunkt / Erwartung (z.B. „Werden Rechte regelmäßig überprüft?“),
- Stichprobe / Prüfumfang (z.B. „3 ausgewählte Systeme“),
- Ergebnis / Feststellung (z.B. „1 System ohne aktuelle Rechteprüfung“),
- Verantwortlichkeit (Rolle / Abteilung)
- Abweichung (Ja/Nein)
- In Risikoanalyse einbringen (Ja/Nein)
- Risiko-ID (Verlinkung zu Risikoregister, wo die Abweichung detaillierter betrachtet wird)

Die Ergebnisse werden dokumentiert und aggregiert in das Management-Review eingebracht.

5.3.4 Unabhängige Überprüfungen

Mapping - NIS2 Durchführungsverordnung (Punkt 2.3.): Im Abschnitt 2.3 der NIS2-Durchführungsverordnung wird von den Einrichtungen gefordert, dass sie ihren Ansatz zum Management der Sicherheit von Netz- und Informationssystemen unabhängig überprüfen (2.3.1). Diese Überprüfungen sollen nicht nur die Verfahren und technischen Maßnahmen, sondern auch die organisatorischen Strukturen (z.B. Rollen und Zuständigkeiten) einbeziehen. Gemäß Punkt 2.3.2 müssen hierfür geeignete Verfahren und Zuständigkeiten definiert werden, um eine unabhängige Durchführung sicherzustellen. Dabei ist zu gewährleisten, dass die prüfenden Personen nicht dem überprüften Bereich unterstellt sind. Ist eine personelle Trennung in kleinen Unternehmen nicht möglich, sind alternative Maßnahmen zur Sicherstellung der Unparteilichkeit erforderlich. Darüber hinaus ist gemäß 2.3.3 vorgeschrieben, dass die Ergebnisse dieser unabhängigen Überprüfungen an die oberste Leitungsebene berichtet werden. Darauf basierend sind entweder Korrekturmaßnahmen

zu ergreifen oder verbleibende Restrisiken zu akzeptieren, unter Berücksichtigung der Risikoakzeptanzkriterien des Unternehmens. Laut Punkt 2.3.4 sind diese unabhängigen Überprüfungen in geplanten Zeitabständen sowie bei sicherheitsrelevanten Vorfällen oder signifikanten Änderungen an Prozessen oder Risiken durchzuführen.

Interpretation der Anforderungen: Im Gegensatz zur internen Überwachung wie im vorherigen Punkt, welche sich auf die Einhaltung interner Vorgaben fokussiert, fordert Abschnitt 2.3 eine systematische und unabhängige Gesamtüberprüfung des ISMS im Hinblick auf die Einhaltung der NIS2. Dies bedeutet eine objektive Beurteilung, ob die eingesetzten Prozesse, Rollen, Verfahren und Maßnahmen insgesamt angemessen und wirksam sind. Diese Überprüfung darf nicht durch Personen durchgeführt werden, die direkt an der Umsetzung oder Steuerung des ISMS beteiligt sind. Für KMUs bedeutet dies, dass sofern keine interne unabhängige Instanz wie eine interne Revision vorhanden ist, auf externe Prüfer:innen zurückgegriffen werden sollte, z.B. spezialisierte Beratungen oder Auditdienstleister:innen. Entscheidend ist, dass die Unabhängigkeit und Fachkompetenz der Prüfer:innen gewährleistet ist, um eine unparteiische Bewertung der NIS2-Compliance sicherzustellen.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt es sich, die unabhängige Überprüfung der Informationssicherheit mit einem strukturierten, aber ressourcenschonenden Vorgehen zu planen und umzusetzen. Ein bewährter erster Schritt ist dabei die Erstellung eines mehrjährigen Prüfprogramms, welches die langfristige Planung, Priorisierung und Zuteilung von Prüfungsschwerpunkten ermöglicht. Damit wird sichergestellt, dass alle relevanten Bereiche des ISMS in einem angemessenen Turnus überprüft werden ohne dabei Kapazitätsgrenzen zu überschreiten.

Im Rahmen dieser Arbeit wurde eine Vorlage für ein Prüfprogramm entwickelt, welche, wie im vorangegangenen Kapitel empfohlen, ein dreijähriges, rollierendes Prüfmodell abbildet. Das Ziel dieser Vorlage ist es, neben unabhängigen Prüfungen auch Synergien zwischen verschiedenen Prüf- und Überwachungsmaßnahmen zu nutzen. Es erscheint zweckmäßig, im Sinne einer ganzheitlichen Steuerung auch weitere relevante Prüfaktivitäten in das Programm zu integrieren. Dazu zählen insbesondere organisatorische Überprüfungen zur Einhaltung interner Vorgaben (siehe Kapitel 5.3.3) sowie technische Sicherheitsüberprüfungen wie Penetrationstests und Schwachstellenscans (siehe Kapitel 5.9.4). Durch diese Integration wird eine zentrale, transparente und umfassende Übersicht über alle sicherheitsrelevanten Prüfmaßnahmen gewährleistet.

Im nächsten Schritt erfolgt die konkrete Planung und Durchführung der einzelnen Prüfungen entsprechend des festgelegten Programms mittels detaillierten Prüfungsplänen. Diese Pläne enthalten:

- eine klare Zieldefinition und Abgrenzung des Prüfumfangs,
- Informationen zur Durchführungsperson oder -stelle (intern oder extern),
- standardisierte Felder zur Erfassung der Prüfergebnisse und etwaiger Schwachstellen und Abweichungen,
- sowie eine Maßnahmenübersicht mit Fristen und Zuständigkeiten.

Die Auswahl der prüfenden Stelle erfolgt unter Berücksichtigung der in der Durchführungsverordnung geforderten Unabhängigkeit: Ist intern keine organisatorische Trennung möglich, empfiehlt sich der Rückgriff auf externe Prüfpersonen, etwa spezialisierte Unternehmensberatungen oder Auditor:innen mit entsprechender Qualifikation.

Die Ergebnisse der Prüfungen fließen in das Risikomanagement als anlassbezogene Risiken ein sowie in die Berichterstattung an die oberste Leitungsebene (im Rahmen des jährlichen Management-Reviews). Das hier beschriebene Vorgehen stellt einen anpassbaren, praxisorientierten Vorschlag dar. Die Vorlagen dienen als Ausgangspunkt und müssen jeweils auf die individuellen Gegebenheiten, Risiken und vorhandenen Ressourcen des KMUs abgestimmt werden.

5.4 Verwaltung von Vermögenswerten

Ein vollständiger Überblick über alle sicherheitsrelevanten Assets eines Unternehmens ist eine elementare Voraussetzung für wirksamen Informationsschutz. Erst durch die systematische Erfassung, Klassifikation und Zuordnung lassen sich Schutzbedarfe und Risiken nachvollziehbar ableiten und Maßnahmen gezielt steuern. Dieses Kapitel zeigt, wie KMUs den Aufbau und die Pflege eines Asset-Managements effizient umsetzen können.

5.4.1 Inventarisierung von Vermögenswerten

Mapping - NIS2 Durchführungsverordnung (Punkt 12.4.): Gemäß Abschnitt 12.4 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, ein umfassendes und aktuelles Inventar ihrer Werte zu erstellen und zu pflegen (12.4.1). Dieses Inventar muss alle relevanten Vermögenswerte umfassen, die für die Betriebsabläufe und Dienste der Einrichtung von Bedeutung sind. Änderungen im Inventar sind nachvoll-

ziehbar zu dokumentieren, um die Integrität und Aktualität der Informationen sicherzustellen. Die Granularität des Inventars sollte dem spezifischen Bedarf der Einrichtung entsprechen (12.4.2). Dies bedeutet, dass das Inventar sowohl eine Liste der Betriebsabläufe und Dienste mit entsprechenden Beschreibungen (12.4.2 a) als auch eine Liste der unterstützenden Netz- und Informationssysteme sowie anderer zugehöriger Anlagen und Werte enthalten muss (12.4.2 b). Darüber hinaus sind Einrichtungen verpflichtet, das Inventar regelmäßig zu überprüfen und zu aktualisieren (12.4.3). Diese Überprüfungen sollen sicherstellen, dass alle Änderungen erfasst und dokumentiert werden, um eine kontinuierliche Genauigkeit und Kohärenz des Inventars zu gewährleisten.

Interpretation der Anforderungen: Die Anforderungen betonen die Bedeutung eines vollständigen und aktuellen Überblicks über alle sicherheitsrelevanten Vermögenswerte („Assets“) eines Unternehmens. Ein zentrales Ziel der Anforderung ist es, sicherzustellen, dass alle Assets, die zur Erbringung von Geschäftsprozessen und Dienstleistungen beitragen, in einem strukturierten Inventar dokumentiert und regelmäßig aktualisiert werden. Dieses Inventar bildet die Grundlage für zahlreiche nachgelagerte Sicherheitsprozesse z.B. für die Schutzbedarfsfeststellung, Risikoanalyse, Business-Impact-Analyse oder die Entwicklung von Notfallplänen. Die Granularität des Inventars soll sich dabei nach den tatsächlichen Bedürfnissen der Einrichtung richten. Für KMUs bedeutet das, dass eine übersichtliche und auf die Geschäftsprozesse konzentrierte Erfassung in der Regel ausreichend ist, sofern zentrale Dienste und Systeme klar beschrieben und nachvollziehbar dokumentiert sind. Die regelmäßige Überprüfung und Pflege des Inventars (z.B. bei Systemwechseln oder organisatorischen Veränderungen) ist ebenfalls verpflichtend, um dessen Aktualität sicherzustellen. Änderungen müssen dabei nachvollziehbar, beispielsweise durch eine Änderungshistorie oder automatisierte Änderungsprotokolle innerhalb eines IT-gestützten Asset-Management-Tools, protokolliert werden. Im Gegensatz zu Best-Practices und Standards fordert die NIS2 Durchführungsverordnung im Hinblick auf Verantwortlichkeiten, keine explizite Zuweisung von Asset-Eigentümer:innen z.B. Personen oder Abteilungen.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt sich eine pragmatische und integrierte Umsetzung der Anforderung zur Erstellung und Pflege eines vollständigen Asset- und Werteinventars. Anstatt einen separaten, rein technischen Inventarprozess aufzubauen, kann die Asset-Erhebung sinnvoll in die Durchführung der BIA, wie sie auch im Rahmen des Risikomanagements ohnehin vorgesehen ist (siehe 5.3), integriert werden.

Im Zuge der BIA werden in Workshops mit den Fachabteilungen bereits jene IT-Anwendungen identifiziert,

die für kritische Geschäftsprozesse oder Dienstleistungen essenziell sind. Diese Anwendungen bilden die erste Ebene des Asset-Inventars. Die darunterliegende Infrastruktur (z.B. Server, Netzwerke, Speicherlösungen, physische Räumlichkeiten) wird anschließend durch die IT-Abteilung ergänzt. Der Schutzbedarf vererbt sich dabei von der Anwendung auf die darunterliegenden technischen Assets. Alternativ können Open-Source-basierte Tools mit Asset-Discovery-Funktionen eingesetzt werden, um einen ersten grundlegenden Überblick über alle im Netzwerk vorhandenen Systeme zu erhalten. Beispiele für solche Tools sind:

- Lansweeper
- Cacti
- OCS inventory
- Open-AudIT

Zur praktischen Umsetzung wurde im Rahmen dieser Arbeit eine Excel-Vorlage entwickelt, welche eine strukturierte und anpassbare Inventarisierung der erfassten Assets ermöglicht. Die Vorlage enthält unter anderem:

- Asset-Klasse (z.B. Anwendung, Server, Dienstleister:in),
- Beschreibung und Verantwortlichkeit,
- zugeordnete Geschäftsprozesse / Dienste,
- Schutzbedarfsstufen (aus der Schutzbedarfsanalyse abgeleitet),
- Status der Aktualität,
- Änderungsverlauf.

Die Einträge werden gemeinsam mit der IT und den Fachbereichen initial aufgenommen und mindestens einmal jährlich oder anlassbezogen, wenn sich wesentliche technische oder organisatorische Änderungen ergeben (z.B. Einführung neuer Software, Migrationen, Auslagerungen), überprüft. Änderungen am Inventar werden dokumentiert.

5.4.2 Klassifikation von Vermögenswerten

Mapping - NIS2 Durchführungsverordnung (Punkt 12.1.): Gemäß Abschnitt 12.1 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, ein Klassifizierungssystem für alle Vermögenswerte (einschließlich Informationen) zu entwickeln, die in den Anwendungsbereich der Netz- und Informationssysteme fallen (12.1.1). Ziel ist es, für jede Anlage bzw. jeden Wert ein angemessenes Schutzniveau zu definieren. Dazu müssen Einrichtungen gemäß Punkt 12.1.2 ein systematisches Klassifizierungsmodell etablieren,

das auf den Schutzzielen Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit basiert (12.1.2 b). Die Klassifizierung muss den spezifischen Anforderungen hinsichtlich Sensibilität, Kritikalität, Risiko und Geschäftswert des jeweiligen Vermögenswerts gerecht werden. Insbesondere die Verfügbarkeitsanforderungen sind gemäß 12.1.2 c mit den Vorgaben aus dem Notfallmanagement, vor allem den dort definierten Wiederherstellungszielen, abzustimmen. Darüber hinaus verlangt Punkt 12.1.3, dass die Klassifizierungen regelmäßig überprüft und bei Bedarf angepasst werden, um Relevanz und Aktualität sicherzustellen.

Interpretation der Anforderungen: Die Anforderungen zielen darauf ab, ein strukturiertes und nachvollziehbares Klassifizierungssystem zu etablieren, das den Schutzbedarf von Assets differenziert abbildet. Dabei steht die Bewertung entlang der vier Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität im Vordergrund. Ziel ist es, eine fundierte Grundlage zur Priorisierung und Auswahl geeigneter Sicherheitsmaßnahmen zu schaffen. Besonderes Augenmerk liegt auf einer ganzheitlichen Bewertung, die neben technischen Kriterien auch betriebswirtschaftliche Faktoren wie Kritikalität für Geschäftsprozesse, Sensibilität der verarbeiteten Daten oder den potenziellen Schaden bei Verlust berücksichtigt. Die Anforderung zur regelmäßigen Überprüfung verdeutlicht, dass die Klassifikation ein dynamisches Steuerungselement im ISMS darstellt und nicht als einmalige Aktivität verstanden werden darf. Nur durch kontinuierliche Anpassung kann gewährleistet werden, dass Schutzmaßnahmen an veränderte Gegebenheiten angepasst werden.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt es sich, die Anforderungen an die Asset-Klassifikation möglichst pragmatisch und ressourcenschonend in bestehende Abläufe zu integrieren. Ein effektiver Ansatz besteht darin, die Klassifizierungsstufen direkt aus der im Rahmen der Schutzbedarfsanalyse (im Zuge des Risikomanagements) ermittelten Werte abzuleiten. Diese Vorgehensweise schafft Konsistenz mit dem Risikomanagementprozess, reduziert den administrativen Aufwand und erhöht die Nachvollziehbarkeit.

Die Bewertung erfolgt entlang der vier Schutzziele, wobei jedes Asset einer Stufe (z.B. Hoch, Mittel, Gering) zugeordnet wird. Ergänzend zur Asset-Klassifikation ist auch eine Informationsklassifikation sinnvoll, beispielsweise über einfache Stufen wie öffentlich, intern, vertraulich und streng vertraulich. Für KMUs genügt oft eine pauschale Zuweisung dieser Stufen zu Dokumentenarten oder Datentypen (z.B. Verträge, Personaldaten, interne E-Mails). Die Umsetzung kann über einfache Richtlinien oder Dokumentenkennzeichnungen erfolgen (siehe nächstes 5.4.3).

Zur operativen Unterstützung wurde im Rahmen dieser Arbeit die Vorlage des Asset-Inventars um ein Klassifizierungsmodul erweitert. Dieses erlaubt eine strukturierte Zuordnung der Klassifizierungen je Asset sowie die Dokumentation von Verantwortlichkeiten, Review-Zyklen und Änderungen.

5.4.3 Handhabung von Vermögenswerten

Mapping - NIS2 Durchführungsverordnung (Punkt 12.2.): Gemäß Abschnitt 12.2 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, ein Konzept für den sicheren und ordnungsgemäßen Umgang mit allen sicherheitsrelevanten Anlagen und Werten, einschließlich Informationen, zu entwickeln, umzusetzen und anzuwenden (12.2.1). Dieses Konzept muss mit dem übergeordneten Sicherheitskonzept der Netz- und Informationssysteme abgestimmt sein und allen Personen zugänglich gemacht werden, die mit diesen Anlagen und Werten arbeiten. Das Konzept muss gemäß 12.2.2 den gesamten Lebenszyklus der Anlagen und Werte, Anschaffung über Nutzung, Speicherung, Transport bis hin zur Entsorgung, abdecken (12.2.2 a). Es sind verbindliche Vorgaben zur sicheren Nutzung, Aufbewahrung, Übermittlung und endgültigen Löschung oder Vernichtung zu definieren (12.2.2 b). Zudem muss sichergestellt werden, dass die Übertragung von Anlagen und Werten entsprechend ihrer Sensibilität abgesichert erfolgt (12.2.2 c). Schließlich verlangt Punkt 12.2.3 eine regelmäßige Überprüfung und Aktualisierung des Konzepts, insbesondere bei sicherheitsrelevanten Vorfällen oder signifikanten organisatorischen oder technischen Änderungen.

Interpretation der Anforderungen: Die Anforderungen aus Abschnitt 12.2 der NIS2-Durchführungsverordnung zielen auf einen sicheren und nachvollziehbaren Umgang mit allen sicherheitsrelevanten Vermögenswerten über deren gesamten Lebenszyklus, von der Anschaffung über Nutzung und Transport bis hin zur Entsorgung, hinweg. Kern ist ein praxisnahes Konzept (also eine themenspezifische Richtlinie), das verbindliche Maßnahmen zur sicheren Handhabung, Speicherung, Löschung und Übertragung von physischen und digitalen Werten definiert. Das Konzept muss allen relevanten Personen bekannt sein, regelmäßig überprüft und bei Bedarf aktualisiert werden.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt sich eine schlanke, praxisnahe Umsetzung der Anforderung zur Handhabung von Vermögenswerten orientiert am Lebenszyklusprinzip. Im Fokus steht dabei nicht nur die technische, sondern auch die organisatorische Behandlung aller sicherheitsrelevanten Werte und Informationen, einschließlich deren Nutzung durch Mitarbeitende und Dienstleister:innen.

Ein zentrales Element ist die Entwicklung einer themenspezifischen Richtlinie zum Umgang von Assets,

welche als Teil des ISMS dokumentiert und kommuniziert wird. Sie definiert klare Regeln für den Umgang mit physischen, technischen und digitalen Vermögenswerten z.B. Laptops, Speichermedien, Zugangskarten oder sensiblen Dokumenten in allen Lebensphasen. Die Anforderungen orientieren sich an den jeweiligen Klassifizierungsstufen (siehe Kapitel 5.4.2). Entsprechend sind Schutzmaßnahmen (z.B. sichere Aufbewahrung, Verschlüsselung, Sperrung bei Verlust, sichere Vernichtung) verbindlich umzusetzen.

Für die Umsetzung wurde im Rahmen dieser Arbeit eine themenspezifische Richtlinie zum Thema Handhabung von Assets entwickelt. Diese Richtlinie enthält:

- Ein klares Klassifizierungs- und Behandlungsschema (z.B. öffentlich, intern, vertraulich, streng vertraulich)
- Konkrete Handlungsanweisungen für alltägliche Situationen (z.B. Ausdruck vertraulicher Dokumente)
- Regeln für Transport, Aufbewahrung und Entsorgung

Die Einhaltung der Richtlinie wird im Rahmen von Awareness-Maßnahmen geschult und durch Stichprobenkontrollen des:der ISB überwacht (siehe Kapitel 5.3.3).

5.4.4 Umgang mit Wechseldatenträger

Mapping - NIS2 Durchführungsverordnung (Punkt 12.3.): Gemäß Abschnitt 12.3 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, ein Konzept für den sicheren Umgang mit Wechseldatenträgern zu erstellen, umzusetzen und anzuwenden (12.3.1). Dieses Konzept muss allen Mitarbeitenden und Dritten zugänglich gemacht werden, die Wechseldatenträger innerhalb der Organisation oder in Verbindung mit deren Netz- und Informationssystemen einsetzen. Das Konzept muss gemäß 12.3.2 sicherstellen, dass Verbindungen mit Wechseldatenträgern grundsätzlich technisch gesperrt werden, es sei denn, es bestehen nachweisbare organisatorische Gründe für deren Einsatz (12.3.2 a). Darüber hinaus ist sicherzustellen, dass Selbstausführungen von Dateien auf Datenträgern verhindert und Datenträger vor Nutzung auf Schadsoftware gescannt werden (12.3.2 b). Es sind Schutzmaßnahmen für tragbare Speichermedien sowohl für gespeicherte als auch übertragene Daten (12.3.2 c) zu definieren. Falls erforderlich, sind auch kryptografische Maßnahmen zum Schutz sensibler Daten vorzusehen (12.3.2 d). Gemäß 12.3.3 ist das Konzept regelmäßig sowie anlassbezogen zu überprüfen und zu aktualisieren.

Interpretation der Anforderungen: Die Anforderungen aus Abschnitt 12.3 der NIS2-Durchführungsver-

ordnung zielen darauf ab, die technische und organisatorische Sicherheit im Umgang mit Wechseldatenträgern deutlich zu erhöhen. Hintergrund ist die hohe Relevanz dieser Medien für potenzielle Schadcode-Infektionen, Datenabflüsse und unbeabsichtigte Offenlegung sensibler Informationen, insbesondere in KMUs, wo oft weniger technische Barrieren bestehen. Zentrales Ziel ist es daher, die Nutzung von USB-Sticks, externen Festplatten, Speicherkarten und vergleichbaren Geräten auf das notwendige Maß zu beschränken, sie streng zu kontrollieren und dabei geeignete Schutzmaßnahmen umzusetzen. Zusätzlich müssen klare Regeln sowohl für firmeneigene als auch private Geräte zur Prüfung auf Schadsoftware, Verhinderung von Autostarts, Datenverschlüsselung und Nachvollziehbarkeit der Nutzung getroffen werden. Die regelmäßige Aktualisierung des Konzepts soll sicherstellen, dass neue Bedrohungslagen oder technische Entwicklungen berücksichtigt werden.

Umsetzung im NIS2-ISMS-Framework: Die geforderten Anforderungen wurden in die bestehende Richtlinienvorlage zur Handhabung von Assets aus Kapitel 5.4.3 um ein spezifisches Unterkapitel „Wechseldatenträger“ ergänzt. Dieses enthält die folgenden zentralen Regelungspunkte:

- **Technische Sperre als Standard:** Die Nutzung von Wechseldatenträgern ist systemseitig zu blockieren. Ausnahmen müssen organisatorisch begründet und durch den:die ISB dokumentiert und freigegeben werden.
- **Sicherheitsprüfung vor Nutzung:** Vor der Verwendung muss eine Prüfung auf Schadsoftware erfolgen. Autorun-Funktionen sind grundsätzlich zu deaktivieren.
- **Schutz in Transport und Lagerung:** Mobile Datenträger mit schützenswerten Informationen sind vor Verlust, Zugriff und Diebstahl zu sichern.
- **Verschlüsselung sensibler Inhalte:** Vertrauliche Daten auf Wechseldatenträgern sind mit geeigneter Kryptografie zu schützen.

Um diese Richtlinienpunkte in einem KMU-Kontext pragmatisch umzusetzen, bieten sich folgende technische und organisatorische Maßnahmen an:

- **Technische Sperre von Wechseldatenträgern:**
  - Windows: Einsatz von Gruppenrichtlinien (Group Policy Objects, „GPO“), um USB-Ports systemseitig zu deaktivieren bzw. gezielt freizugeben (z.B. nur für signierte Geräte).
  - Linux: Nutzung von „USBGuard“, einem Open-Source-Framework zur Policy-basierten Kontrolle über USB-Geräte.
- **Schadsoftwareprüfung & Autorun-Deaktivierung:**

  - Windows: Verwendung von Microsoft Defender Antivirus mit aktiviertem Echtzeitschutz sowie GPO zur Deaktivierung von AutoPlay/Autorun.
  - Linux: Einsatz von „ClamAV“ als Open-Source-Virenscanner, ideal für ressourcenschonende Umgebungen.
- **Schutz beim Transport und in der Lagerung:**
  - Organisatorische Maßnahmen: Beschriftungspflicht für Wechseldatenträger, Verwahrung in abschließbaren Schränken, Ausgabe über dokumentierte Ausleihprotokolle.
  - Physische Maßnahmen: Nutzung von Hardware mit physischen Zugriffsschutzmechanismen (z.B. Kensington-Schlösser, transportgesicherte Koffer bei Außeneinsätzen).
  - Praktische Umsetzungshilfe: Erstellung einer „Checkliste für Wechseldatenträger“ als Bestandteil der Awareness-Maßnahmen (siehe Kapitel 5.6).
- **Verschlüsselung:** Die Verschlüsselung von Daten auf mobilen Datenträgern ist bei vertraulichen oder personenbezogenen Informationen verpflichtend. KMUs sollten sich hierbei an bewährten technischen Standards orientieren:
  - Empfohlene Tools: BitLocker (Windows Pro/Enterprise), VeraCrypt (plattformunabhängig, Open Source)
  - Standardempfehlung: Orientierung an der BSI-Technischen Richtlinie „TR-02102-1“ [41], welche anerkannte Kryptographie-Verfahren und Schlüsselmanagementstandards für staatliche und wirtschaftliche Stellen definiert.

Eine detaillierte Betrachtung kryptografischer Grundlagen in Bezug auf den Punkt „Verschlüsselung“, empfohlener Algorithmen und Schlüsselstärken erfolgt im nachfolgenden Kapitel 5.10, welches eine Auswahl geeigneter Maßnahmen für KMUs beleuchtet und auch auf den Proportionalitätsrahmen der NIS2 eingeht.

5.4.5 Rücknahme oder Löschung von Vermögenswerten

Mapping - NIS2 Durchführungsverordnung (Punkt 12.5.): Gemäß Abschnitt 12.5 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, Verfahren festzulegen, umzusetzen und anzuwenden, die sicherstellen, dass alle sich im Besitz von Mitarbeitenden befindlichen Anlagen und Werte bei Beendigung des Beschäftigungsverhältnisses zurückgegeben, gelöscht oder anderweitig entzogen werden (12.5). Diese Vorgänge müssen nachvollziehbar dokumentiert werden. Ist eine Rückgabe oder Löschung nicht möglich z.B bei verlorenen Geräten oder nicht zurückführbaren Wechseldatenträgern, so ist sicherzustellen, dass von diesen kein Zugriff mehr auf Netz- und Informationssysteme möglich ist.

Interpretation der Anforderungen: Die Anforderung zielt darauf ab, die Informationssicherheit auch beim Austritt von Mitarbeitenden und auch Externen aus der Organisation aufrechtzuerhalten. In der Praxis bedeutet dies, dass Unternehmen über standardisierte Prozesse verfügen müssen, um sicherzustellen, dass bei einer Beendigung des Arbeitsverhältnisses keine sensiblen Informationen oder sicherheitsrelevanten Ressourcen unbeabsichtigt im Zugriff der betroffenen Person verbleiben. Dabei geht es nicht nur um die Rückgabe physischer Geräte (z.B. Laptops, USB-Sticks, Zugangskarten), sondern auch um digitale Themen, wie Benutzerkonten, Zugangsdaten oder Berechtigungen in Systemen. Zentral ist, dass diese Rückgaben, Löschungen und Sperrungen nachvollziehbar dokumentiert werden z.B. durch Checklisten oder Übergabeprotokolle. Falls eine Rückgabe oder vollständige Löschung nicht möglich ist, muss durch technische oder organisatorische Maßnahmen sichergestellt werden, dass keine Verbindung mehr zu den Netz- und Informationssystemen besteht (z.B. durch Deaktivierung des Accounts, Blockieren von IP-Adressen oder Entfernen aus Gruppen). Ziel ist es, unbeabsichtigte Sicherheitslücken zu vermeiden, die durch veraltete Zugänge oder unkontrollierte Geräte entstehen könnten.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt sich die Etablierung eines standardisierten, leicht umsetzbaren Offboarding-Prozesses, der sowohl organisatorische als auch technische Maßnahmen integriert. Dieser sollte automatisiert durch die HR-Abteilung angestoßen und durch die IT-Abteilung bzw. ISB begleitet werden. Zentrale Bestandteile sind:

- **Physische Rückgaben:** z.B. Laptop, Smartphone, USB-Sticks, Tür- und Zutrittskarten
- **Digitale Zugänge:** E-Mail-Postfächer, Cloud-Konten, interne Portale, VPN-/Zertifikatszugänge
- **Informationswerte:** z.B. sensible Dokumente, Projektdaten, lokal gespeicherte Inhalte

Die Prozesse zur Rückgabe und gegebenenfalls Löschung sind verbindlich zu dokumentieren. Dafür wurde im Rahmen dieser Arbeit eine Offboarding-Checklisten-Vorlage entworfen, die von der jeweiligen vorgesetzten Person gemeinsam mit der IT-Abteilung bzw. dem:der ISB und dem:der Mitarbeitenden durchgearbeitet und gegengezeichnet wird. Diese Checkliste erfüllt zugleich die regulatorische Anforderung der Nachweisführung über die Umsetzung der Anforderung.

Zusätzlich wurde die Umsetzung der Anforderungen durch eine Erweiterung der bestehenden Richtlinienvorlage zur Handhabung von Assets um das neue Kapitel „Abgabe, Rückgabe und Löschung“ konkretisiert. Diese Ergänzung beschreibt unter anderem den standardisierten Rückgabeprozess, die Dokumentationspflicht sowie den Umgang mit nicht mehr rückführbaren Assets. Um die Anforderung zur Abgabe, Rückga-

be und Löschung einfach und effizient in KMUs umsetzten zu können, empfehlen sich folgende Maßnahmen hierzu:

- **Technisch-organisatorisch:** Der Zugriff auf Systeme wird zentral deaktiviert (z.B. Benutzerkonten, VPN); bei Geräten ohne Rückgabe ist gegebenenfalls eine Sperrung auf Netzwerkebene (Firewall-Regel, MAC-Blockierung) erforderlich.
- **Sichere Datenlöschung:** Zur Unterstützung der sicheren Datenlöschung empfiehlt das BSI in dem Online-Artikel „Daten auf Festplatten, Datenträgern und Smartphones sicher löschen“ praxisgerechte Methoden wie das Überschreiben mit spezieller Software, den Einsatz von Herstellerbefehlen (z.B. „Secure Erase“) oder bei Defekten die physische Zerstörung des Speichermediums. Die BSI-Anleitung berücksichtigt dabei gängige Gerätearten (PCs, USB-Sticks, Smartphones) und warnt vor unsicheren Verfahren wie dem bloßen Formatieren oder Zurücksetzen auf Werkseinstellungen. [42]

5.5 Personalwesen

Einrichtungen müssen geeignete organisatorische Maßnahmen im Personalbereich umsetzen, um sicherzustellen, dass sicherheitsbezogene Aufgaben, Zuständigkeiten und Prozesse im Lebenszyklus der Beschäftigung geregelt und wirksam sind. Dies betrifft sowohl interne Mitarbeitende als auch direkte Dienstleister:innen und Lieferant:innen.

5.5.1 Sicherheit im Personalwesen

Mapping - NIS2 Durchführungsverordnung (Punkt 10.1.): Gemäß der NIS2-Durchführungsverordnung müssen betroffene Einrichtungen sicherstellen, dass ihre Mitarbeitenden sowie direkte Dienstleister:innen und Lieferant:innen die ihnen zugewiesenen Sicherheitsverantwortlichkeiten verstehen und einhalten (10.1.1). Hierzu sind geeignete Mechanismen vorzusehen, um die Einhaltung von etablierten Cyberhygienepraktiken (10.1.2 a), das Verständnis privilegierter Nutzer:innen für ihre Aufgaben und Befugnisse (10.1.2 b), die Kenntnis der Leitungsorgane über ihre sicherheitsbezogenen Verantwortungen (10.1.2 c) sowie die Auswahl qualifizierter Mitarbeitender auf Basis definierter Kriterien (10.1.2 d) sicherzustellen. Darüber hinaus ist die Zuordnung sicherheitsrelevanter Rollen regelmäßig, mindestens jedoch jährlich zu überprüfen und bei Bedarf anzupassen (10.1.3).

Interpretation der Anforderungen: Die Anforderungen verdeutlichen, dass Informationssicherheit nur dann wirksam umgesetzt werden kann, wenn alle beteiligten Personen insbesondere Mitarbeitende und

Dienstleister:innen ihre sicherheitsbezogenen Pflichten verstehen und aktiv einhalten. Dies schließt sowohl grundlegende Verhaltensregeln der Cyberhygiene als auch spezifische Anforderungen je nach Rolle ein (z.B. bei Administrator:innen oder Mitglieder:innen der obersten Leitungsebene). Ein zentrales Element ist die Notwendigkeit, eine explizite Verpflichtung zur Einhaltung der Informationssicherheitsvorgaben sicherzustellen. Im Sinne einer „Einverständniserklärung“ müssen alle Beteiligten z.B. durch Unterschrift, Schulungsnachweis oder Vertragsklausel bestätigen, dass sie sich der Bedeutung der Sicherheitsanforderungen bewusst sind und deren Einhaltung aktiv unterstützen. Dies gilt nicht nur bei der Einstellung neuer Mitarbeitender, sondern auch im laufenden Betrieb. Darüber hinaus unterstreichen die Anforderungen die Bedeutung einer regelmäßigen Überprüfung der Rollenzuordnung und Qualifikation, insbesondere bei sicherheitskritischen Funktionen.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt es sich, sicherheitsbezogene Anforderungen im Personalwesen durch ein strukturiertes, gleichzeitig pragmatisches Vorgehen zu operationalisieren. Ein zentraler Baustein hierfür ist die Einführung einer Verpflichtungserklärung zur Informationssicherheit, welche von allen neuen Mitarbeitenden, Mitglieder:innen der obersten Leitungsebene sowie relevanten externen Dienstleistenden und Lieferant:innen bei Onboarding oder Vertragsabschluss unterzeichnet wird. Diese kurze Erklärung dient der dokumentierten Bestätigung, dass die unternehmensinternen Sicherheitsvorgaben insbesondere jene zur Cyberhygiene, Nutzung von IT-Ressourcen und zum vertraulichen Umgang mit Informationen verstanden und eingehalten werden. Im Sinne der regulatorischen Nachweisführung kann beispielsweise im Arbeitsvertrag bzw. im Onboarding-Prozess eine Verpflichtung zur Einhaltung der Sicherheitsrichtlinien aufgenommen werden.

Darüber hinaus muss für privilegierte Nutzer:innen (z.B. Administrator:innen, personalverantwortliche Stelle, Buchhaltung) beispielsweise eine spezifische Rollenbeschreibung erstellt werden, welche Aufgaben, Befugnisse und sicherheitsrelevante Pflichten bündelt und die jeweiligen Rollen kommuniziert.

Zur Sensibilisierung der obersten Leitungsebene ist vorgesehen, dass Mitglieder:innen der Leitungsebene in regelmäßigen Abständen ein kompaktes Sicherheitsbriefing (wird im Kapitel 5.6 näher thematisiert) erhalten, welches deren strategische Verantwortung im Sinne der NIS2 beleuchtet. Inhaltlich wird dabei auf Pflichten wie Ressourcenbereitstellung, Steuerung des ISMS sowie Rechenschaftspflichten bei Sicherheitsvorfällen eingegangen (siehe Kapitel 5.1.1).

Die regelmäßige Überprüfung sicherheitsrelevanter Rollen erfolgt jährlich durch den:die ISB mithilfe der personalverantwortlichen Stelle. Veränderungen im Organisationsaufbau, personelle Wechsel oder neue Anforderungen werden dabei berücksichtigt. Die Ergebnisse werden dokumentiert und fließen sowohl in die Rollenbeschreibungen als auch in die Awareness- und Schulungsplanung (siehe Kapitel 5.6) ein. Mit dieser Vorgehensweise wird sichergestellt, dass sicherheitsrelevante Zuständigkeiten im Unternehmen nicht nur formal zugewiesen, sondern auch aktiv kommuniziert, dokumentiert und regelmäßig überprüft werden.

5.5.2 Hintergrundüberprüfung

Mapping - NIS2 Durchführungsverordnung (Punkt 10.2.): Die Einrichtungen haben im Rahmen ihrer Möglichkeiten sicherzustellen, dass für sicherheitskritische Rollen eine Hintergrundüberprüfung von Mitarbeitenden sowie gegebenenfalls von relevanten Dienstleistern erfolgt (10.2.1). Dazu sind Kriterien festzulegen, welche Tätigkeiten nur von Personen mit überprüftem Hintergrund ausgeführt werden dürfen (10.2.2 a). Diese Prüfungen müssen vor Beginn der jeweiligen Tätigkeit durchgeführt werden und unterliegen der Verhältnismäßigkeit in Bezug auf geltendes Recht, den Schutzbedarf der betroffenen Systeme sowie das jeweilige Risiko (10.2.2 b). Die entsprechenden Kriterien sind regelmäßig zu überprüfen und erforderlichenfalls zu aktualisieren (10.2.3).

Interpretation der Anforderungen: Ziel dieser Anforderung ist es, sicherzustellen, dass sicherheitskritische Tätigkeiten nicht an Personen übertragen werden, bei denen begründete Zweifel an deren Integrität, Qualifikation oder Zuverlässigkeit bestehen. Dabei ist die Pflicht zur Hintergrundüberprüfung nicht pauschal, sondern risikobasiert zu verstehen, also nur für bestimmte Rollen anzuwenden. Neben internen Mitarbeitenden können auch externe Dienstleistende einbezogen werden, insbesondere wenn sie privilegierte Zugriffe auf Systeme, Netzwerke oder vertrauliche Daten erhalten.

Umsetzung im NIS2-ISMS-Framework: Die Umsetzung erfolgt durch eine risikobasierte Einstufung sicherheitskritischer Rollen, für die eine Hintergrundüberprüfung erforderlich ist. Dazu zählen typischerweise IT-Administrator:innen, Mitarbeitende mit Zugang zu sensiblen Informationen (z.B. Personal- oder Finanzdaten) sowie externe Dienstleistende mit Systemzugriff. Diese Einstufung erfolgt auf Basis der Kritikalität der jeweils genutzten Systeme (siehe 5.3). Hierfür wurde im Rahmen der Arbeit eine Vorlage für Hintergrundüberprüfungen mit Kriterien zur einfacheren Einstufung von Rollen inklusive einer Dokumentation der als sicherheitskritisch-eingestuften Rollen erstellt. Die Überprüfung dieser Kriterien erfolgt durch den:die ISB mindestens jährlich oder anlassbezogen.

Für betroffene Rollen ist ein schlanker Prüfprozess definiert, welcher in bestehende Onboarding-Prozesse in der personalverantwortlichen Stelle (z.B. Personalabteilung) integriert wird und mindestens die Überprüfung von Qualifikationsnachweisen (z.B. Zertifikate, Ausbildung) und das Einholen von Referenzen umfasst. Weitergehende Prüfungen sind nur bei entsprechend hohem Risiko vorgesehen. Die Anwendung der Vorlage erfolgt dabei durch die personalverantwortliche Stelle und/oder ISB im Zuge von Neueinstellungen oder Vertragsabschlüssen, indem relevante Rollen geprüft, die vorgesehenen Maßnahmen dokumentiert und die Prüfung entsprechend abgezeichnet werden. Die Dokumentation dient zugleich als prüffähiger Nachweis im Rahmen interner oder externer Prüfungen.

5.5.3 Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses

Mapping - NIS2 Durchführungsverordnung (Punkt 10.3.): Einrichtungen müssen sicherstellen, dass nach Beendigung oder Änderung eines Beschäftigungsverhältnisses weiterhin gültige sicherheitsbezogene Verpflichtungen, etwa hinsichtlich Vertraulichkeit, vertraglich definiert und durchsetzbar sind (10.3.1). Diese Verpflichtungen sind in die jeweiligen Arbeitsverträge, Vereinbarungen oder sonstigen Beschäftigungsbedingungen zu integrieren (10.3.2).

Interpretation der Anforderungen: Die Anforderung zielt darauf ab, das Sicherheitsniveau einer Organisation über den aktiven Beschäftigungszeitraum hinaus abzusichern. Ehemalige Mitarbeitende, die in sicherheitskritischen Bereichen tätig waren oder Zugriff auf sensible Informationen hatten, bleiben potenzielle Risikoträger:innen, z.B. durch unbeabsichtigte Weitergabe von Informationen oder gezielte Nutzung von internem Wissen. Um dieser Gefahr zu begegnen, ist eine klare, vertraglich bindende Absicherung erforderlich, die über das Ausscheiden hinauswirkt. Ebenso gilt es, bei internen Rollenwechseln sicherzustellen, dass nicht mehr benötigte Rechte und Zugriffe vollständig entzogen werden.

Umsetzung im NIS2-ISMS-Framework: In KMUS empfiehlt sich die Umsetzung dieser Anforderung über zwei zentrale Maßnahmenbereiche: vertragliche Absicherung und technisch-organisatorisches Offboarding. Zum einen ist sicherzustellen, dass alle Mitarbeitenden mit Zugang zu vertraulichen Informationen oder sicherheitsrelevanten Systemen eine Vertraulichkeitsvereinbarung unterzeichnen, die ausdrücklich auch nach Beendigung des Arbeitsverhältnisses wirksam bleibt. Im Sinne der regulatorischen Nachweisführung wird im Arbeitsvertrag bzw. im Onboarding-Prozess eine Verpflichtung zur Einhaltung der Sicherheitsrichtlinien aufgenommen kann diese Vereinbarung als eigene Klausel im Arbeitsvertrag oder als separate Zusatzvereinbarung (z.B. im Rahmen des Onboardings) ausgestaltet sein.

Zum anderen muss das Offboarding organisatorisch klar geregelt und dokumentiert erfolgen. Hierzu zählt die Rückgabe physischer Assets (z.B. Laptops, Zugangsmedien), der Entzug aller Benutzer:innenkonten sowie die Entfernung aus Verteiler:innengruppen oder Berechtigungssystemen. Auch bei internen Funktionswechseln ist sicherzustellen, dass nicht mehr benötigte Rechte konsequent entzogen werden, um Berechtigungsakkumulation zu vermeiden. Dies erfolgt idealerweise über eine Offboarding-Checkliste, welche in Kapitel 5.4.5 bereits thematisiert wurde.

5.5.4 Disziplinarmaßnahmen

Mapping - NIS2 Durchführungsverordnung (Punkt 10.4.): Von Einrichtungen ist ein formalisierter Disziplinarprozess zu etablieren, zu kommunizieren und aufrechtzuerhalten, um Verstöße gegen Sicherheitsrichtlinien systematisch zu behandeln (10.4.1). Dabei sind rechtliche, vertragliche und geschäftsbezogene Anforderungen zu berücksichtigen. Der Prozess ist regelmäßig zu überprüfen und bei rechtlichen Änderungen oder veränderten Rahmenbedingungen anzupassen (10.4.2).

Interpretation der Anforderungen: Ein funktionierendes ISMS erfordert klare Reaktionen auf sicherheitsbezogenes Fehlverhalten. Die Einführung eines strukturierten Disziplinarprozesses stellt sicher, dass Verstöße, ob vorsätzlich oder fahrlässig, nachvollziehbar bewertet und verhältnismäßig sanktioniert werden. Damit erfüllt der Prozess nicht nur eine steuernde, sondern auch eine präventive Funktion im Sinne der Sicherheitskultur. Wichtig ist dabei, dass arbeitsrechtliche Grundsätze, Datenschutzvorgaben sowie innerbetriebliche Abläufe berücksichtigt werden. Der Fokus liegt nicht auf Bestrafung, sondern auf Sensibilisierung, Transparenz und konsistenter Behandlung von Regelverstößen.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt sich ein einfacher, aber wirksamer Disziplinarprozess, welcher typisches sicherheitsbezogenes Fehlverhalten definiert, abgestufte Reaktionsmaßnahmen beschreibt und die Zuständigkeiten klar zuweist. Typische Verstöße sind z.B. die Weitergabe von Passwörtern, Missachtung von Zugangskontrollen, Installation nicht autorisierter Software oder der unsachgemäße Umgang mit sensiblen Informationen. Die Reaktionsmaßnahmen empfiehlt sich beispielsweise ein dreistufiges Eskalationsmodell, abgestimmt auf Schweregrad und Häufigkeit des Vorfalls:

- **Stufe 1:** Informelles Gespräch / Hinweis mit dem:der Vorgesetzten (bei erstmaligem, geringfügigem Verstoß)
- **Stufe 2:** Schriftliche Ermahnung oder Abmahnung von dem:der ISB (bei wiederholtem oder mittelschwerem Verstoß)

- **Stufe 3:** Arbeitsrechtliche Maßnahmen bis hin zur Kündigung (bei schwerwiegenden oder vorsätzlichen Verstößen)

Die Zuständigkeit für die Bewertung und Einleitung von Maßnahmen liegt bei der personalverantwortlichen Stelle in Abstimmung mit der vorgesetzten Stelle und dem:der ISB. Alle Vorfälle und Maßnahmen sind zu dokumentieren z.B. im Personalakt. Datenschutzrechtliche Anforderungen (insbesondere Speicherfristen) sind dabei zu beachten. Der Prozess wird mindestens einmal jährlich durch die personalverantwortliche Stelle (eventuell in Zusammenarbeit mit dem:der ISB) überprüft und an neue gesetzliche Anforderungen oder organisatorische Veränderungen angepasst. Zudem erfolgt eine anlassbezogene Aktualisierung, z.B. bei neuen gesetzlichen Vorgaben oder sicherheitsrelevanten Vorfällen. Zur Unterstützung der Umsetzung wurde im Rahmen dieser Arbeit ein Mustertext (Disziplinarmaßnahmen bei Verstößen) für die Informationssicherheitsleitlinie (siehe 5.2) entwickelt.

5.6 Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen

Dieses Kapitel behandelt die Anforderungen im Bereich der Sicherheitskultur, konkret: Maßnahmen zur Förderung grundlegender Cyberhygiene sowie rollenbasierte Cybersicherheitsschulungen. Im Fokus stehen die Sensibilisierung aller Mitarbeitenden sowie die gezielte Fortbildung sicherheitskritischer Rollen. Ziel ist es, das Sicherheitsbewusstsein auf allen Organisationsebenen strukturiert zu fördern und kontinuierlich weiterzuentwickeln.

5.6.1 Bewusstseinsschaffung und Cyberhygiene

Mapping - NIS2 Durchführungsverordnung (Punkt 8.1.): Gemäß Punkt 8.1 sind betroffene Einrichtungen verpflichtet, dafür zu sorgen, dass ihre Mitarbeitenden einschließlich der Mitglieder:innen der Leitungsorgane sowie gegebenenfalls auch direkte Lieferant:innen und Dienstleister:innen ein angemessenes Bewusstsein für Cybersicherheitsrisiken entwickeln und grundlegende Cyberhygienepraktiken anwenden (8.1.1). Zur Umsetzung dieser Anforderung ist ein Awareness-Programm bereitzustellen, das zeitlich geplant ist, regelmäßig wiederholt wird und auch neue Mitarbeitende einbezieht (8.1.2 a). Es muss mit den bestehenden Sicherheitsrichtlinien und Prozessen abgestimmt sein (8.1.2 b) und Inhalte wie aktuelle Bedrohungen, bestehende Schutzmaßnahmen, Kontaktstellen sowie Cyberhygiene-Verhaltensweisen für Nutzer:innen vermitteln (8.1.2 c). Die Wirksamkeit des Programms ist zu evaluieren und es muss regelmäßig

aktualisiert werden, insbesondere bei veränderten Bedrohungslagen oder neuen Best Practices (8.1.3).

Interpretation der Anforderungen: Das Ziel dieser Anforderungen besteht darin, Cybersicherheit nicht allein technisch zu denken, sondern als organisationsweite Kultur zu verankern. Mitarbeitende sind oft das schwächste Glied in der Sicherheitskette z.B. durch Unachtsamkeit, Unwissen oder mangelnde Sensibilisierung. Entsprechend muss ein Grundverständnis für Cyberhygiene auf allen Ebenen geschaffen werden. Die Anforderungen gelten nicht nur für „IT-nahe“ Rollen, sondern auch für oberste Leitungsebene, Fachbereiche und abhängig vom Zugriff auf für externe Lieferant:innen. Die Verordnung fordert nicht nur eine Einmalmaßnahme, sondern ein strukturiertes, wiederkehrendes und anpassungsfähiges Programm. Der Fokus liegt dabei auf der langfristigen Verhaltensänderung und der Integration von Sicherheitsbewusstsein in den betrieblichen Alltag.

Umsetzung im NIS2-ISMS-Framework: In der Praxis bedeutet dies, dass KMUs ein strukturiertes, aber zugleich pragmatisches Cyber-Awareness-Programm etablieren sollten, das Mitarbeitende systematisch für sicherheitsrelevante Themen gemäß den themenspezifischen Richtlinien sensibilisiert. Ein solches Programm umfasst wiederkehrende Schulungen, niedrigschwellige Kommunikationsmaßnahmen und eine klare Verankerung von Sicherheitsbewusstsein im betrieblichen Alltag. Im Rahmen dieser Arbeit wurde eine Vorlage für ein Awareness-Programm erstellt. Die Vorlage muss vor Verwendung an die eigenen Bedürfnisse der KMUs angepasst werden.

Im ersten Schritt sollten Mitarbeitende in zwei **Zielgruppen** eingeteilt werden:

- Alle Mitarbeitenden (Basis-Awareness-Schulungen)
- Sicherheitsrelevante Rollen (Tiefergehende Fachschulungen; als Basis hierfür können die sicherheitskritischen Rollen verwendet werden, welche im Punkt zu 5.5.2 identifiziert wurden, z.B. IT-Administrator:innen)

Im nächsten Schritt muss ein jährlicher **Schulungsplan** mit festen Terminen festgelegt werden, beispielsweise:

- Jährliche Awareness-Basis-Schulung für alle Mitarbeitenden
- Regelmäßige Wiederholungen (z.B. quartalsweise kurze Erinnerungen, simulierte Phishing-Angriffe, etc.)
- Schulungen für neue Mitarbeitende im Onboarding-Prozess

- Rollenspezifische Fachschulungen nach Bedarf (z.B. halbjährlich oder jährlich)

Nachdem die festen Termine festgelegt wurden, müssen nun die Inhalte (auf Basis potenzieller Bedrohungen der Rollen) definiert werden, beispielsweise:

- **Basis-Awareness-Schulung (auf Basis geltender themenspezifischen Richtlinien sowie der Leitlinie):** Wie erkennt man Phishing? Was mache ich bei einem Sicherheitsvorfall? Wie erstelle ich sichere Passwörter und warum sind diese wichtig? Wer ist mein:e Ansprechpartner:in bei Sicherheitsfragen?
- **Tiefergehende Fachschulungen:** Sichere Konfiguration von IT-Systemen, Umgang mit Sicherheitsvorfällen, Aktuelle Bedrohungslage und Schwachstellen, Anforderungen aus Regulierungen, etc.

Sobald die Inhalte festgelegt sind, muss die passende Schulungsform gewählt werden, um die Themen gut kommunizieren zu können. Hierbei eignen sich bei KMUs vor allem diese Formate:

- E-Learning (z.B. über Plattformen wie KnowBe4)
- Interne Kurzschulungen (z.B. vor Ort oder remote als Präsentation durch ISB)
- Phishing-Simulationen (z.B. GoPhish, OpenSource und kostenloses Phishing-Framework)

Wie schon zuvor im Schulungsplan erwähnt, sollten neue Mitarbeitende direkt im Onboarding-Prozess sofort sensibilisiert werden. Hierfür ist es ratsam, dass beispielsweise im Zuge des Onboardings neue Mitarbeitende innerhalb des ersten Monats die verpflichtenden E-Learning-Module absolviert haben. Die Teilnahme an der Schulung muss dokumentiert werden und wird regelmäßig durch die personalverantwortliche Stelle kontrolliert. Wichtig ist ebenfalls, die Dokumentation welche Rollen, wann und welche Schulungen abgeschlossen haben. Hierfür ist ebenso die personalverantwortliche Stelle zuständig, welche den aktuellen Stand regelmäßig, zumindest jährlich überprüft und wenn nötig an Betroffene kommuniziert.

Um die Wirksamkeit des Awareness-Programms und der spezifischen Awareness-Maßnahmen zu überprüfen, empfehlen sich kleine Multiple Choice Tests, die Auswertungen der Phishing-Klickrate bei Simulationen sowie die Einholung von Feedback von Mitarbeitenden. Diese Ergebnisse sollen mindestens einmal jährlich durch den:die ISB mithilfe der personalverantwortlichen Stelle auf Verbesserungsbedarf überprüft und in das Management-Review miteinbezogen werden. Die Metriken und KPIs sind ebenso in Kapitel 5.3.2 sowie in der Vorlage für die Berichterstattung an die oberste Leitungsebene (Kapitel 5.1.1) thematisiert. Die Ergebnisse der Wirksamkeitsüberprüfungen sowie neue Bedrohungen, organisatorische Änderungen oder gesetzliche Anforderungen fließen in die zumindest jährliche Überprüfung und Anpassung des

Cyber-Awareness-Programms durch den:die ISB ein.

Zur praxisnahen und ressourcenschonenden Umsetzung des Awareness-Programms empfiehlt sich für KMUs ergänzend die Nutzung öffentlich zugänglicher, kostenfreier Schulungsressourcen für die Basis-Awareness-Schulungen, welche von europäischen und nationalen Cybersicherheitsinstitutionen bereitgestellt werden. Kostenlose und freie Ressourcen aus nationalen Quellen (Österreich und Deutschland):

- **WKO - „IT-Sicherheitshandbuch für Mitarbeiter/innen“:** Behandelt Themen, die Nutzer:innen selbst beeinflussen können: z.B. sicherer Umgang mit PC und Informationen, Passwörter, Internetnutzung, Malware, E-Mail/Spam. [43]
- **WKO - „MA-Schulung“:** Basisschulung als Präsentation zur Informationssicherheit für Mitarbeitende. Enthält praxisorientierte Inhalte zu sicherem Umgang mit Passwörtern, E-Mail und Internet, Social Engineering, mobilen Geräten sowie Entsorgung sensibler Daten. Kann als Teil des Awareness-Programms in Onboardings oder jährlichen Wiederholungsschulungen genutzt werden. [44]
- **ÖIAT (Österreichisches Institut für angewandte Telekommunikation) - Cybersecurity Awareness Playbook:** Web-Plattform mit Tools- und Methodensammlung für Awareness-Maßnahmen in Unternehmen. Bietet Schritt-für-Schritt-Anleitungen für Awareness-Kampagnen, welche auch kleine Betriebe mit geringem Aufwand umsetzen können (z.B. Anleitungen für Phishing-Simulationen, Spielerische Trainings und andere Aktivitäten). Fokus auf praxisnahe, alltagsnahe Inhalte zur Stärkung der Sicherheitskultur im Unternehmen. [45]
- **BSI - Broschüre „Cyber-Sicherheit für KMU“:** Ein kompakter Leitfaden für KMUs, welcher leicht verständlich grundlegende Cyberhygiene-Themen vermittelt: Verantwortlichkeiten für Informationssicherheit im Unternehmen, Bedeutung regelmäßiger Updates/Patches, Notwendigkeit von Antivirus und Backups etc. [46]
  - Inhalt: Basismaßnahmen zum Schutz der IT in KMUs, mit praxisnahen Erklärungen ohne Branchenspezifik.
- **BSI - „Leichter Einstieg“ Videos:** Vom BSI entwickelte Reihe kurzer Erklärvideos für KMUs, welche die wichtigsten Grundlagen der Informations- und Cybersicherheit anschaulich vermitteln. Der Inhalt umfasst unter anderem Updates einspielen, Datensicherung, sichere Passwörter (und Passwortmanager), E-Mail-Sicherheit (Erkennen von Phishing), Browsersicherheit und Benutzerkontentrennung. [47]

5.6.2 Cybersicherheitsschulungen

Mapping - NIS2 Durchführungsverordnung (Punkt 8.2.): Zusätzlich zur allgemeinen Sensibilisierung verlangt die Verordnung, dass Einrichtungen spezifische Cybersicherheitsschulungen für jene Mitarbeitenden anbieten, deren Aufgaben sicherheitsrelevantes Fachwissen erfordern (8.2.1). Dafür ist ein strukturiertes Schulungsprogramm zu entwickeln, das sich an der Sicherheitleitlinie sowie den funktionalen Anforderungen orientiert und konkrete Schulungsbedarfe für bestimmte Rollen definiert (8.2.2). Die Schulungsinhalte müssen rollenbezogen und wirksam sein sowie auf aktuelle Schutzmaßnahmen und Bedrohungslagen eingehen. Dies umfasst insbesondere: sichere Konfiguration und Betrieb von IT-Systemen, Bedrohungsbriefings und Verhalten bei sicherheitsrelevanten Vorfällen (8.2.3 a-c). Mitarbeitende, die in neue sicherheitskritische Rollen wechseln, müssen entsprechend nachgeschult werden (8.2.4). Das Schulungsprogramm ist regelmäßig zu aktualisieren, um es an neue technische, organisatorische und regulatorische Entwicklungen anzupassen (8.2.5).

Interpretation der Anforderungen: Während Punkt 8.1 die organisationsweite Sensibilisierung adressiert, fokussiert Punkt 8.2 gezielt auf jene Rollen, deren Tätigkeiten ein erhöhtes Risiko für die Informationssicherheit darstellen. Im folgenden Abschnitt wird daher die Umsetzung rollenspezifischer Cybersicherheitsschulungen im Detail erläutert. Dabei geht es nicht nur um technische IT-Positionen, sondern auch um fachlich besonders exponierte Rollen (z.B. Personalabteilung, Buchhaltung, Datenschutz, Einkauf), welche beispielsweise Zugriff auf vertrauliche Informationen oder kritische Systeme haben. Entscheidend ist, dass die Schulungen nicht pauschal, sondern funktionsspezifisch konzipiert sind und im Einklang mit der jeweiligen Verantwortlichkeit stehen. Zudem verlangt die Verordnung eine regelmäßige Wirksamkeitsprüfung und inhaltliche Aktualisierung der Schulungen unter anderem durch die Berücksichtigung aktueller Bedrohungslagen und technischer Entwicklungen.

Umsetzung im NIS2-ISMS-Framework: In der Praxis bedeutet dies, dass KMUs zusätzlich zum allgemeinen Awareness-Programm ein strukturiertes Schulungsprogramm für sicherheitsrelevante Rollen etablieren müssen, das sich an den spezifischen Aufgaben und Risiken dieser Funktionen orientiert. Dieses Programm ist gezielt auf Mitarbeitende auszurichten, deren Tätigkeiten ein erhöhtes Maß an Sicherheitskompetenz erfordern, z.B. in der Systemadministration, Netzwerkinfrastruktur oder im Management sensibler Daten und Zugriffsrechte. Sofern schon erfolgt, können hierfür als Basis die in Punkt 5.5.2 identifizierten sicherheitsrelevanten Rollen verwendet werden. Beispielhafte sicherheitsrelevante Rollen sind hierbei IT-Administrator:innen, die oberste Leitungsebene oder Rollen, welche Zugriff auf sensible Daten haben

(z.B. Buchhaltung). Ebenso sind hierbei extern Dienstleister:innen, welche Zugriffe auf sensible Daten oder kritische Systeme (siehe 5.3) haben zu beachten. Anschließend ist ein Programm für die Fachschulungen zu entwickeln, welches für jede identifizierte Rolle spezifische Inhalte, Schulungsmethoden und Frequenzen definiert, welche in der nachfolgenden Tabelle 5.1 beispielhaft dargestellt werden:

Rolle	**Schulungsinhalte**	**Frequenz**	**Format**
Oberste Leitungsebene	• Überblick Bedrohungslage • CEO-Fraud • Bedeutung ISMS und Managementpflichten gemäß NIS2 • Notfallmanagement, Kommunikationsstrategie bei Sicherheitsvorfällen	Jährlich und anlassbezogen bei wesentlichen Änderungen (z.B. NIS2)	Präsenzschulung (60-90 Minuten) durch ISB mit Präsentation

Rolle	Schulungsinhalte	Frequenz	Format
IT-Administrator:in	• Sichere Konfiguration von Servern, Clients, Netzwerkkomponenten • Patch- und Schwachstellenmanagement (inklusive CVSS-Einstufung) • Logging, Monitoring, Detection & Response • Benutzer- und Rechtemanagement (Least Privilege, MFA, etc.) • Umgang mit Zero-Day-Schwachstellen und Sicherheitsvorfällen • Überblick zu regulatorischen Anforderungen (NIS2, ISO/IEC 27001)	1-2x jährlich und anlassbezogen bei neuer Bedrohungslage oder neuen Technologien/Tools	Präsenzschulung (60-90 Minuten) durch ISB mit Präsentation • Interne Workshops zur Systemhärtung • Teilnahme an CERT-/BSI-Briefings

Rolle	Schulungsinhalte	Frequenz	Format
Mitarbeiter:in mit Zugriff auf sensible Daten/Informationen (z.B. Buchhaltung)	• Erkennung typischer Angriffsmuster (Phishing-Arten, Rechnungsbetrug, etc.) • Sensibilisierung auf Datensicherheit/Datenschutz und Vertraulichkeit • Handlungsfähigkeit im Sicherheitsvorfall	Jährlich und anlassbezogen bei Vorfällen oder Änderungen in Prozessen	Interaktive Schulung (remote) durch ISB

Tabelle 5.1: Beispielhaftes Schulungsprogramm für Fachschulungen

Ergänzend dazu ist ein Prozess für Nachschulungen bei Rollenwechsel zu implementieren. Mitarbeitende, welche in sicherheitsrelevante Funktionen wechseln, müssen innerhalb eines festgelegten Zeitraums (z.B. 30 Tage) in die relevanten Sicherheitsthemen eingearbeitet und geschult werden. Die Verantwortung für die Erfassung solcher Rollenwechsel und die Initiierung der Schulungsmaßnahmen liegt bei der personalverantwortlichen Stelle in enger Abstimmung mit dem:der ISB. Auch das Fachschulungsprogramm unterliegt einer regelmäßigen Wirksamkeitskontrolle und Aktualisierungspflicht. Diese erfolgt mindestens einmal jährlich durch den:die ISB in Zusammenarbeit mit den fachlich zuständigen Stellen. Grundlage für die Überprüfung bilden unter anderem Feedbacks der Teilnehmenden, Schulungsergebnisse, relevante Vorfälle sowie Veränderungen in der Bedrohungslage oder gesetzlichen Anforderungen. Die Ergebnisse fließen in das Management-Review ein und dienen der kontinuierlichen Verbesserung des Programms. Als offene bzw. frei zugängliche Ressource steht unter anderem das Awareness-Poster-Dokument, welches unter anderem von Europol, Bundeskriminalamt und WKO entwickelt wurde, zur Verfügung. Dieses Dokument enthält Informationen und Tipps zur Erkennung und Reaktion zu verschiedenen Bedrohungsszenarien (z.B. CEO-Fraud, Rechnungsbetrug, verschiedenen Phishing-Arten, etc.). [48] Es bildet eine gute Basis zur Gestaltung der spezifischen Schulungsinhalte.

5.7 Sicherheit von Lieferketten

Die Sicherheit von Lieferketten stellt einen zentralen Bestandteil der Informationssicherheit eines Unternehmens, insbesondere im Hinblick auf externe Dienstleistende und Lieferant:innen dar. Ziel dieses Kapitels ist es, sicherzustellen, dass alle relevanten Liefer- und Leistungsbeziehungen systematisch im Hinblick auf Sicherheitskriterien bewertet, vertraglich abgesichert und fortlaufend überwacht werden.

5.7.1 Richtlinie zur Sicherheit von Lieferketten

Mapping - NIS2 Durchführungsverordnung (Punkt 5.1.): Gemäß Punkt 5.1 der Durchführungsverordnung sind betroffene Einrichtungen verpflichtet, eine Richtlinie zur Sicherheit von Lieferketten zu entwickeln, anzuwenden und aufrechtzuerhalten, die alle Beziehungen zu direkten Lieferant:innen und Dienstleister:innen im Hinblick auf die Sicherheit von Netz- und Informationssystemen regelt (5.1.1). Ziel ist es, Risiken innerhalb der Lieferkette frühzeitig zu erkennen und durch geeignete Vorgaben zu mindern. Die Einrichtungen müssen darin ihre Rolle innerhalb der Lieferkette identifizieren und an ihre direkten Partner:innen kommunizieren. Im Rahmen dieser Richtlinie sind Auswahl- und Vertragskriterien für Lieferant:innen zu definieren (5.1.2), insbesondere in Bezug auf:

- deren Cybersicherheitspraktiken und sichere Entwicklungsmethoden (5.1.2 a),
- die Fähigkeit zur Einhaltung technischer Sicherheitsanforderungen (5.1.2 b),
- die Qualität und Resilienz der eingesetzten Produkte und Dienstleistungen (5.1.2 c),
- sowie die Möglichkeit zur Lieferant:innen-Diversifikation bzw. Vermeidung von Herstellerabhängigkeiten (5.1.2 d).

Ergänzend dazu sind die Ergebnisse koordinierter Sicherheitsrisikobewertungen innerhalb kritischer Lieferketten zu berücksichtigen (5.1.3), sofern diese vorliegen. Auf Basis der Lieferkettenrichtlinie sowie der durchgeführten Risikoanalyse (siehe Punkt 2.1 der Durchführungsverordnung) sind vertragliche Regelungen mit Lieferant:innen zu treffen, die sicherstellen, dass Cybersicherheitsanforderungen vertraglich durchgesetzt werden können (5.1.4). Dies kann über vertraglich vereinbarte Sicherheitsanforderungen oder SLAs erfolgen und muss unter anderem folgende Inhalte abdecken:

- technische Sicherheitsanforderungen und Vorgaben bei der Beschaffung von IKT-Produkten und -Services (5.1.4 a),
- Schulungs- und Kompetenzanforderungen für Mitarbeitende der Lieferant:innen (5.1.4 b),
- Hintergrundüberprüfungen für sicherheitskritisches Personal (5.1.4 c),

- Verpflichtung zur Meldung von Sicherheitsvorfällen ohne unangemessene Verzögerung (5.1.4 d),
- Prüf- und Auditierungsrechte (5.1.4 e),
- Verpflichtung zur Schwachstellenbehandlung (5.1.4 f),
- Anforderungen an Subunternehmer und deren Sicherheitsniveau (5.1.4 g),
- Regelungen zur Rückgabe und Löschung von Informationen bei Vertragsende (5.1.4 h).

Diese Kriterien sind sowohl im Rahmen von Auswahl- und Beschaffungsprozessen zu berücksichtigen (5.1.5) als auch regelmäßig zu überprüfen. Einrichtungen müssen bei Änderungen im Risikoprofil von Lieferant:innen, etwa durch Vorfälle, neue Produkte oder geänderte Sicherheitspraktiken, proaktiv bewerten, ob ihre Lieferkettenrichtlinie angepasst werden muss (5.1.6). Zur Umsetzung sind unter anderem folgende Maßnahmen erforderlich (5.1.7):

- Monitoring der Vertragseinhaltung und SLAs,
- Analyse relevanter Sicherheitsvorfälle bei Lieferanten,
- risikobasierte Ad-hoc-Überprüfungen,
- Analyse von Änderungen bei IKT-Produkten und -Dienstleistungen der Lieferant:innen.

Interpretation der Anforderungen: Die Anforderungen verpflichten Einrichtungen zur Etablierung einer formellen Richtlinie zur Sicherheit von Lieferketten, die sicherstellt, dass Risiken aus externen Beschaffungs- und Dienstleistungsbeziehungen systematisch erkannt, gesteuert und reduziert werden. Die Richtlinie muss insbesondere Vorgaben zur Auswahl, Bewertung, Vertragsgestaltung und Überwachung von Lieferant:innen und Dienstleister:innen enthalten, welche direkt die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der Assets beeinflussen können.

Von zentraler Bedeutung ist, dass die Anforderungen risikobasiert formuliert werden: Kritische Lieferanten (z.B. IT-Dienstleister:innen, Hosting-Anbieter:innen, Software-Zuliefer:innen) unterliegen strengeren Anforderungen als Lieferant:innen ohne IT-Bezug. Ferner müssen sicherheitsrelevante Mindestanforderungen vertraglich abgesichert werden, insbesondere über Service Level Agreements (SLAs) oder Verpflichtungserklärungen. Die Sicherheit der Lieferkette wird dadurch zu einem integralen Bestandteil der organisatorischen Sicherheitsstrategie.

Umsetzung im NIS2-ISMS-Framework: In der Praxis bedeutet dies, dass KMUs im ersten Schritt eine kompakte themenspezifische Richtlinie für das Thema Lieferkettensicherheit erstellen sollten, um externe

Abhängigkeiten gezielt zu steuern und potenzielle Risiken durch Drittparteien frühzeitig zu erkennen und zu minimieren. Hierfür wurde im Rahmen der Arbeit eine Richtlinien-Vorlage erstellt. Um die Richtlinie praktisch umzusetzen, werden zunächst die konkreten Kriterien zur Einstufung der Kritikalität (z.B. unkritisch/kritisch) für Lieferant:innen und Dienstleister:innen festgelegt. Diese Kriterien können beispielsweise folgendes beinhalten:

- Zugriff auf kritische Assets (siehe 5.3)
- Zugriff auf vertrauliche oder personenbezogene Daten (z.B. Zugriff auf geschäftskritische Informationen; siehe 5.4.2)
- Bedeutung der erbrachten Leistungen für den Geschäftsbetrieb (z.B. „Ist Betrieb ohne die erbrachte Dienstleistung beeinträchtigt oder sogar nicht möglich?“)
- Regulatorische Relevanz (z.B. tragen jeweiligen Dienstleistung zur Erfüllung der NIS2-Anforderungen bei)

Diese Kriterien werden im Zuge einer Checkliste für neue und bestehende Dienstleister:innen von der jeweilig verantwortlichen Stelle (z.B. IT-Abteilung mit ISB) beurteilt sowie dokumentiert und es ergibt sich inwiefern diese als unkritisch oder kritisch zu betrachten sind.

Lieferant:innen, welche gemäß der Einstufung als unkritisch gelten, unterliegen reduzierten Auswahlkriterien. Es werden lediglich grundlegende Sicherheitsmaßnahmen erwartet, da keine wesentlichen Risiken für die Informationssicherheit, den Geschäftsbetrieb oder regulatorische Pflichten bestehen. Für als kritisch eingestufte Lieferant:innen gelten erhöhte Anforderungen, da hier ein potenzieller Ausfall, eine Kompromittierung oder ein Verstoß unmittelbare Auswirkungen auf die Sicherheit, die Betriebsfähigkeit oder die rechtliche Konformität des Unternehmens hätte. Folgende Auswahlkriterien sind hier beispielsweise zu definieren und bei kritischen Lieferant:innen im Zuge des Auswahlprozesses zu überprüfen:

- Verpflichtende Sicherheitszertifizierungen (z.B. ISO/IEC 27001)
- Verpflichtende Technische Sicherheitsmaßnahmen (MFA, Patchmanagement, etc.) inklusive Nachweise zu den umgesetzten Maßnahmen
- Verpflichtende Awareness-Schulungsmaßnahmen für alle Mitarbeitenden
- Verpflichtendes etabliertes Risikomanagement für Informationssicherheitsrisiken

Im Zuge dieser Arbeit wurde eine Vorlage bzw. ein Beispieldokument einer Checkliste für die Lieferant:innenbewertung erstellt, welche unter anderem die Kritikalitätseinstufung (unkritisch/kritisch) sowie

die Auswahlkriterien je nach Kritikalität enthält. Im nächsten Schritt sollten Verträge mit bestehenden oder neuen Dienstleister:innen oder Lieferant:innen, um Sicherheitsanforderungen ergänzt werden, welche sich an den themenspezifischen Richtlinien sowie der Leitlinie orientieren. Diese können in Form eines standardisierten Vertragsergänzungsblatts oder als Bestandteil von SLAs geregelt werden. Die Inhalte umfassen insbesondere:

- **Cybersicherheitsanforderungen** für Produkte oder Services, beispielsweise:
  - Verschlüsselung von Datenübertragungen (z.B. TLS 1.3)
  - Authentifizierungsmechanismen (z.B. MFA)
  - Redundanzen bei Hosting (z.B. zweiter Standort)
  - Logging von sicherheitsrelevanten Zugriffen
- **Anforderungen an Sicherheitsupdates und Lebenszyklusmanagement:**
  - Verpflichtung zur Bereitstellung von Sicherheitspatches während des gesamten Unterstützungszeitraums
  - Klar definierte Fristen zur Behandlung von kritischen Schwachstellen (z.B. Patches innerhalb von 72 Stunden)
  - Verpflichtung zur rechtzeitigen Information bei Support-Ende („End-of-Life“)
- **Anforderungen an transparente Systeminformationen:**
  - Beschreibung der eingesetzten Hard- und Softwarekomponenten
  - Dokumentation der implementierten Sicherheitsmaßnahmen
  - Empfehlungen zur sicheren Konfiguration (z.B. Konfiguration-Baselines)
- **Anforderungen an Schulung, Qualifikation und gegebenenfalls Zertifizierung** der Mitarbeitenden beim Lieferant:innen, beispielsweise:
  - Awareness-Schulung für alle mit Zugriff
  - Schulungspflichten in Bezug auf sichere Entwicklung bei Softwareentwicklungsleistungen
- **gegebenenfalls eine verpflichtende Hintergrundüberprüfung** bei besonders kritischen Zugriffen
- **Meldepflichten bei sicherheitsrelevanten Vorfällen**, beispielsweise:
  - Sicherheitsvorfälle mit potenziell kritischer Auswirkung auf die Systeme und Daten sind innerhalb von 24 Stunden nach Kenntniserlangung zu melden
- **das Recht auf Audit oder Vorlage von Prüfberichten** (z.B. Pentests)
  - Themen, zu welchen es keine Nachweise gibt bzw. welche nicht bereitgestellt werden, gelten als „nicht konform“
- **Verpflichtung zur proaktiven Schwachstellenbehandlung**, beispielsweise:

  - Kritische Schwachstellen (CVSS < 8) sind binnen 48 Stunden zu beheben, Verzögerungen sind aktiv zu begründen
- Anforderungen an den sicheren Umgang mit Subunternehmer:innen, beispielsweise:
  - Subunternehmer:innen sind vertraglich auf das gleiche Sicherheitsniveau zu verpflichten wie der:die Hauptauftragnehmer:in
- **Regeln zur Beendigung der Zusammenarbeit** (z.B. Datenrückgabe, Nachweise zur Datenlöschung)

Zur wirksamen Umsetzung gehört auch ein Prozess zur laufenden Überprüfung der Einhaltung der definierten Sicherheitsanforderungen durch den:die ISB gemeinsam mit den jeweils verantwortlichen Stellen (z.B: IT-Abteilung, Einkauf, Vertragsmanagement). Bei kritischen Dienstleister:innen muss jährlich eine Überprüfung zur Einhaltung der Sicherheitsanforderungen durchgeführt werden. Bei nicht kritischen Dienstleistungen erfolgt diese Überprüfung stichprobenartig nur alle zwei bis drei Jahre. Alle Bewertungen und Maßnahmen werden nachvollziehbar dokumentiert und jährlich bzw. anlassbezogen überprüft. Bei Bedarf werden bei Abweichungen im Zuge einer Risikoanalyse (siehe 5.3.1) geeignete Korrekturmaßnahmen eingeleitet, wie z.B. Anpassungen der Anforderungen, technische Schutzmaßnahmen oder ein Wechsel des:der Dienstleister:in.

5.7.2 Lieferantenverzeichnis

Mapping - NIS2 Durchführungsverordnung (Punkt 5.2.): Zusätzlich zur Sicherheitsrichtlinie verlangt die Durchführungsverordnung von den betroffenen Einrichtungen, ein aktuelles Verzeichnis aller direkten Lieferant:innen und Dienstleister:innen zu führen (5.2). Dieses muss mindestens folgende Informationen enthalten:

- benannte Ansprechpartner:innen je Lieferant:in oder Dienstleister:in (5.2 a),
- sowie eine Auflistung der durch sie bereitgestellten IKT-Produkte, -Services oder -Prozesse (5.2 b).

Interpretation der Anforderungen: Gemäß Punkt 5.2 der NIS2-Durchführungsverordnung sind betroffene Einrichtungen verpflichtet, ein aktuelles und gepflegtes Verzeichnis über alle direkten Lieferanten und Dienstleister zu führen, deren Produkte, Services oder Prozesse für den Betrieb der Organisation relevant sind. Dieses Verzeichnis muss mindestens die Kontaktdaten der jeweiligen Lieferant:innen und eine Liste für die gelieferten IKT-Produkte, -Dienste oder -Prozesse enthalten. Ziel dieser Anforderung ist es, vollständige Transparenz über externe Abhängigkeiten und potenzielle Risikofaktoren innerhalb der digitalen Lieferkette zu schaffen. Das Verzeichnis bildet zudem eine wichtige Grundlage für die Risikoanalyse, Not-

fallplanung, Sicherheitsvorfallbehandlung sowie für mögliche Prüfungen durch Aufsichtsbehörden.

Umsetzung im NIS2-ISMS-Framework: Für KMUs empfiehlt es sich im ersten Schritt zu definieren, welche Lieferant:innen und Dienstleister:innen erfasst werden müssen. Typische Beispiele für relevante Einträge sind:

- IT-Dienstleister:innen für Support, Hosting, Wartung
- Anbieter:innen von Cloud-Diensten (z.B. Microsoft 365, Dropbox Business)
- Sicherheitslösungen (z.B. Firewall-Management, Antivirus)
- Software-Anbieter mit regelmäßiger Fernwartung
- Externe Betreiber von geschäftskritischen Anwendungen (z.B. Zeiterfassung, ERP)

Im nächsten Schritt sollte ein strukturiertes Verzeichnis (beispielsweise in Form einer Excel-Datei) erstellt werden, welches insbesondere folgende Informationen enthalten muss:

- Name des:der Lieferant:in/Dienstleister:in (z.B. „Muster IT GmbH“)
- Kontaktperson mit E-Mail-Adresse und gegebenenfalls Telefonnummer
- Beschreibung der Leistung (z.B. „Hosting Firmenwebsite“, „Patchmanagement Server“)
- Aufgelistete IKT-Produkte oder -Dienste, welche geliefert oder betrieben werden
- Datum der letzten Aktualisierung
- Einschätzung der Kritikalität (kritisch/unkritisch; siehe hierfür Kapitel 5.7.1)

Die Angabe von IKT-Produkten oder -Diensten soll hierbei möglichst konkret formuliert werden, beispielsweise:

- „Cloud-Backup für Endgeräte“
- „Netzwerk-Monitoring via PRTG“
- „Support Microsoft Exchange“

Diese Angaben helfen dabei, bei Sicherheitsvorfällen oder technischen Störungen schnell relevante Zusammenhänge zu erkennen. Um sicherzustellen, dass das Verzeichnis aktuell bleibt, ist ein einfacher Prozess zur jährlichen oder anlassbezogenen Pflege (z.B. neue Dienstleister:innen, Vertragsbeendigungen, etc.) zu definieren. Die Pflege übernimmt hierbei idealerweise die verantwortliche Stelle (z.B. IT-Abteilung, Einkauf oder Vertragsmanagement) gegebenenfalls mit der Hilfe des:der ISB. Das Lieferantenverzeichnis ist als relevantes sicherheitsbezogenes Dokument zu behandeln und sollte dementsprechend zentral gespeichert

werden und nur für autorisierte Personen zugänglich sein. Im Zuge dieser Arbeit wurde eine Excel-Vorlage für das Verzeichnis erstellt, welche von KMUs als grundlegende Basis angepasst und verwendet werden kann.

5.8 Zugangssteuerung

Ein wirksames Zugangsmanagement ist ein zentraler Baustein für die Sicherheit von Asset. Der kontrollierte Zugriff auf physische und digitale Assets schützt nicht nur vor unautorisierten Zugriffen, sondern ist auch Voraussetzung für die Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit sensibler Daten. Dieses Kapitel behandelt die Anforderungen an eine umfassende Zugangssteuerung gemäß der NIS2-Durchführungsverordnung und zeigt auf, wie KMUs ein konsistentes Konzept zur Steuerung, Verwaltung und Überwachung von Zugriffen entwickeln und umsetzen können. Der Fokus liegt dabei auf der Ausgestaltung von Zugriffsrichtlinien, der Verwaltung von Berechtigungen sowie der sicheren Authentifizierung einschließlich der Anforderungen an privilegierte Konten, Systemadministration und Multi-Faktor-Authentifizierung.

5.8.1 Zugangssteuerungsrichtlinie

Mapping - NIS2 Durchführungsverordnung (Punkt 11.1.): Gemäß Abschnitt 11.1 der NIS2-Durchführungsverordnung sind betroffene Einrichtungen verpflichtet, ein Konzept zur logischen und physischen Zugangssteuerung für Netz- und Informationssysteme zu erstellen, zu dokumentieren und umzusetzen (11.1.1). Diese Zugangsrichtlinien müssen sich sowohl an den geschäftlichen Erfordernissen als auch an den Sicherheitsanforderungen der Systeme orientieren. Das Konzept muss dabei alle Formen des Zugangs, insbesondere durch interne Mitarbeitende, externe Dienstleistende sowie Besucher:innen (11.1.2 a), durch Systeme und Netzkomponenten (11.1.2 b) adressieren und sicherstellen, dass Zugriffe ausschließlich auf Grundlage adäquater Authentifizierung gewährt werden (11.1.2 c). Zudem ist vorgeschrieben, dass das Konzept in regelmäßigen Abständen sowie bei wesentlichen Änderungen oder sicherheitsrelevanten Vorfällen überprüft und gegebenenfalls angepasst werden (11.1.3).

Interpretation der Anforderungen: Im Rahmen der Zugangskontrolle sind Organisationen verpflichtet, eine dokumentierte und themenspezifische Richtlinie zu etablieren und fortlaufend zu pflegen. Diese Richtlinie bildet das Fundament für alle zukünftigen Entscheidungen im Bereich der Zugriffsvergabe und hat sowohl physische als auch logische Zugriffsmöglichkeiten zu berücksichtigen. Zentrales Anliegen dieser

Vorgabe ist die Festlegung klarer, an den Geschäftsprozessen und Sicherheitsanforderungen orientierter Prinzipien zur Steuerung von Zugriffen. Dabei sind sämtliche Zugriffskategorien (z.B. von internen Mitarbeitenden über externe Dienstleistende und Lieferant:innen bis hin zu Gästen und technischen Systemen) in angemessener Weise zu berücksichtigen. Ein wesentliches Element stellt hierbei die Sicherstellung einer eindeutigen Authentifizierung vor jeder Zugriffsgewährung dar. Die Richtlinie ist nicht nur regelmäßig, sondern auch anlassbezogen zu evaluieren und bei Bedarf anzupassen. Auf diese Weise kann gewährleistet werden, dass Veränderungen in der Bedrohungslage, der IT-Systemarchitektur oder den organisatorischen Rahmenbedingungen zeitnah abgebildet werden. Die konsequente Umsetzung dieser Maßnahme schafft eine belastbare Grundlage für ein transparentes und nachvollziehbares Berechtigungsmanagement, das in den folgenden Kapiteln näher ausgeführt wird.

Umsetzung im NIS2-ISMS-Framework: Im ersten Schritt sollten KMUs eine kompakte themenspezifische Richtlinie zum Thema „Zugangssteuerung“ erstellen, welche die unternehmensweiten Regelungen zum Thema Zugriffskontrolle dokumentiert. Im Rahmen dieser Arbeit wurde die Richtlinienvorlage für die Zugriffskontrolle erstellt, welche von KMUs als Basis genutzt werden kann und an die eigenen Bedürfnisse angepasst werden muss. Auf der Grundlage der Richtlinienvorlage werden in den darauffolgenden Kapiteln die spezifisch organisatorischen und technisch beschriebenen Maßnahmen thematisiert. Damit die definierten Anforderungen schließlich eingehalten und umgesetzt werden können, müssen diese im nächsten Schritt über rollenspezifische Schulungen bzw. Awareness-Maßnahmen (siehe Kapitel 5.6) kommuniziert werden. Die Richtlinie zur Zugriffssteuerung sollte mindestens jährlich und anlassbezogen durch den:die ISB bzw. mithilfe der IT-Abteilung überprüft und gegebenenfalls angepasst werden.

5.8.2 Verwaltung der Zugriffsberechtigungen

Mapping - NIS2 Durchführungsverordnung (Punkt 11.2.): Gemäß Abschnitt 11.2 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, Zugriffsrechte auf Netz- und Informationssysteme entsprechend der definierten Zugriffsrichtlinie zu vergeben, zu ändern, zu entziehen und zu dokumentieren (11.2.1). Die Verwaltung dieser Rechte muss auf den Prinzipien des „Need-to-know“, des „Least-Privilege“ sowie der funktionalen Trennung basieren (11.2.2 a). Darüber hinaus ist sicherzustellen, dass Zugriffsrechte bei Beendigungen oder Änderungen des Beschäftigungsverhältnisses unverzüglich angepasst werden (11.2.2 b), dass alle Zugriffe autorisiert erfolgen (11.2.2 c) und dass Zugriffe von Dritten, wie Dienstleister:innen oder Besucher:innen, streng limitiert und zeitlich begrenzt sind (11.2.2 d). Ein Zugriffsregister ist verpflichtend zu führen (11.2.2 e), ebenso wie ein Logging der Berechtigungsverwaltung (11.2.2 f). Zugriffsrechte sind in

regelmäßigen Abständen sowie bei organisatorischen Änderungen zu überprüfen und bei Bedarf anzupassen (11.2.3). Die Ergebnisse dieser Prüfungen einschließlich aller Änderungen müssen dokumentiert werden.

Interpretation der Anforderungen: Ein zentrales Element in der Steuerung der Informationssicherheit gemäß NIS2-Durchführungsverordnung ist das Management von Zugriffsrechten auf Netz- und Informationssysteme. Gemäß Kapitel 11.2 sind Unternehmen verpflichtet, Zugriffsrechte systematisch zu vergeben, anzupassen, zu entziehen und zu dokumentieren. Die zugrunde liegende Zielsetzung der Anforderung ist die konsequente Anwendung der Prinzipien „Need-to-know“, „Least Privilege“ sowie „Separation of Duties“. Dies bedeutet, dass jede Person nur jene Rechte erhalten darf, die für die jeweilige Aufgabe zwingend erforderlich sind, ohne gleichzeitig kritische Funktionen zu vereinen, die zu Missbrauch führen könnten (z.B. Buchung und Freigabe). Zugleich ist sicherzustellen, dass Drittparteien, wie z.B. externe Dienstleistende, ausschließlich zeitlich befristeten und kontrollierten Zugang zu relevanten Systemen erhalten.

Umsetzung im NIS2-ISMS-Framework: Im ersten Schritt ist ein rollenbasiertes Berechtigungskonzept zu erstellen, das für jede definierte Rolle innerhalb des Unternehmens die erforderlichen Zugriffsmöglichkeiten systematisch festlegt. Dieses Konzept bildet die Grundlage für eine konsistente, prüfbare und nachvollziehbare Vergabe von Zugriffsrechten auf Systeme und Informationen.

Zur operativen Umsetzung dient eine sogenannte Rollen- und Berechtigungsmatrix („RBAC-Matrix“), in welcher für jede Rolle die zulässigen Zugriffe auf relevante Assets etwa IT-Systeme, Anwendungen, Datenbanken oder Netzwerke dokumentiert sind. [49] Zuerst werden sämtliche relevanten Rollen innerhalb des Unternehmens identifiziert und hinsichtlich ihrer typischen Tätigkeitsbereiche analysiert. Anschließend werden pro Rolle ausschließlich jene Berechtigungen zugewiesen, welche zur Erfüllung der Aufgaben zwingend erforderlich sind („Least Privilege“). Zur typischen RBAC-Matrix wurde zusätzlich noch die Genehmigungsebene hinzugefügt, womit Rechte noch zusätzlich von einer weiteren Person genehmigt werden müssen, bevor die Rechte vergeben werden.

Eine beispielhafte Rollen- und Berechtigungsmatrix ist in der folgenden Tabelle 5.2 dargestellt:

Rolle	System / Anwendung	Zugriffsrecht	Genehmigungsebene	Letztes Review
Buchhaltung	ERP-System	Lesen/Schreiben	Teamleitung Finanz	2025-04-01
IT-Administrator:in	Domain Controller	Admin	ISB	2025-04-01
Externe:r Miterabeiter:in	SharePoint-Projekt	Lesen (temporär)	Projektleitung	2025-03-10

Tabelle 5.2: Beispielhafte Rollen- und Berechtigungsmatrix

Die RBAC-Matrix bildet zugleich die Grundlage für die operative Zugriffsverwaltung entlang des Identitätslebenszyklus. Um eine konsistente und revisionssichere Handhabung sicherzustellen, wird ein strukturierter „Joiner-Mover- Leaver-Prozess“ definiert und etabliert.

Dieser Prozess umfasst im Normalfall folgende Phasen:

- **Eintritt (Joiner):** Beim Eintritt neuer Mitarbeitender erfolgt eine Zuweisung von Berechtigungen gemäß der zuvor definierten RBAC-Matrix. In einem KMU kann hierzu ein einfacher, digitaler Antrag (z.B. Service Desk Formular oder E-Mail), welcher von der personalverantwortlichen Stelle (z.B. HR-Abteilung) initiiert wird, an die zuständigen Verantwortlichen (z.B. IT-Abteilung) zur Freigabe weitergeleitet werden. Der Antrag muss vor Vergabe der Rechte noch von der definierten Genehmigungsebene genehmigt werden.
- **Abteilungswechsel (Mover):** Bei internen Wechseln ist sicherzustellen, dass sowohl neue als auch nicht mehr benötigte Berechtigungen angepasst werden. Im Normalfall ist es hierbei am pragmatischsten die alten Rechte zu löschen und gemäß der RBAC-Matrix an die neue Rolle anzupassen.
- **Austritt (Leaver):** Beim Verlassen des Unternehmens muss eine Deaktivierung des Kontos spätestens am letzten Arbeitstag erfolgen. Auch hier ist ein einfacher, aus der personalverantwortlichen Stelle initiierter Prozess ausreichend. Die Deaktivierung erfolgt typischerweise durch die IT-Abteilung, basierend auf einem per E-Mail übermittelten Ticket. (siehe Offboarding-Prozess in 5.5.3)

Ein besonderes Augenmerk ist auf dem Zugriff von externen Dienstleistenden oder Lieferant:innen zu werfen. Der Zugriff solcher auf interne Systeme ist grundsätzlich restriktiv zu behandeln. Die Zugriffe müssen

hierfür zeitlich befristet werden (z.B. durch VPN mit Ablaufdatum oder mithilfe von eingestellten Erinnerungen in Kalendern), dokumentiert (inklusive Zweck, Zeitraum, Ansprechperson und betroffener Systeme) sowie durch zusätzliche Sicherheitsmaßnahmen (z.B. MFA) zu schützen.

Um einen Überblick über die vergebenen Rechte gewährleisten zu können, muss im nächsten Schritt ein Verzeichnis manuell erstellt (z.B. Excel-Format) oder exportiert werden, welches alle vergebenen Zugriffsrechte darstellt. Ein Beispiel eines solchen Verzeichnisses ist in der folgenden Tabelle 5.3 als Auszug dargestellt:

Name	**Abteilung**	**System**	**Rolle**	**Zugriffsart**	**Freigabe-datum**	**Verantwortl-iche Geneh-miger:in**
Lisa Bauer	Buchhaltung	DATEV	Fachanwen-derin	Vollzugriff	10.01.2025	S. Huber
T. Kö-nig	Vertrieb	CRM-System	Power-User	Lesen/Schrei-ben	15.01.2025	V. Meier
IT-Support GmbH	Dienstleist-er:in (extern)	Serverkonsole	Admin (be-fristet)	Vollzugriff (48h)	12.01.2025	ISB

Tabelle 5.3: Beispielhafte Verzeichnis der Rollen

Um nun eine gute Übersicht über Änderungen (z.B. Neuanlage, Rechteänderungen, Deaktivierung) von Benutzer:innenkonten zu haben, muss die Protokollierung sichergestellt werden. Die Überwachung und Protokollierung solcher Änderungen ist insbesondere im Hinblick auf die Nachverfolgung von Sicherheitsvorfällen relevant und wird im Kapitel 5.11.2 näher thematisiert. Zuletzt muss in Bezug auf Zugriffsberechtigungen sichergestellt werden, dass die vergebenen regelmäßig (zumindest jährlich) sowie anlassbezogen durch die jeweiligen Genehmigungsebene überprüft, Rückmeldung erfasst sowie Anpassungen dokumentiert werden. Üblicherweise wird dies durch ein gemeinsames Durchgehen der RBAC-Matrix mit dem im System tatsächlich vergebenen Rechten mit der IT-Abteilung sowie der entsprechenden Genehmigungsebene realisiert. Abweichungen bei dieser Überprüfung fließen in die Risikoanalyse (siehe 5.3.1) ein und werden mit Korrekturmaßnahmen behandelt und gegebenenfalls an die oberste Leitungsebene eskaliert. Die weiterführende Betrachtung privilegierter und administrativer Zugänge erfolgt im nachfolgenden Kapitel.

5.8.3 Privilegierte und administrative Zugänge

Mapping - NIS2 Durchführungsverordnung (Punkt 11.3.): Gemäß Abschnitt 11.3 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, Konzepte für den Umgang mit privilegierten Konten und Systemadministrationskonten als Bestandteil des Zugriffskontrollkonzepts gemäß Punkt 11.1 zu definieren und umzusetzen (11.3.1). Diese Konzepte müssen insbesondere folgende Anforderungen erfüllen (11.3.2):

- Verwendung von starken Authentifizierungs- und Autorisierungsverfahren, wie z.B. Multi-Faktor-Authentifizierung und Genehmigung für privilegierte Konten (11.3.2 a),
- Trennung von Administrationskonten für spezifische Tätigkeiten wie Konfiguration, Wartung oder Installation (11.3.2 b),
- Individuelle und möglichst restriktive Vergabe von Administratorrechten (11.3.2 c),
- Nutzung von Administrationskonten ausschließlich für dedizierte Administrationssysteme (11.3.2 d).

Zudem sind die Zugriffsrechte privilegierter Konten regelmäßig zu überprüfen, an organisatorische Änderungen anzupassen und die Änderungen nachvollziehbar zu dokumentieren (11.3.3).

Interpretation der Anforderungen: Privilegierte Konten stellen ein besonders hohes Sicherheitsrisiko dar. Im Missbrauchsfall ermöglichen sie weitreichenden Zugriff auf kritische Systeme. Die Anforderung legt daher besonderen Fokus auf die strikte Kontrolle, Trennung und Überwachung solcher Konten. Für die Praxis bedeutet das, dass Administrationsrechte nicht unkontrolliert oder dauerhaft vergeben werden dürfen. Es muss klar geregelt sein, wer wann warum welche privilegierten Zugriffe erhalten darf. Die Nutzung von Sammel- oder generischen Administrator:innen-Konten ist zu vermeiden. Stattdessen ist eine personalisierte, zweckgebundene und technisch abgesicherte Verwaltung erforderlich. Gerade für KMUs ist es entscheidend, dabei praxisnahe Prozesse zu etablieren, die sowohl IT-Sicherheit als auch betriebliche Effizienz berücksichtigen (z.B. durch getrennte Admin-Konten pro Funktion, automatisierte Protokollierung und regelmäßige Berechtigungsreviews). Diese Maßnahmen erhöhen nicht nur die Transparenz, sondern erschweren auch potenzielle Angriffe von innen wie außen erheblich. Die Einhaltung dieser Anforderung ist daher nicht nur regulatorisch geboten, sondern auch ein zentraler Bestandteil jeder nachhaltigen Sicherheitsarchitektur.

Umsetzung im NIS2-ISMS-Framework: Im ersten Schritt ist festzulegen und zu dokumentieren, welche Konten im Unternehmen zunächst als „privilegiert“ gelten. In der Praxis zählen hierzu alle Konten, welche administrative Tätigkeiten an Systemen, Netzwerken oder sicherheitsrelevanten Anwendungen er-

möglichen. Beispiele sind hierfür:

- Domänen-Administrator:innen (Windows Server, Active Directory)
- Administrator:innen in ERP-, Cloud- oder Firewall-Systemen
- Superuser-Konten auf Linux-/Unix-Systemen

Eine wesentliche Maßnahme ist, dass auf die funktionale Trennung zwischen Benutzer:innen- und Administrator:innenkonten unterschieden werden muss. Administrator:innen dürfen ihre Admin-Rechte nicht für alltägliche Aufgaben wie E-Mail, Internet oder Office-Nutzung einsetzen. Für Systemadministrationen ist stattdessen ein dediziertes Administrationskonto zu verwenden, welches ausschließlich für administrative Tätigkeiten genutzt wird. Beispiel: „max.huber@kmu.at“ für den täglichen Gebrauch; „admin-huber@kmu.local“ für administrative Aufgaben auf den Servern. Diese Trennung ermöglicht es, Risiken wie Phishing, Malware oder unautorisierte Datennutzung im Kontext privilegierter Zugänge erheblich zu reduzieren. Zusätzlich unterliegen privilegierte Konten besonders hohen Anforderungen an die Authentifizierung. Gemäß NIS2 ist ein starkes, mehrstufiges Authentifizierungsverfahren (MFA) verpflichtend. Das Thema MFA wird im Kapitel 5.8.7 näher betrachtet. Neben starken Authentifizierungsmaßnahmen sind privilegierte Zugänge auf ein Mindestmaß zu beschränken. Dieser Punkt muss in der Rollen- und Berechtigungsmatrix sowie den darauffolgenden Schritten von Kapitel 5.8.2 berücksichtigt werden. Wie auch schon bei Standardkonten müssen privilegierte Konten regelmäßig sowie anlassbezogen überprüft werden. Hierfür muss es eine zentrale Liste aller privilegierten Konten geben, wobei hierfür die Liste von Kapitel 5.8.2 ergänzt werden kann. Idealerweise erfolgt die Überprüfung quartalsweise oder halbjährlich durch den:die ISB und die IT-Abteilung. Bei Inaktivität, Wechsel oder Rollenanpassung muss unverzüglich eine sofortige Sperrung oder der Entzug der Rechte sichergestellt werden.

5.8.4 Systeme und Anwendungen zur Systemadministration

Mapping - NIS2 Durchführungsverordnung (Punkt 11.4.): Abschnitt 11.4 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen dazu, den Einsatz von Systemadministrationssystemen streng zu beschränken und zu kontrollieren, im Einklang mit dem übergeordneten Zugriffskontrollkonzept gemäß Punkt 11.1 der Verordnung (11.4.1). Konkret bedeutet dies (11.4.2):

- Systemadministrationssysteme dürfen ausschließlich für administrative Zwecke verwendet werden (11.4.2 a),
- Sie müssen logisch von anderen Systemen getrennt werden, insbesondere von Anwendungssystemen (11.4.2 b),

- Der Zugang zu diesen Systemen muss durch geeignete Authentifizierungs- und Verschlüsselungsmaßnahmen abgesichert sein (11.4.2 c).

Interpretation der Anforderungen: Systemadministrationssysteme sind hochkritische Komponenten, da sie tiefgreifenden Zugriff auf IT-Infrastrukturen ermöglichen. Die Anforderung macht deutlich, dass der Schutz dieser Systeme nicht dem Zufall überlassen werden darf. Ihre Nutzung muss klar definiert, technisch abgesichert und organisatorisch geregelt sein. Ziel ist es, Missbrauchs- und Manipulationsrisiken zu minimieren, indem administrativen Systemen eine isolierte, ausschließlich zweckgebundene Rolle zugewiesen wird. Sie dürfen nicht für allgemeine Tätigkeiten genutzt werden. Eine klare Trennung von operativen und administrativen Umgebungen ist zwingend erforderlich. Technische Maßnahmen wie Netzwerksegmentierung, dedizierte Administrationsumgebungen sowie verschlüsselte Zugänge mit starker Authentifizierung müssen etabliert werden auch wenn dies zusätzliche Komplexität in der Infrastruktur bedeutet. Der Aufwand zahlt sich jedoch aus, da Angriffsflächen reduziert und unautorisierte administrative Zugriffe verhindert werden.

Umsetzung im NIS2-ISMS-Framework: Im ersten Schritt erfolgt eine Kategorisierung und Identifikation sämtlicher Systemverwaltungssysteme im Unternehmen. Typische Beispiele sind:

- Active Directory (z.B. Domain Controller)
- zentrale Verwaltungskonsolen (z.B. VMWare vCenter, Veeam, SCCM)
- Remote-Admin-Zugänge (z.B. RDP-Gateways, Jump-Hosts)
- Geräte-Managementsysteme (z.B. MDM-Server)

Diese Systeme dürfen ausschließlich für administrative Aufgaben wie Konfiguration, Wartung, Monitoring oder Benutzerverwaltung verwendet werden. Eine Nutzung zu Alltagszwecken (z.B. E-Mail, Office, Browsing) ist ausnahmslos untersagt. Zur Trennung von Verwaltungs- und anderen Systemen kann durch eine logische Segmentierung der Verwaltungsumgebung erfolgen. In einem KMU kann dies pragmatisch durch beispielsweise Netzwerksegmentierung mit eigenen VLANs für Admin-Systeme umgesetzt werden (siehe Kapitel 5.9.8). Der Zugriff auf Systemverwaltungssysteme kann durch die Nutzung von dedizierten Admin-Konten (siehe Kapitel 5.8.3) abgesichert werden.

5.8.5 Identifikation

Mapping - NIS2 Durchführungsverordnung (Punkt 11.5.): Gemäß Abschnitt 11.5 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, den gesamten Lebenszyklus von Identitäten in ihren Netz- und Informationssystemen sowie der zugehörigen Nutzer:innen systematisch zu verwalten (11.5.1). Konkret bedeutet dies (11.5.2):

- Jede Identität, egal ob System oder Benutzer:in muss eindeutig zugeordnet sein (11.5.2 a),
- Nutzer:innenidentitäten müssen klar einer natürlichen Person zuordenbar sein (11.5.2 b),
- Die Verwaltung dieser Identitäten muss überwacht und protokolliert werden (11.5.2 c-d).

Identitäten, die mehreren Personen zugeordnet sind, sind nur in begründeten Ausnahmefällen zulässig. Sie müssen genehmigt, dokumentiert und in das Risikomanagement eingebunden werden (11.5.3). Zudem sind alle Identitäten regelmäßig zu überprüfen und bei Nichtbedarf unverzüglich zu deaktivieren (11.5.4).

Interpretation der Anforderungen: Die Verwaltung digitaler Identitäten ist die Basis jeder sicheren Zugriffskontrolle. Die Anforderung verdeutlicht, dass nur eindeutig identifizierbare und kontrollierbare Identitäten ein tragfähiges Sicherheitskonzept ermöglichen. Die Anforderung geht damit über einfache Benutzer:innenverwaltung hinaus, denn sie fordert ein systematisches Identitätsmanagement über den gesamten Lebenszyklus hinweg. Jede Identität, egal ob für Personen, Dienste oder Systeme, muss nachvollziehbar, individuell zuordenbar und aktuell sein. Der Einsatz von Shared Accounts ist kritisch zu hinterfragen und nur bei absoluter Notwendigkeit unter strengen Bedingungen zuzulassen. Gerade in KMUs mit begrenzten Ressourcen ist es wichtig, schlanke und, falls möglich, automatisierte Prozesse zur Identitätsvergabe, -pflege und -löschung zu etablieren. Denn veraltete oder ungenutzte Identitäten sind ein häufig unterschätztes Risiko.

Umsetzung im NIS2-ISMS-Framework: Obwohl die NIS2 kein explizites Verzeichnis aller Identitäten fordert, empfiehlt es sich eines zu erstellen, um die Anforderungen an das Management der Identitäten einhalten zu können. Inhalt des Verzeichnisses, sollen alle Benutzeridentitäten im Unternehmen sein. Inhalt des Verzeichnisses sollten mindestens der Benutzername, der vollständige Name, die Rolle gemäß der im Kapitel 5.8.2 definierten RBAC-Matrix, die Art der Identität und das Datum der Kontoerstellung sein. Ein Beispiel eines solchen Verzeichnisses ist in der untenstehenden Tabelle 5.4 ersichtlich.

Name	Benutzer-name	Art der Identität	RBAC-Rolle	Abteilung	Erstellt am	Datum der letzten Überprü-fung
Lisa Bauer	lisa.bauer@-unternehmen-.at	Mitarbeitende	Buchhaltung	Buchhaltung	20.09.2024	01.03.2025
Admin Bauer	admin-bauer@doma-in.local	Admin-Konto	IT-Administra-tor:in	IT-Abteilung	12.04.2025	

Tabelle 5.4: Beispielhaftes Verzeichnis der Konten

Jede Identität ist eindeutig und einer natürlichen Person zugeordnet. Sogenannte „shared accounts“ (z.B. „admin“, „support“) sind nur in absoluten Ausnahmefällen erlaubt und bedürfen einer dokumentierten Begründung, Freigabe durch den:die ISB sowie spezieller Schutzmaßnahmen (z.B. zusätzliche Logging-Mechanismen).

Im Rahmen des Identitätslebenszyklus gelten folgende Prinzipien:

- Anlage: Nur durch genehmigtes Antragsverfahren (z.B. HR-initiierter IT-Antrag).
- Änderung: Bei Wechsel der Rolle/Funktion Überprüfung der Rechte.
- Deaktivierung: Bei Austritt unverzüglich durch die IT-Abteilung.

Änderungen an Identitäten (Neuanlage, Anpassung, Deaktivierung) sind systemseitig zu durch z.B. Windows AD-Logs zu erfassen und regelmäßig durch die IT-Abteilung zu kontrollieren. Zudem muss das erstelle Verzeichnis aller Identitäten jährlich durch die IT-Abteilung überprüft werden, um zu überprüfen, ob es beispielsweise noch aktive Konten für ehemalige Mitarbeitende gibt oder ob shared Accounts noch legitime Gründe zur Verwendung haben.

5.8.6 Authentifikation

Mapping - NIS2 Durchführungsverordnung (Punkt 11.6.): Abschnitt 11.6 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur Einführung sicherer Authentifizierungsverfahren und -technologien, die sich an den im Zugriffskontrollkonzept definierten Anforderungen orientieren (11.6.1). Konkret müssen

folgende Maßnahmen umgesetzt werden (11.6.2):

- Die Stärke der Authentifizierung ist abhängig vom Schutzbedarf des jeweiligen Assets zu definieren (11.6.2 a),
- Die Vergabe und Verwaltung von Authentifizierungsdaten erfolgt kontrolliert und unter Wahrung der Vertraulichkeit (11.6.2 b),
- Zugangsdaten müssen bei der Erstvergabe, in regelmäßigen Abständen sowie bei Verdacht auf Kompromittierung geändert werden (11.6.2 c),
- Bei Fehlversuchen und Inaktivität sind Benutzer:innen zu sperren bzw. Sitzungen automatisch zu beenden (11.6.2 d-e),
- Für privilegierte Zugänge sind separate Zugangsdaten zu verwenden (11.6.2 f).

Darüber hinaus sollen moderne Authentifizierungsmethoden eingesetzt werden, orientiert an den ermittelten Risiken und dem Schutzbedarf (11.6.3). Die eingesetzten Verfahren sind regelmäßig zu überprüfen und gegebenenfalls zu aktualisieren (11.6.4).

Interpretation der Anforderungen: Sichere Authentifizierung ist ein zentraler Schutzmechanismus gegen unautorisierten Zugriff. Die Anforderung macht deutlich, dass Authentifizierungsprozesse nicht pauschal, sondern risikobasiert gestaltet sein müssen. In der Praxis bedeutet dies: Je sensibler die Assets gemäß Schutzbedarf (siehe 5.3), desto stärker müssen die Authentifizierungsmaßnahmen ausfallen (z.B. durch Komplexitätsanforderungen an Passwörter, zeitbasierte Abläufe oder den Einsatz von MFA (siehe nächstes 5.8.7)). Zudem ist sicherzustellen, dass alle Prozesse zur Vergabe, Änderung und Deaktivierung von Zugangsdaten klar definiert und technisch abgesichert sind.

Umsetzung im NIS2-ISMS-Framework: Da der Schutzbedarf durch die BIA bereits identifiziert wurde, kann auf eine separate Klassifizierung der zu schützenden Assets verzichtet werden. Die Stärke der Authentifizierung wird direkt an die Schutzbedarfsstufe gemäß BIA gekoppelt.

Für Systeme mit geringem Schutzbedarf ist die Verwendung eines starken Passworts ausreichend, wobei technische Mindestanforderungen wie Passwortlänge und Komplexität eingehalten werden müssen. Systeme mit mittlerem Schutzbedarf sollten grundsätzlich ebenfalls durch starke Passwörter geschützt werden; bei erhöhten Risiken, insbesondere bei externem Zugriff, ist optional eine zusätzliche Mehr-Faktor-Authentifizierung (MFA) einzusetzen. Systeme mit hohem Schutzbedarf, insbesondere kritische IT-Infras-

trukturen oder sensible personenbezogene Daten, sind verpflichtend durch starke Passwörter in Kombination mit einer Mehr-Faktor-Authentifizierung abzusichern. [50]

Im Rahmen des Passwortmanagements ist sicherzustellen, dass Initialpasswörter bei der ersten Anmeldung zwingend geändert werden. Darüber hinaus sollen Passwörter in definierten Intervallen, beispielsweise alle 180 Tage, geändert werden. Um eine Brute-Force-Angriffe zu verhindern, wird die Anzahl der zulässigen Fehlversuche beim Login beschränkt, etwa auf fünf Fehlversuche, bevor eine automatische Kontosperrung erfolgt. Sitzungen ohne Aktivität sollen nach einer definierten Zeit, beispielsweise 15 Minuten, automatisch beendet werden. Authentifizierungsinformationen wie Passwörter oder PINs dürfen grundsätzlich nicht im Klartext gespeichert oder über unverschlüsselte Kanäle übertragen werden. Falls eine Speicherung erforderlich ist, muss diese verschlüsselt erfolgen, etwa durch die Verwendung von Hashingverfahren. Für privilegierte Konten gelten verschärfte Anforderungen: Es sind separate Zugangsdaten zu verwenden, die nicht mit dem Standardbenutzerkonto kombiniert werden dürfen. Der Zugriff auf solche Konten erfolgt verpflichtend über eine Mehr-Faktor-Authentifizierung und ausschließlich über sichere, verschlüsselte Kommunikationskanäle.

Ein weiterer Aspekt ist die Sensibilisierung der Mitarbeitenden für den sicheren Umgang mit Authentifizierungsdaten. Hierzu zählen insbesondere Schulungen oder regelmäßige Hinweise zum sicheren Erstellen und Verwalten von Passwörtern sowie die Empfehlung zur Nutzung von Passwortmanagern (siehe 5.6.1 in der Basis-Cyber-Awareness-Schulung).

Abschließend ist sicherzustellen, dass Authentifizierungsverfahren und -technologien mindestens einmal jährlich überprüft werden. Dabei ist von der IT-Abteilung zu bewerten, ob neue technologische Entwicklungen (wie passwortlose Authentifizierungsverfahren) oder veränderte Bedrohungslagen eine Anpassung der bisherigen Mechanismen erforderlich machen.

5.8.7 Multi-Faktor-Authentifikation

Mapping - NIS2 Durchführungsverordnung (Punkt 11.6.): Gemäß Abschnitt 11.7 der NIS2-Durchführungsverordnung sind Einrichtungen verpflichtet, für den Zugriff auf Netz- und Informationssysteme, sofern dem Schutzbedarf entsprechend, MFA oder kontinuierliche Authentifizierungsmechanismen einzusetzen (11.7.1). Dabei ist sicherzustellen, dass die Stärke der Authentifizierung dem Schutzbedarf (Klassifikation) des jeweiligen Assets angemessen ist (11.7.2). Die Anwendung von MFA ist somit risikobasiert zu

beurteilen und bei besonders schützenswerten Systemen verpflichtend umzusetzen.

Interpretation der Anforderungen: Multi-Faktor-Authentifizierung ist kein optionales Komfortmerkmal, sondern ein elementarer Sicherheitsstandard für schützenswerte Systeme. Die Anforderung unterstreicht, dass besonders bei sensiblen oder kritischen Assets ein einfacher Username-Passwort-Schutz nicht mehr ausreicht. Die Entscheidung für oder gegen den Einsatz von MFA muss schutzbedarfsorientiert (siehe 5.3) erfolgen. Das bedeutet: Je höher die Kritikalität eines Systems oder einer Information, desto zwingender ist der Einsatz von mindestens zwei voneinander unabhängigen Authentifizierungsfaktoren (z.B. Passwort und Token, Biometrie, etc.). Für KMUs ist die Umsetzung zunehmend praktikabel, da viele moderne Lösungen niedrigschwellige MFA-Mechanismen anbieten, die sich ohne hohen administrativen Aufwand integrieren lassen.

Umsetzung im NIS2-ISMS-Framework: Da die Schutzbedarfsstufen im Unternehmen bereits durch eine BIA ermittelt wurden, erfolgt die Entscheidung über den verpflichtenden Einsatz von MFA auf Basis dieser Einordnung. Wie bereits im Kapitel 5.8.6 beschrieben, ist MFA bei Systemen mit hohem Schutzbedarf zwingend einzusetzen. Dies betrifft insbesondere kritische IT-Infrastrukturen, sensible personenbezogene Daten sowie privilegierte Konten. Zusätzlich zur verpflichtenden MFA bei hochschutzbedürftigen Systemen empfiehlt es sich, auch bei Systemen mit mittlerem Schutzbedarf, bei denen ein erhöhtes Risiko besteht, etwa bei Zugriffen aus dem Internet, bei Cloud-Diensten oder bei Fernzugriffen über VPN, MFA einzuführen.

5.9 Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung

Die Sicherheit von Assets muss über ihren gesamten Lebenszyklus hinweg gewährleistet sein. Dieses Kapitel stellt dar, wie KMUs sicherstellen können, dass Informationssicherheit integraler Bestandteil ihrer technischen und organisatorischen Prozesse ist. Im Fokus stehen dabei unter anderem die sichere Beschaffung von IKT-Produkten und -Dienstleistungen, das Secure Development Life Cycle (SDLC), Konfigurations- und Änderungsmanagement, Schwachstellen- und Patchmanagement, Sicherheitstests sowie Netzwerksicherheit und -segmentierung. Ziel ist es, ein belastbares Sicherheitsniveau im laufenden Betrieb zu etablieren und gleichzeitig die Reaktionsfähigkeit gegenüber neuen Bedrohungen zu erhöhen.

5.9.1 Konfigurationsmanagement

Mapping - NIS2 Durchführungsverordnung (Punkt 6.3.): Abschnitt 6.3 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur Einführung eines strukturierten Konfigurationsmanagements, das sowohl die Initialkonfiguration als auch die kontinuierliche Pflege sicherer Systemkonfigurationen umfasst (6.3.1). Konkret müssen Einrichtungen:

- Sichere Konfigurationen für Hardware, Software, Netzwerke und Dienste festlegen und umsetzen (6.3.2 a),
- Prozesse und Werkzeuge einführen, mit denen diese Konfigurationen sowohl bei neuen als auch bei bestehenden Systemen wirksam durchgesetzt und überprüft werden können (6.3.2 b).

Darüber hinaus ist vorgeschrieben, dass alle Konfigurationen regelmäßig sowie anlassbezogen überprüft und bei Bedarf aktualisiert werden müssen, insbesondere nach sicherheitsrelevanten Vorfällen oder signifikanten Änderungen der Betriebsumgebung (6.3.3).

Interpretation der Anforderungen: Sichere IT beginnt bei der Konfiguration. Die Anforderung betont, dass Standardkonfigurationen selten sicher und in vielen Fällen sogar risikobehaftet sind. Ein wirksames Konfigurationsmanagement bedeutet daher, bewusst abweichend von Werkseinstellungen sichere Vorgaben zu definieren und technisch durchzusetzen. Für KMUs heißt es, dass es nicht mehr ausreicht, einmalig Systeme sicher einzurichten. Vielmehr müssen alle Konfigurationen dokumentiert, überwacht und bei Bedarf angepasst werden, etwa durch das Patching (siehe Kapitel 5.9.5), neuen Versionen oder Systemänderungen. Ohne ein solches Vorgehen drohen Inkonsistenzen, Shadow-IT (nähere Informationen siehe Kapitel 5.4.1) und „unnötige“ Angriffsflächen. Besonders wichtig ist auch, dass sichere Konfigurationen regelmäßig, falls möglich automatisiert, überprüft und durch technische Maßnahmen wie Skripte, Policies oder Tools kontinuierlich durchgesetzt werden. So lässt sich gewährleisten, dass sicherheitsrelevante Einstellungen auch im laufenden Betrieb nicht unbeabsichtigt verloren gehen. Konfigurationsmanagement ist zusammenfassend, wie auch viele andere Sicherheitsbereiche, kein einmaliges Projekt, sondern ein fortlaufender, kontrollierter Prozess zur technischen Absicherung der Systemlandschaft.

Umsetzung im NIS2-ISMS-Framework: Als Grundvoraussetzung ist es empfehlenswert im ersten Schritt ein vollständiges Asset-Inventar etabliert zu haben, welches sämtliche relevante Assets samt zugeordneter Asset-Klassen abbildet (siehe Kapitel 5.4.1). Ergänzend dazu ist die Kritikalität der einzelnen Assets auf Basis einer BIA zu bewerten (Kapitel 5.3.1).

Ist diese Grundvoraussetzung abgeschlossen, müssen im nächsten Schritt für jede definierte Asset-Klasse Konfigurations-Baselines mit klaren Soll-Werten zur Konfigruation erstellt und dokumentiert werden. Als Basis hierfür können beispielsweise die Härtungs-Leitlfäden der Hersteller:innen selbst (z.B. Security Baslines von Microsoft) herangezogen werden, welche gute Grundlagen zur sicheren Konfiguration enthalten. Das Center for Internet Security (CIS) stellt auch sogenannte „CIS Benchmarks“ öffentlich zur Verfügung, die im Wesentlichen eine Dokumentensammlung von Best Practices zur sicheren Konfiguration unter anderem für verschiedene Systeme, Software und Netzwerke beinhalten, welche sich an den international anerkannten „CIS Controls“ orientieren. [51] Beispielhafte definierte Konfigurations-Baselines könnten folgende Soll-Werte beinhalten:

- **Windows-Clients:** Aktivierung von Windows Defender, Entfernung lokaler Admin-Rechte, Deaktivierung von SMBv1, etc.
- **Netzwerk-Router:** Änderung des Standard-Admin-Passworts, Deaktivierung des Remote-Zugriffs, Aktualisierung der Firmware auf den aktuellsten Stand, etc.
- **Webanwendungen:** Erzwingen von HTTPs, Begrenzung der Login-Versuche, Aktivierung von Logging, etc.

Sobald die Baselines konfiguriert sind, sind diese im weiteren Schritt auf den Assets umzusetzen. Bei der Umsetzung empfiehlt es sich die Konfiguration risikobasiert anzugehen und zuerst die bestehenden kritischen Assets zu priorisieren. Ebenso sollten alle neuen Assets von Anfang an gemäß der standardisierten und sicheren Konfiguration eingerichtet werden. Die Umsetzung selbst sollte, sofern es auch in der Organisation möglich ist, automatisiert umgesetzt werden, um den Aufwand gering zu halten und Konfigurationsfehler zu vermeiden. Die Soll-Vorgaben (z.B. Passwortrichtlinien, Automatische Updates, Sperrung von Wechseldatenträgern) können beispielsweise bei Windows-Systemen mittels Gruppenrichtlinien (GPOs) zentral bei einem Windows-Server eingestellt werden. Ebenso können für häufig verwendete Geräte-Typen (z.B. Windows-Clients) vordefinierte Images mit bereits installierter nötiger Software, festgelegter Struktur der Benutzer:innen und Rechten und sonstigen nötigen Vorgaben erstellt und verwendet werden. Dies ist beispielsweise bei Windows-Systemen mittels der Klonsoftware „Clonezilla“ [52] und bei Linux-Servern mittels „Kickstart“ [53] möglich. Neben spezifischen Tools, können auch Installations- und Konfigurationsskripte verwendet werden und viel Zeit sparen. Sofern bei einzelnen oder kleineren Systemen keine Automatisierung möglich ist, sollten diese manuell per Checkliste, welche sich aus den Baselines ableitet, zur Ersteinrichtung konfiguriert werden. Ist die Konfiguration eines Systems abgeschlossen, sollte anhand noch eine kurze Funktionsprüfung durchgeführt werden und die abgeschlossene Konfiguration dokumen-

tiert werden. Empfehlenswert hierfür ist es ein zentrales Konfigurationsregisters zu erstellen, welches die Konfigurationen zentral dokumentiert. Im Zuge dieser Arbeit wurde die Excel-Vorlage für Konfigurationsregister erstellt, welche von KMUs als Basis verwendet werden kann. Um Abweichungen frühzeitig zu erkennen, müssen die Systeme regelmäßig anhand der definierten Baselines stichprobenartig durch die jeweilige Stelle, welche für die Assets verantwortlich sind (z.B. IT-Abteilung) unter der Kontrolle des:der ISB. Die Frequenz dieser Prüfung richtet sich hierbei je nach Kritikalität des Assets und muss gemäß der dokumentierten Definition durchgeführt werden (siehe Kapitel 5.9.4). Ergebnisse der Überprüfung werden in einer zentralen Übersicht dokumentiert. Der:die ISB überprüft diese dann hinsichtlich Wirksamkeit und Einhaltung und integriert Abweichungen gegebenenfalls in die Risikoanalyse. Sollten sich bei Systemen die bestehende Konfiguration ändern, müssen diese im Zuge des Änderungsmanagement-Prozesses (siehe Kapitel 5.9.2) berücksichtigt sowie dokumentiert werden. Hierfür muss für jede Konfigurationsänderung unter anderem angegeben werden was geändert wurde, von wem es durchgeführt wurde, warum es geändert werden musste und wann die Durchführung der Änderung geschehen ist. Sollt es sich um eine Notfall-Änderungen aufgrund einer kritischen Konfigurationsänderung handeln, muss dies im Nachhinein dokumentiert werden. Nähere Informationen zum Änderungsmanagement sowie zum Prozess sind im nächsten Kapitel 5.9.2 thematisiert. Damit sichergestellt wird, dass die Konfigurations-Baselines den aktuellen Standards entsprechen und auch für neue Technologien und Bedrohungen passend sind, müssen diese mindestens jährlich sowie anlassbezogen (z.B. bei Sicherheitsvorfällen oder Änderungen in der Infrastruktur) von den verantwortlichen Stellen der jeweiligen Assets überprüft und gegebenenfalls angepasst werden.

5.9.2 Änderungsmanagement und Wartung

Mapping - NIS2 Durchführungsverordnung (Punkt 6.4.): Abschnitt 6.4 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur Einführung und Anwendung von Änderungsmanagement-Verfahren, um Änderungen an Netz- und Informationssystemen kontrolliert und risikoorientiert durchzuführen (6.4.1). Diese Verfahren müssen konsistent zu allgemeinen unternehmensweiten Änderungsmanagement-Regelungen sein. Sie gelten insbesondere für (6.4.2):

- Releases, Modifikationen, Notfalländerungen an Hard- und Software sowie
- Konfigurationsänderungen, die auf Basis einer Risikobewertung getestet und dokumentiert werden müssen.

In Ausnahmefällen, in denen reguläre Prozesse nicht eingehalten werden können, ist eine nachträgliche Dokumentation inklusive Begründung verpflichtend (6.4.3). Zudem müssen die Verfahren regelmäßig über-

prüft und bei Bedarf angepasst werden. (6.4.4).

Interpretation der Anforderungen: Systemänderungen gehören zum Alltag in jeder IT-Umgebung, doch genau diese Eingriffe bergen erhöhte Risiken für Stabilität und Sicherheit. Abschnitt 6.4 definiert klar, dass Änderungen kontrolliert, geplant und dokumentiert erfolgen müssen, unabhängig davon, ob es sich um Updates, Erweiterungen oder Notfallmaßnahmen handelt. Für KMUs bedeutet das, strukturierte und risikoorientierte Prozesse für jegliche Änderungen zu etablieren, nicht nur in der Theorie, sondern in der praktischen Umsetzung. Dies umfasst auch klare Verantwortlichkeiten, Genehmigungswege und Testverfahren vor Produktivsetzung. Sicherheitsrelevante Änderungen (sofern sie keine Notfall-Änderungen sind) dürfen nicht ad hoc erfolgen, sondern müssen nachvollziehbar dokumentiert und technisch bewertet werden. Selbst bei kurzfristigen Eingriffen (z.B. zur Fehlerbehebung) ist eine lückenlose Nachdokumentation verpflichtend. So wird sichergestellt, dass Transparenz gewahrt bleibt und spätere Sicherheitsanalysen oder Rückverfolgungen möglich sind.

Umsetzung im NIS2-ISMS-Framework: Um Änderungen an Systemen (z.B. Konfigurationsänderungen wie im vorherigen Kapitel thematisiert) klar zu steuern ist ein Änderungsmanagement-Prozess zu definieren und dokumentieren. Das generelle Änderungsmanagement kann mithilfe vorhandener Ressourcen (z.B. Office-Produkte und E-Mail) oder auch Ticket-Systemen erfolgen. Zur Definition des Prozesses müssen im ersten die Verantwortlichkeiten klar geregelt werden, welche Rollen Änderungen an Assets durchführen dürfen und wer für die Überwachung und Dokumentation dieser Änderungen zuständig ist. Bestenfalls sollten bereits im Themenbereich Asset-Inventar (siehe Kapitel 5.4.1) jedem Asset Asset-Verantwortliche zugewiesen worden sein. Diese Verantwortlichen sind in der Regel auch jene für die Änderungs-Berechtigung. Der:die ISB koordiniert hier die Gesamtübersicht und prüft, ob Änderungen sicherheitsrelevant sind.

Da es sich nicht bei jeder Änderung um denselben Prozess handelt sollten im nächsten Schritt zwischen beispielsweise drei definierten Änderungskategorien unterschieden werden:

- **Standardänderung:** Wiederkehrende, geringfügige Änderungen (z.B. monatliche Windows-Sicherheitspatches) mit geringem Risiko und Auswirkung auf andere Systeme
- **Normale Änderungen:** Beispielsweise geplante Änderungen an System- oder Netzwerkeinstellungen (z.B. Öffnen von Ports auf Firewall), welche die Sicherheit oder Verfügbarkeit beeinflussen können und daher dokumentiert und freigegeben werden müssen (z.B. durch ISB oder IT-Leitung)
- **Notfalländerungen:** Kurzfristige, nicht vorhersehbare Änderungen zur Behebung von akuten Proble-

men oder Sicherheitsvorfällen (z.B. schnelles Einspielen von Zero-Day-Patches), welche unmittelbar umgesetzt werden müssen, mit nachträglicher Dokumentationspflicht

Änderungen, welche aus der Umsetzung von Patches (siehe Kapitel 5.9.5) oder Schwachstellenbehandlungen (siehe Kapitel 5.9.3) resultieren, sind ebenfalls über diesen Änderungsmanagementprozess zu steuern, zu dokumentieren und freizugeben.

Eine Beantragung einer Änderung (z.B. durch Abteilungsleitung oder externe Dienstleistende) sollte mithilfe Ausfüllens eines kurzen Formulars geschehen, welche zumindest folgende Informationen beinhalten sollte:

- Was soll geändert werden?
- Warum ist die Änderung wichtig? (z.B. neuer Prozess oder Softwareanforderung)
- Dringlichkeit der Änderung bzw. Terminwunsch
- Betroffene Assets/Systeme (sofern bekannt)

Das Formular wird im weiteren Schritt an die IT-Abteilung geschickt (z.B. mittels E-Mail, Online-Formular, Ticket-System, etc.), welche es dann an die jeweilig zuständige Rolle (z.B. Asset-Verantwortliche) zuordnen. Jeder Änderungsantrag, unabhängig davon, ob dieser per E-Mail, Online-Formular oder über ein Ticketsystem gestellt wird, sollte eine eindeutige Antrags-ID erhalten (z.B. Antrag-2025-004). Diese ID dient der sauberen Verknüpfung zwischen dem Antrag und der Umsetzung im Änderungsregister und wird dort dokumentiert.

Die Rolle, welche die Änderung zugewiesen bekommen hat, muss dann grundlegend prüfen, ob die Änderung technisch möglich ist und gegebenenfalls den:die ISB hinzuziehen, sofern es sich um eine sicherheitsrelevante Änderung handelt (z.B. bei Konfigurationsänderungen). Um dies zu evaluieren, muss mithilfe einer kleinen Risikoabschätzung evaluieren, ob die Änderung andere Systeme beeinträchtigen könnte und ob sich ein Sicherheitsrisiko ergeben könnte, beispielsweise anhand einer kurzen Checkliste, mit folgenden beispielhaften Fragen:

- Könnte die Änderung die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität gefährden?
- Besteht die Gefahr, dass andere Systeme betroffen werden?
- Gibt es eine Rückfallebene (z.B. Backup, Snapshot, etc.)?

Sofern mindestens eine Frage mit „Ja“ beantwortet wird, muss die Risikoeinschätzung kurz dokumentiert werden (z.B. „Öffnung von Port 80 für internen Webservice; niedriges Risiko, da intern und abgesichert mit VLAN“). Sollte sich ein mittleres/hohes Risiko herausstellen, muss hierzu vor der Umsetzung der:die ISB konsultiert werden. Schlussendlich wird die Änderung in eine der definierten Änderungskategorien zugeordnet und je nach Kategorie behandelt und muss gegebenenfalls freigegeben werden. Änderungen sollten Änderungen vor Produktivsetzung auf die Funktionsfähigkeit und Nebeneffekte getestet werden. Sollte dies beispielsweise nicht durch ein dezidierte Testsystem möglich sein, muss der Test mit Alternativmaßnahmen (z.B. Durchführung außerhalb der Geschäftszeiten und direkte Überwachung nach Umsetzung) sichergestellt werden. Wichtig hierbei ist durch die Dokumentation sicherzustellen ob und wie getestet wurde.

Damit alle Änderungen standardisiert dokumentiert werden, empfiehlt es sich ein zentral abgelegtes Änderungsregister (z.B. in Excel-Format) zu erstellen, auf welches alle relevanten Stellen Zugriff haben. Im Zuge dieser Arbeit wurde eine Excel-Vorlage für ein Änderungsregister erstellt, welche von KMUs als Basis verwendet werden kann. Änderungen, welche aus der Behebung von Schwachstellen (siehe Kapitel 5.9.3) oder aus der Umsetzung von Patches (siehe Kapitel 5.9.5) resultieren, müssen im Änderungsregister klar mit der jeweiligen Schwachstellen-ID oder der Patch-ID referenziert werden. Dies ermöglicht eine vollständige Rückverfolgbarkeit der sicherheitsrelevanten Änderungen. Im Prozess müssen Notfalländerung, da sie aufgrund der Dringlichkeit direkt umgesetzt werden, im Nachhinein sorgfältig dokumentiert werden. Außerdem muss die Dokumentation nachträglich seitens des:der ISB oder IT-Leitung formell freigegeben werden.

Um sicherzustellen, dass der Änderungsmanagement-Prozess angemessen für das Unternehmen ist und vollständig angewendet wird, muss dieser mindestens jährlich und anlassbezogen durch den:die ISB oder die IT-Leitung überprüft und gegebenenfalls angepasst werden. Die Ergebnisse der Prüfung müssen schriftlich festgehalten werden.

5.9.3 Umgang mit Schwachstellen und deren Offenlegung

Mapping - NIS2 Durchführungsverordnung (Punkt 6.10.): Abschnitt 6.10 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen dazu, Informationen über technische Schwachstellen ihrer Netz- und Informationssysteme aktiv zu beschaffen, deren Relevanz zu bewerten und geeignete Gegenmaßnahmen zu ergreifen (6.10.1). Konkret umfasst das (6.10.2):

- Überwachung relevanter Quellen (z.B. CSIRTs, Hersteller, Behörden) zur Identifikation neuer Schwachstellen (6.10.2 a),

- Durchführung von regelmäßigen Schwachstellenscans und dokumentierte Ergebnissicherung (6.10.2 b),
- Unverzügliche Behandlung kritischer Schwachstellen (6.10.2 c),
- Integration der Schwachstellenbehandlung in bestehende Prozesse wie Änderungs-, Patch-, Risiko- und Sicherheitsvorfalls-Management (6.10.2 d),
- Definition eines Prozesses zur verantwortungsvollen Offenlegung gemäß nationaler Richtlinien (6.10.2 e).

Bei erheblichen Risiken ist ein konkreter Maßnahmenplan zur Beseitigung der Schwachstelle zu erstellen (6.10.3). Falls keine Beseitigung erfolgt, muss dies dokumentiert und begründet werden. Zudem sind die genutzten Überwachungs-Kanäle regelmäßig zu überprüfen und bei Bedarf anzupassen (6.10.4).

Interpretation der Anforderungen: Ein wirksames Schwachstellenmanagement beginnt nicht mit der Behebung, sondern mit der frühzeitigen Erkennung potenzieller Angriffsvektoren, und genau hier setzt Abschnitt 6.10 der NIS2-Durchführungsverordnung an. Die Pflicht zur aktiven Beschaffung und Auswertung von Informationen zu technischen Schwachstellen geht über rein operative Maßnahmen hinaus und etabliert den Anspruch, Vulnerability Management als strategische Komponente der Cyberabwehr zu begreifen. Neben technischen Maßnahmen wie automatisierten Schwachstellenscans (siehe 5.9.4) ist hierbei auch der Aufbau eines strukturierten Threat-Intelligence-Prozesses zentrales Element. Organisationen sind gefordert, Informationen aus vertrauenswürdigen Quellen wie CSIRTs, Herstellerwarnungen oder Behördenmitteilungen gezielt zu überwachen und auszuwerten, um diese dann in die kontinuierliche Verbesserung vieler Themenbereiche mitzubeachten. Damit wird Threat Intelligence zu einem essenziellen Bestandteil der Früherkennung und Risikoabschätzung. Die Bewertung der Kritikalität der Schwachstellen sowie die Entscheidung über Gegenmaßnahmen und, wo nötig, die Entwicklung eines konkreten Maßnahmenplans müssen nachvollziehbar dokumentiert und priorisiert erfolgen. Auch die verantwortungsvolle Offenlegung von Schwachstellen, etwa gegenüber Lieferanten:innen oder in Koordination mit nationalen Stellen, gehört hierbei zum professionellen Umgang mit Sicherheitslücken.

Umsetzung im NIS2-ISMS-Framework: Ein Schwachstellenmanagement kann in einem KMU mithilfe vorhandener Ressourcen (z.B. Office-Produkte für Dokumentation sowie E-Mail für Meldung) und unterstützende Tools (Schwachstellenscanner) erfolgen. Im ersten Schritt ist hierbei festzulegen, an welche zentrale Stelle die Informationen über Schwachstellen geleitet werden sollen. Idealerweise handelt es sich

hierbei um den:die ISB und/oder der Leitung der IT-Abteilung. Des Weiteren ist festzuglegen, über welche Kanäle Informationen zu neuen Schwachstellen bezogen werden. Dazu sollten öffentliche und offizielle Stellen wie CERT.at sowie Newsletter von Hersteller:innen abonniert werden. Optional können hierfür auch Informationen über IT-Dienstleister:innen bezogen werden, sofern diese vertraglich geregelt sind (siehe Kapitel 5.7.1)

Um die eigenen Systeme aktiv auf bekannte Schwachstellen zu prüfen, sind geplante Schwachstellenscans in definierten Intervallen (zumindest halbjährlich) durchzuführen. Nähere Informationen zum Thema Durchführung von Schwachstellenscans werden im darauffolgenden Kapitel zu Sicherheitstests (5.9.4) behandelt. Wesentlich hierbei ist, dass die Ergebnisse von Scans, aber auch von Penetrationstests, dokumentiert (z.B. Ergebnisberichte der Tools inklusive der Kritikalität von CVSS) werden, sodass sie in das Schwachstellenmanagement integriert und behandelt werden können. Bei der Feststellung einer Schwachstelle muss diese bewertet werden. Empfehlenswert ist es hierbei den jeweiligen CVSS-Score der Schwachstelle zu betrachten, welcher üblicherweise durch das Schwachstellenscanner-Tool im Endbericht mitübergeben wird. Der CVSS-Score stammt aus dem Common Vulnerability Scoring System (CVSS), einem internationalen Industriestandard, welcher von FIRST.Org, Inc definiert und weiterentwickelt wird. Auf Basis des Scores wird nun die Kritikalität der Schwachstelle eingestuft, wofür die folgende Tabelle 5.5 des National Institute of Standards (NIST) herangezogen wird, welche den numerischen CVSS-Basis-Score (0-10) vordefinierten Schwereklassen zuordnet und somit ein sofort verständliches „Ampelsignal“ für die operative Priorisierung von Schwachstellenbehandlung liefert:

CVSS-Version	**Keine**	**Gering**	**Mittel**	**Hoch**	**Kritisch**
v2.0	0	0.0 - 3.9	4.0 - 6.9	7.0 - 10.0	-
v3.x / v4.0	0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0

Tabelle 5.5: Schwachstellenpriorisierung anhand des CVSS-Scores [54]

Zusätzliche sollte hier mitbetrachtet werden welches System von der Schwachstelle betroffen ist und ob es sich hierbei um ein kritisches Asset (siehe 5.3) handelt. Ist dies der Fall, sollte die Kritikalität manuell höhergestuft werden, um eine schnellere Priorisierung sicherzustellen. Sofern eine Schwachstelle als „Kritisch“ eingestuft wird, sollte diese ohne unangemessene Verzögerung behandelt werden. Beispielhafte Richtwerte könnten folgende sein, müssen jedoch an die eigenen Anforderungen und Bedürfnisse angepasst werden:

- Kritisch: innerhalb von 3 Werktagen

- Hoch: innerhalb von 5 Werktagen
- Mittel: innerhalb von 30 Kalendertagen
- Gering: Innerhalb von 90 Kalendertagen
- Keine: keine Maßnahmen erforderlich

Im nächsten Schritt erfolgt die Auswahl der Behandlungsmethode. Ist die Schwachstelle durch die Implementierung eines Patches zu beheben, wird der definierte Patchmanagement-Prozess angewendet (siehe Kapitel 5.9.5). Ist hingegen eine Behebung durch Anpassung der Konfiguration möglich, wird der Prozess des Konfigurationsmanagements herangezogen (siehe Kapitel 5.9.1).

Die Erfassung und Verwaltung erfolgt über ein zentrales Schwachstellenregister, in welchem Schwachstellen systematisch bewertet, Maßnahmen zugeordnet und relevante Verknüpfungen zu Patches, Änderungen sowie Risikoanalysen dokumentiert werden. Im Zuge dieser Arbeit wurde die Excel-Vorlage für ein Schwachstellenregister erstellt, welche von KMUs als Basis verwendet werden kann. Sollte eine Behebung weder durch Patches noch durch Konfigurationsänderungen möglich sein oder kann eine Schwachstelle aus nachvollziehbaren Gründen nicht innerhalb des vorgesehenen Zeitrahmens behandelt werden (beispielsweise aufgrund erheblicher technischer Komplexität oder fehlender personeller Ressourcen), ist eine strukturierte Ausnahmebehandlung erforderlich. Im Rahmen dieser Ausnahmebehandlung muss eine Risikoanalyse (siehe Kapitel 5.3.1) durchgeführt werden. Dabei sind insbesondere das betroffene Asset, die Kritikalität der Schwachstelle (CVSS) sowie die potenziellen Bedrohungen systematisch zu bewerten und nachvollziehbar zu dokumentieren. Darüber hinaus ist die konkrete Begründung für die verzögerte Umsetzung der Behebung festzuhalten und es müssen temporäre Schutzmaßnahmen definiert und dokumentiert werden (z.B. Einschränkung von Systemzugriffen oder eine intensivierte Überwachung relevanter Systeme).

Die Ergebnisse dieser Risikoanalyse sowie die getroffenen Schutzmaßnahmen sollten idealerweise durch den:die ISB oder die Leitung der IT-Abteilung formell freigegeben werden. Weiterhin ist ein Termin zur erneuten Überprüfung oder Neubewertung der Situation verbindlich festzulegen, um sicherzustellen, dass die Schwachstelle nicht unbegrenzt unbehandelt bleibt.

5.9.4 Sicherheitstests

Mapping - NIS2 Durchführungsverordnung (Punkt 6.5.): Abschnitt 6.5 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur Einführung und Umsetzung eines Konzepts sowie standardisierter Ver-

fahren für Sicherheitstests (6.5.1). Im Detail bedeutet dies (6.5.2):

- Die Notwendigkeit, der Umfang, die Häufigkeit und Art der Sicherheitstests sind risikobasiert festzulegen (6.5.2 a),
- Sicherheitstests sind auf Basis einer dokumentierten Testmethodik durchzuführen und müssen alle im Rahmen der Risikoanalyse als sicherheitsrelevant identifizierten Komponenten abdecken (6.5.2 b),
- Ergebnisse sind vollständig zu dokumentieren, inklusive Kritikalität und erforderlicher Gegenmaßnahmen (6.5.2 c),
- Bei kritischen Schwachstellen sind geeignete Maßnahmen ohne Verzögerung umzusetzen (6.5.2 d).

Das Konzept für Sicherheitstests ist regelmäßig zu überprüfen und bei Bedarf anzupassen (6.5.3).

Interpretation der Anforderungen: Sicherheitstests sind ein zentrales Instrument, um Schwachstellen in Assets nicht erst im Ernstfall, sondern kontrolliert im Vorfeld zu identifizieren. Die Anforderung unterstreicht, dass solche Tests nicht sporadisch, sondern systematisch, risikoorientiert und methodisch fundiert durchzuführen sind. Für KMUs bedeutet es, dass es einen klar definierten Prozess geben muss, welcher regelt, wann, wie und mit welchem Ziel Tests wie z.B. Penetrationstests, Schwachstellenscans oder Konfigurationsprüfungen durchgeführt werden. Grundlage dafür ist die Kritikalität der Assets (siehe 5.3) im Vorfeld analysiert zu haben. Wesentlich sind auch die Dokumentation und Bewertung der Testergebnisse: Nur wer genau nachvollziehen kann, welche Schwachstellen mit welcher Kritikalität bestehen, kann die richtigen Prioritäten setzen und Gegenmaßnahmen effizient umsetzen. Gerade bei kritischen Abweichungen und Schwachstellen ist eine schnelle Reaktion erforderlich. Dabei sind die Schnittstellen zu Änderungs- und Patch-Management (siehe Kapitel 5.9.2 und 5.9.5) entscheidend.

Umsetzung im NIS2-ISMS-Framework: Der erste Schritt ist die Erstellung einer themenspezifischen Richtlinie zum Thema Sicherheitstests, welche die grundlegenden Anforderungen an die Planung, Durchführung und Dokumentation von Sicherheitstests festlegt. Im Rahmen dieser Arbeit wurde hierfür die Richtlinienvorlage erstellt, welche KMUs als Basis verwendet und an die eigenen Wünsche anpassen können.

Im nächsten Schritt werden auf Basis der festgelegten Kritikalität der Assets (siehe Kapitel 5.3.1) die Art, der Umfang sowie die Frequenz der Sicherheitstests festgelegt. Diese Einteilung kann beispielsweise wie folgt aussehen:

- **Hohe Kritikalität:** Halbjährliche Schwachstellenscans und rotierende jährliche Penetrationstests aus-

gewählter Assets

- **Mittlere Kritikalität:** Jährliche Schwachstellenscans
- **Geringe Kritikalität:** Alle zwei Jahre Stichprobenkontrollen mittels Konfigurationsprüfungen

Die strategische Planung der Sicherheitstests erfolgt idealerweise zentral im Prüfprogramm (siehe Kapitel 5.3.4), um sicherzustellen, dass diese Aktivitäten nicht isoliert, sondern als integraler Bestandteil der kontinuierlichen Überwachung und Verbesserung der Informationssicherheit betrachtet werden.

Um darüber hinaus eine konsolidierte Übersicht sowie eine strukturierte Dokumentation sowohl geplanter als auch bereits durchgeführter Sicherheitstests sicherzustellen, wird die Nutzung eines zentralen Sicherheitstestregisters empfohlen. Dieses Register fasst die relevanten Informationen wie Art des Tests, Testumfang, Prüfziel und verantwortliche Stelle kompakt zusammen und verweist gegebenenfalls auf zugehörige Prüfberichte sowie auf weiterführende Prozesse wie das Schwachstellenmanagement. Im Rahmen dieser Arbeit wurde hierfür die Vorlage für das Sicherheitstestregister entwickelt, welche KMUs als Basis für die praktische Umsetzung dienen kann. Die Durchführung von Sicherheitstests richtet sich je nach der dokumentierten Testmethodik. Je nach Art des Tests wird ein eigenes Testverfahren definiert. Dies kann in einem KMU beispielsweise wie folgt erfolgen:

- **Automatisierte Schwachstellenscans:** Mithilfe von Schwachstellenscanner (z.B. OpenVAS, Nikto, Nmap, Nessus Tenable, Qualys, etc.) werden möglichst außerhalb der Geschäftszeiten Scans durchgeführt. Anschließend erstellt das Tool zur Dokumentation einen Scanbericht bestenfalls inklusive der CVSS-Scores.
- **Manuelle Konfigurationsprüfung:** Mithilfe von Checklisten wird stichprobenartig die Konfigurationseinstellungen gemäß den Konfigurations-Baselines überprüft. Ergebnisse und Abweichungen werden dokumentiert.
- **Penetrationstests:** Bei kritischen Systemen bzw. bei Bedarf werden durch spezielle IT-Dienstleister:innen Pentests durchgeführt. Hier sind vorab mit dem:der Dienstleister:in klare Kriterien wie Umfang und Ziele (z.B. Handelt es hierbei sich um einen „Blackbox“, „Greybox“-Test?) inklusive eines schriftlichen Statement of Work (SOW). Ein SOW stellt vertraglich sicher, welche Leistungen ein:e Dienstleister:in im Rahmen eines Auftrags erbringen muss. [55] Die Ergebnisse werden idealerweise mittels eines dokumentierten Endberichtes seitens Dienstleister:in festgehalten.

Aus den verschiedenen Tests resultieren schlussendlich Ergebnisse, welche typischerweise Schwachstellen

(z.B. Konfigurationslücken, CVEs) oder Abweichungen von Konfigurations-Baselines sein können. Diese dokumentierten Ergebnisse werden im nächsten Schritt in den Prozess des Schwachstellenmanagements (siehe Kapitel 5.9.3) in das zentrale Schwachstellenregister aufgenommen und dort auf Basis der Kritikalität weiterbehandelt.

Abschließend ist die Sicherheitstest-Richtlinie selbst mindestens jährlich durch den:die ISB gegebenenfalls mit der Unterstützung der IT-Abteilung sowie anlassbezogen zu überprüfen und bei Bedarf anzupassen. Die Ergebnisse der Überprüfung sind zu dokumentieren, um die kontinuierliche Verbesserung der Sicherheitstestprozesse sicherzustellen.

5.9.5 Patchmanagement

Mapping - NIS2 Durchführungsverordnung (Punkt 6.6.): Abschnitt 6.6 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur Einführung und Anwendung strukturierter Verfahren für das Management von Sicherheitspatches, abgestimmt auf die Prozesse des Änderungs-, Schwachstellen- und Risikomanagements (6.6.1). Konkret ist sicherzustellen, dass:

- Sicherheitspatches zeitnah nach Verfügbarkeit implementiert werden (6.6.1 a),
- Patches vor der Anwendung in Produktivsystemen getestet werden (6.6.1 b),
- Nur vertrauenswürdige und überprüfte Patchquellen verwendet werden (6.6.1 c),
- Bei nicht verfügbaren oder nicht umsetzbaren Patches Ersatzmaßnahmen definiert und Restrisiken akzeptiert werden (6.6.1 d).

In begründeten Ausnahmefällen kann auf die Anwendung eines Patches verzichtet werden, sofern die Nichtumsetzung nachvollziehbar begründet und dokumentiert wird (6.6.2).

Interpretation der Anforderungen: Patchmanagement ist nicht als „Nebenbei-Prozess“, sondern Teil eines koordinierten Sicherheits- und Betriebsmodells zu betrachten, welches eng mit dem Änderungs- und Schwachstellenmanagement (siehe Kapitel 5.9.2 und 5.9.3) verzahnt sein muss. Patches sind dabei nicht blind umzusetzen. Sie müssen getestet, geprüft und in ihrer Herkunft in Hinblick auf Integrität und Authentizität verifiziert werden. Für KMUs stellt sich oft die Herausforderung, zwischen Betriebssicherheit und Aktualität abzuwägen. Ausnahmen müssen hierfür sauber begründet, dokumentiert und im Rahmen des Risikomanagements (siehe Kapitel 5.3.1) bewertet werden.

Umsetzung im NIS2-ISMS-Framework: Als Basis zur Definition eines Patchmanagement-Prozesses sollte vorab ein Asset-Inventar inklusive der Zuordnung der jeweiligen verantwortlichen Stellen (z.B. IT-Abteilung) erfolgt sein (siehe Kapitel 5.4.1), welche dann im Normalfall später auch für den Prozess des Patchings zuständig sind. Ebenso ist die festgelegte Kritikalität der Assets entscheidend (siehe 5.3). Außerdem ist es ratsam, dass vorab die Themenbereiche Risikomanagement (siehe Kapitel 5.3.1) sowie Schwachstellenmanagement (siehe Kapitel 5.9.3) eine grundlegende Struktur aufweisen, da diese zur Einschätzung der Auswirkungen sowie Entscheidungsgrundlagen eine wichtige Rolle spielen. Schlussendlich sollte auch darauf geachtet werden, wie das Patchmanagement in der Umsetzung von Patches gestaltet sein kann, damit der Prozess in der Praxis auch umsetzbar ist. Beispielhafte Gedanken hierbei sind:

- Geschieht die Patchverteilung manuell oder automatisiert?
  - z.B. mithilfe von WSUS bei Windows, Skripte, etc.
- Gibt es Möglichkeiten Patches vor einem Rollout auf einem Testsystem zu testen?
  - Falls nein, beispielsweise vorab auf weniger kritischen Systemen testen

Sobald der Großteil dieser Voraussetzungen geschehen und abgestimmt ist, kann die Definition und Dokumentation eines Patchmanagement-Prozesses gestartet werden. Hierfür sollte im ersten Schritt im Prozess definiert und dokumentiert werden, wie die Zyklen regelmäßiger Patches z.B. nach Asset-Klassen und Kritikalität durchgeführt werden müssen. Patches, welche sich aus kritischen Schwachstellen ad-hoc ergeben, sind unverzüglich außerhalb des regulären Patch-Zyklus zu implementieren (siehe Kapitel 5.9.3). Beispielhafte regelmäßige Zyklen sind in der nachfolgenden Tabelle 5.6 dargestellt:

Systemtyp	**Beispielsysteme**	**Kritikalität**	**Patch-Intervall**	**Bemerkungen**
Server (physisch/ virtuell)	Domänencontroller, Fileserver, Anwendungsserver	Hoch	Monatlich (z.B. fix am 2. Dienstag)	Ad-hoc-Patching gemäß CVSS-Score (siehe Kapitel 5.9.3)
		Mittel / Gering	Quartalsweise	Dokumentation von Ausnahmen erforderlich

Systemtyp	Beispielsysteme	Kritikalität	Patch-Intervall	Bemerkungen
Clients / Endgeräte	Office-PCs, Notebooks	Alle Kategorien	Monatlich	WSUS / Windows Update empfohlen; bei geringer Kritikalität ggf. via Autoupdate

Tabelle 5.6: Beispielhafte Patch-Zyklen

Ein solcher Prozess ist im folgenden Text beispielhaft für ein KMU zusammengefasst. Monatlich sowie anlassbezogen sind verfügbare Patches zentral von den verantwortlichen Stellen der Assets zu überprüfen. Quellen umfassen Herstellerfeeds, CSIRTs, automatische Tools (z.B. WSUS) sowie manuelle Recherche. Dabei ist neben dem Patch selbst auch das Datum der Verfügbarkeit des Patches zu dokumentieren. Die zuständige Stelle bewertet im weiteren Schritt die Relevanz auf Basis betroffener Systeme sowie derer Kritikalität (siehe 5.3) und die Dringlichkeit des Patches. Ergebnis ist eine Patch-Entscheidung (z.B. „Umgesetzt“, „Ausnahme“, „Entfällt“), welche nachvollziehbar dokumentiert werden muss. Patches, welche zur Behebung von identifizierten Schwachstellen (siehe Kapitel 5.9.3) eingespielt werden, müssen entsprechend im Schwachstellenregister dokumentiert und der Status der Schwachstelle beispielsweise auf „behoben“ gesetzt werden. Falls möglich, sollte der Patch vorab auf einem Testsystem geprüft werden. Ist dies nicht umsetzbar (z.B. bei kritischen Updates), muss dies mit Begründung festgehalten werden. Die formelle Freigabe erfolgt durch eine autorisierte Person (z.B. ISB oder Leitung der IT-Abteilung). Die Umsetzung kann manuell oder automatisiert erfolgen. Zu dokumentieren sind der Zeitpunkt, die durchführende Person bzw. das beauftragte Unternehmen sowie gegebenenfalls Hinweise zu erforderlichen Reboots oder Besonderheiten (z.B. Fehlerhinweise). Zusätzlich ist bei der Patchdokumentation die zugehörige Schwachstellen-ID zu erfassen, um die vollständige Rückverfolgbarkeit der Schwachstellenbehandlung zu gewährleisten. Die Ergebnisse der Umsetzung werden in eines zentralen Patchregisters (z.B. Excel-Format) erfasst. Im Zuge dieser Arbeit wurde eine Vorlage für das Patchregister erstellt, welche von KMUs als Basis verwendet werden kann. Neben den technischen Details (z.B. Patch-ID, CVSS-Score) ist zusätzlich die Quelle des Patches (z.B. Microsoft Security Advisory, CERT.at-Meldung, Schwachstellenscan) im Register aufzunehmen. Kann ein sicherheitskritischer Patch nicht innerhalb des vorgesehenen Zeitrahmens eingespielt werden, ist eine Risikoanalyse gemäß dem Schwachstellenmanagement (siehe Kapitel 5.9.3) erforderlich. Neben der Durchführung einer Risikoanalyse ist im Fall einer Patch-Ausnahme ein Neubewertungsdatum im Patchregister zu dokumentieren, um die Risikoentwicklung regelmäßig zu überprüfen.

Der Prozess ist jährlich sowie anlassbezogen durch die verantwortlichen Stellen auf Aktualität zu überprüfen. Die Überprüfung der Einhaltung und Wirksamkeit des Patchmanagement-Prozesses obliegt dem:der ISB. Die Ergebnisse dieser Überprüfung fließen in die kontinuierliche Verbesserung ein.

5.9.6 Sicherheit bei der Beschaffung von Dienstleistungen, Systemen und Produkten

Mapping - NIS2 Durchführungsverordnung (Punkt 6.1.): Abschnitt 6.1 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen dazu, sicherheitsrelevante Risiken bei der Beschaffung von IKT-Produkten und -Dienstleistungen zu identifizieren, zu bewerten und zu steuern (6.1.1). Diese Prozesse müssen auf einer vorangegangenen Risikoanalyse basieren und den gesamten Lebenszyklus der Produkte bzw. Services (von der Auswahl über den Betrieb bis zum Austausch oder zur Außerbetriebnahme) abdecken. Konkret müssen folgende Anforderungen erfüllt sein (6.1.2):

- Definition spezifischer Sicherheitsanforderungen an zu beschaffende IKT-Produkte oder -Dienstleistungen (6.1.2 a),
- Festlegung von Anforderungen an Sicherheitsupdates und Support über den gesamten Lebenszyklus (6.1.2 b),
- Bereitstellung technischer Informationen zu verwendeten Komponenten und Sicherheitsfunktionen (6.1.2 c-d),
- Nachweis über die Einhaltung definierter Sicherheitsanforderungen durch die Lieferant:innen (6.1.2 e),
- Etablierung eines Validierungsprozesses zur Prüfung der Konformität der gelieferten Leistungen mit den Anforderungen (6.1.2 f).

Diese Beschaffungsprozesse sind regelmäßig zu überprüfen und bei Bedarf, insbesondere nach sicherheitsrelevanten Vorfällen anzupassen (6.1.3).

Interpretation der Anforderungen: Diese Anforderung konkretisiert die Anforderung aus dem Punkt zur Sicherheit in der Lieferkette und verpflichtet Einrichtungen, Sicherheitsanforderungen systematisch in Beschaffungsprozesse für IKT-Produkte und -Dienstleistungen zu integrieren. Kritische Komponenten dürfen nur beschafft werden, wenn:

- Sicherheitsanforderungen definiert, dokumentiert und vertraglich fixiert sind (z.B. zu Updates, sicheren Konfigurationen, Nachweispflichten),

- Lieferanten die Einhaltung nachweislich bestätigen, idealerweise durch Prüfberichte oder Zertifizierungen,
- der gesamte Lebenszyklus, inklusive Supportende, risikobasiert betrachtet wird.

Die Anforderung ist eng mit der Lieferkettenrichtlinie nach Kapitel 5.7.1 verknüpft. Insbesondere für sicherheitskritische Lieferanten gelten verschärfte Auswahl- und Kontrollvorgaben. So wird Beschaffung zu einem aktiven Steuerungsinstrument für die Informationssicherheit im Unternehmen.

Umsetzung im NIS2-ISMS-Framework: Auf Basis der identifizierten kritischen Assets (siehe 5.3) wird für die Beschaffung von IKT-Dienstleistungen und -Produkten, welche für die Assets relevant sind, ein kompakter Prozess definiert, welcher im Folgenden näher erklärt wird.

Vor der Beschaffung sicherheitsrelevanter IKT-Dienstleistungen und -Produkte sind risikobasiert Sicherheitsanforderungen festzulegen, welche sich auf Basis der themenspezifischen Richtlinien sowie der Leitlinie ableiten und bei Bedarf in der Ausschreibung beziehungsweise Bestellung zu berücksichtigen. Die Anforderungen wurden im Kapitel 5.7.1 bereits erläutert. Die Anforderungen sind verbindlich beispielsweise in einer Anforderungsliste oder einem Vertragsergänzungsblatt zu dokumentieren. Zur Absicherung der definierten Anforderungen wird bei kritischen Dienstleistungen (wird mithilfe einer Checkliste wie in Kapitel 5.7.1 evaluiert und dokumentiert) und Produkten folgendes vertraglich vereinbart:

- Verpflichtung zur Einhaltung aller spezifizierten Sicherheitsanforderungen
- Pflicht zur regelmäßigen Information über relevante Schwachstellen und Sicherheitsupdates
- Recht auf Prüfungen oder Einsicht in Sicherheitsaudits auf Anforderung
- Verpflichtung zur proaktiven Schwachstellenbehandlung mit definierten Fristen
- Vorgaben zur sicheren Entsorgung von Alt-Systemen nach Ende der Nutzungsdauer

Für bestehende Rahmenverträge sind diese Punkte bei Gelegenheit der Vertragsverlängerung oder im Rahmen von Nachträgen (z.B. SLA-Erweiterungen) nachzuziehen. Vor produktiver Nutzung sicherheitskritischer Komponenten erfolgt eine Prüfung der kritischen IKT-Dienstleistungen auf Konformität mit den definierten Sicherheitsanforderungen:

- Sichtprüfung anhand der gelieferten Dokumentationen
- Prüfung der Konfiguration auf Basis definierter Konfigurations-Baselines (siehe Kapitel 5.9.1)
- Optionale Durchführung von Schwachstellenscans oder Konfigurationsprüfungen

- Dokumentation der Ergebnisse im zentralen Sicherheitstestregister (siehe Kapitel 5.9.4)

Wie in Kapitel 5.7.1 erwähnt, findet eine Überprüfung der Einhaltung der Sicherheitsanforderungen bei kritischen Dienstleister:innen jährlich durch den:die ISB sowie die verantwortliche Stelle (z.B. Einkauf, IT-Abteilung) statt. Bei nicht kritischen Dienstleistungen und Produkten erfolgt diese Überprüfung stichprobenartig nur alle zwei bis drei Jahre. Erkannte Abweichungen sind im Risikomanagement (siehe Kapitel 5.3.1) zu integrieren und zu behandeln.
Alle beschafften sicherheitsrelevanten Produkte und Dienstleistungen sind im Lieferant:innenverzeichnis (siehe Kapitel 5.7.2) zu dokumentieren und pflegen. Der gesamte Beschaffungsprozess wird mindestens jährlich durch den:die ISB auf Aktualität und Wirksamkeit überprüft. Die Ergebnisse werden dokumentiert und in die kontinuierliche Verbesserung einbezogen.

5.9.7 Sichere Softwareentwicklung

Mapping - NIS2 Durchführungsverordnung (Punkt 6.2.): Abschnitt 6.2 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur Implementierung und Anwendung von Sicherheitsvorgaben im gesamten Entwicklungslebenszyklus (Secure Development Life Cycle, SDLC) für Netz- und Informationssysteme. Das ist unabhängig davon zu tun, ob die Entwicklung intern oder durch Dritte erfolgt (6.2.1). Folgende Anforderungen sind hierbei umzusetzen (6.2.2):

- Sicherheitsanforderungen sind bereits in den Spezifikations- und Designphasen zu analysieren (6.2.2 a),
- Es sind sichere Entwicklungsprinzipien und -methoden anzuwenden (6.2.2 b),
- Sicherheitsvorgaben für Entwicklungsumgebungen müssen definiert werden (6.2.2 c),
- Es sind Sicherheitstests innerhalb des Entwicklungsprozesses zu etablieren (6.2.2 d),
- Testdaten müssen gezielt ausgewählt, geschützt und anonymisiert werden (6.2.2 e-f).

Bei ausgelagerter Entwicklung gelten zusätzlich die Anforderungen aus den Punkten 5 und 6.1 der Verordnung (6.2.3). Die SDLC-Vorgaben sind regelmäßig zu überprüfen und bei Bedarf zu aktualisieren (6.2.4).

Interpretation der Anforderungen: Sicherheit darf nicht erst am Ende eines Entwicklungsprojekts geprüft werden, sondern sie muss von Anfang an systematisch mitgedacht und technisch verankert sein. Abschnitt 6.2 der Durchführungsverordnung stellt klar, dass die Integration von Sicherheitsaspekten über alle Phasen des Entwicklungsprozesses hinweg zwingend erforderlich ist, unabhängig davon, ob es sich um Eigenent-

wicklungen oder externe Aufträge handelt. Für KMUs bedeutet das, dass bereits vor den ersten Code-Zeilen Sicherheitsanforderungen analysiert, dokumentiert und berücksichtigt werden müssen. Ebenso wichtig ist die Absicherung der Entwicklungsumgebungen selbst, inklusive Zugangskontrollen und Trennung von Test- und Produktionsdaten. Insbesondere beim Testen sensibler Funktionen ist darauf zu achten, dass personenbezogene oder geschäftskritische Informationen ausschließlich in anonymisierter Form verarbeitet werden. Auch bei ausgelagerter Entwicklung bleibt die Verantwortung bei der Organisation. Es gilt, Sicherheitsvorgaben vertraglich festzuschreiben, zu kontrollieren und bei Verstößen Konsequenzen zu ziehen (siehe Kapitel 5.7.1)

Umsetzung im NIS2-ISMS-Framework: Zu Beginn ist die Definition und Dokumentation von Vorgaben für einen sicheren Softwareentwicklungsprozess („Secure Software Development Lifecycle“, SDLC) erforderlich. Hierfür können KMUs ein kompaktes Dokument mit SDCL-Vorgaben erstellen. Als Basis hierfür eignet sich die technische Richtlinie „TR-03185 Sicherer Software-Lebenszyklus“ des BSI IT-Grundschutzes, welche praxistaugliche Vorgaben zur sicheren Entwicklung enthält und an die eigenen Bedürfnisse abgeleitet und angepasst werden kann. [56] Die Richtlinie behandelt Anforderungen im gesamten Lebenszyklus von Software, von Projektmanagement, Entwicklung und Test über Auslieferung bis hin zur Außerbetriebnahme. Sie strukturiert Anforderungen sowohl für die Nutzung von Entwicklungswerkzeugen als auch für die eigentliche Softwareproduktion und orientiert sich dabei an etablierten Normen (z.B. NIST, BSI IT-Grundschutz, etc.). [57, pp. 5-6] Vorab ist seitens der IT-Abteilung sicherzustellen, dass alle Entwicklungsumgebungen durch organisatorische und technische Maßnahmen geschützt werden. Dazu gehören beispielsweise:

- Trennung der Entwicklungs-, Test- und Produktivsysteme (siehe Kapitel 5.9.8)
- Einschränkung der Zugriffsrechte auf Entwicklungsumgebungen (z.B. nur berechtigte Entwickler:innen)

Bereits in der Spezifikations- und Designphase von Entwicklungen und Projekten müssen die vorher definierten SDLC-Anforderungen in Bezug auf die Planung überprüft und ihre Konformität dokumentiert werden. Hierzu kann eine einfache Checkliste verwendet werden, welche sicherstellt, dass beispielsweise folgende Punkte vor der Entwicklung oder Einführung von Projekten geprüft werden:

- Erforderliche Authentifizierungs- und Autorisierungsmechanismen
- Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit sowie Authentizität
- Anforderungen an sichere Datenhaltung und Übertragung (z.B. Verschlüsselung)

Die Ergebnisse dieser durchgearbeiteten Checkliste sind projektbegleitend durch eine verantwortliche Stelle (z.B. Projekt- /Entwicklungsleiter:innen) beispielsweise direkt in der jeweiligen Checkliste zu dokumentieren.

Im nächsten Schritt sollten bei der Entwicklung selbst Prinzipien der sicheren Entwicklung „Secure Coding Guidelines“ durch die Entwickler:innen angewendet werden. Hierfür empfiehlt es sich auf öffentliche Ressourcen wie die „Secure Coding Practices“ des „Open Worldwide Application Security Project“ („OWASP“) zurückzugreifen. Die OWASP „Secure Coding Practices“ bieten eine technologieunabhängige, praxisorientierte Sammlung allgemeiner sicherer Programmierpraktiken, die in den Softwareentwicklungszyklus integriert werden können, um typische Sicherheitslücken zu vermeiden. Thematisch decken sie Bereiche wie Eingabevalidierung, sichere Authentifizierung, Sitzungsmanagement, Fehlerbehandlung, Datenschutz, kryptographische Verfahren und weitere sicherheitsrelevante Aspekte der Softwareentwicklung ab. [58, pp. 3-14] Die Einhaltung dieser Coding Guidelines sollte im Rahmen von Code-Reviews geprüft werden. Dabei ergänzen manuelle Code-Reviews automatisierte Analysen um die Erkennung komplexer Sicherheitslogiken und Designfehler, welche durch Tools alleine oft nicht entdeckt werden. Im Zuge der Softwareentwicklung sind gezielte Sicherheitstests, unter Verantwortung der verantwortlichen Stelle, integraler Bestandteil, um Schwachstellen frühzeitig zu erkennen und zu beheben, bevor Systeme produktiv eingesetzt werden. KMUs sollten hierzu pragmatisch und ressourcenschonend vorgehen. In der folgenden Tabelle 5.7 werden empfohlene Testmethoden inklusive deren Nutzen und Umsetzung für KMUs zusammengefasst:

Testmethode	**Zweck im SDLC-Prozess**	**Beispielhafte Umsetzung**
Automatisierte statische Codeanalyse (“Static Application Security Testing”; “SAST”)	Identifiziert Schwachstellen im Quellcode, bevor die Anwendung läuft	One-Click Code-Scanning Workflow (z.B. GitHub CodeQL/Code Scanning) vor jedem Commit/Pull-Request bzw. spätestens vor Merge in Main-Branch [59]
Dynamische Sicherheitstests (“Dynamic Application Security Testing”, “DAST”)	Findet Laufzeitfehler wie SQL-Injection, Fehlkonfigurationen, etc.	OWASP ZAP Baseline als GitHub/GitLab Action [60]

Tabelle 5.7: Empfohlene Testmethoden für KMUs

Zusätzlich sollten anlassbezogen und je nach Kritikalität des entwickelten Produktes (z.B. Anwendungen, die an kritische Assets angebunden werden) Sicherheitstests durch externe Dienstleistende in Form von Penetrationstests durchgeführt werden. Nähere Details zur Durchführung und vertraglichen Absicherung solcher Tests werden in Kapitel 5.9.4 erläutert. Im Rahmen von Sicherheitstests ist zudem sicherzustellen, dass keine echten personenbezogenen oder sensiblen Daten verwendet werden. Stattdessen sind anonymisierte oder synthetische Testdaten zu generieren und nach Abschluss der Tests sicher zu löschen. Werden Entwicklungen an externe Dienstleistende ausgelagert, sind diese verpflichtet die definierten Sicherheitsanforderungen zur sicheren Entwicklung sowie des SDCL-Prozesses einzuhalten. Hierzu müssen entsprechende Vorgaben und Pflichten vertraglich geregelt werden (siehe Kapitel 5.7.1 sowie 5.9.6)

Die definierten Vorgaben für die sichere Entwicklung sowie die festgelegten Prozesse sind mindestens jährlich sowie anlassbezogen durch den:die ISB sowie gegebenenfalls die IT-Abteilung zu prüfen und gegebenenfalls zu aktualisieren. Ergebnisse werden dokumentiert und in die kontinuierliche Verbesserung integriert.

5.9.8 Netzwerksegmentierung

Mapping - NIS2 Durchführungsverordnung (Punkt 6.8.): Abschnitt 6.8 verpflichtet Einrichtungen zur risikobasierten Segmentierung von Netzwerken und Systemen gemäß der Risikoanalyse nach Punkt 2.1 der Verordnung (6.8.1). Im Detail müssen Einrichtungen (6.8.2):

- Funktionale, logische und physische Beziehungen zwischen Systemen berücksichtigen (a),
- Zugriffe zonenbasiert und schutzbedarfsorientiert steuern (b),
- Kritische Systeme in besonders gesicherten Zonen betreiben (c),
- Demilitarisierte Zonen (DMZ) für externe Kommunikation einsetzen (d),
- Zonenkommunikation auf das Notwendige beschränken (e),
- Admin-Netze, Produktions-, Entwicklungs- und Backup-Systeme voneinander trennen (f-h).

Die Segmentierung ist regelmäßig und bei Änderungen zu überprüfen und anzupassen (6.8.3).

Interpretation der Anforderungen: Netzwerksegmentierung ist ein zentrales Instrument zur Eindämmung von Sicherheitsvorfällen und zur Vermeidung lateraler Bewegungen durch Angreifer:innen. Die Anforderung verlangt, dass Systeme nicht pauschal vernetzt, sondern gezielt in Zonen auf Basis ihrer Kritikalität (siehe 5.3) sowie Funktion unterteilt werden. Kritische Systeme gehören in isolierte, besonders geschützte

Segmente. Kommunikationswege (intern sowie extern) müssen gezielt beschränkt und über DMZs abgesichert werden. Entwicklungs- und Testumgebungen sind strikt von produktiven Systemen zu trennen. Eine saubere Segmentierung erhöht nicht nur die Sicherheit, sondern erleichtert auch die Überwachung, Fehler- sowie Ursachenanalyse bei Sicherheitsvorfällen.

Umsetzung im NIS2-ISMS-Framework: Als Grundvoraussetzung sollte im Zuge der BIA (siehe Kapitel 5.3.1) sowie der Verwaltung der Vermögenswerte (siehe Kapitel 5.4.1) bereits eine vollständige Identifikation und Dokumentation der sicherheitsrelevanten Assets inklusive ihrer Kritikalität erfolgen. Zusätzlich ist empfehlenswert die im nachfolgenden Kapitel 5.9.9 beschriebene Netzwerkübersicht bereits erstellt zu haben. Auf Basis der erstellten Netzwerkübersicht empfiehlt es sich, dass idealerweise die IT-Abteilung unter Kontrolle des:der ISB die Systeme in logische Sicherheitszonen einteilt. Diese Vorgehensweise basiert auf dem Ansatz, wie im Whitepaper SSecurity Segmentation in a Small Manufacturing Environment"des NIST beschrieben wird. [61, pp. 5-14] Das Whitepaper bietet eine praxisorientierte, schrittweise Anleitung, die speziell auf kleinere Organisationen sowie KMUs zugeschnitten ist und deren begrenzte Ressourcen berücksichtigt. Das NIST-Whitepaper schlägt dabei unter anderem folgende Grundsätze vor:

- Kritische Systeme (wie produktive Server oder Fertigungsanlagen) sollten in eigenen, stark gesicherten Zonen betrieben werden.
- Verwaltungs- und Managementnetzwerke (z.B. für Firewalls, Switches) müssen von produktiven Netzen physisch oder logisch getrennt sein.
- Entwicklungs-, Test- und Backup-Systeme sollten in eigene Zonen ausgelagert werden, um Risiken durch unbeabsichtigte Fehler oder Schwachstellen zu minimieren.
- Externe Verbindungen und öffentlich erreichbare Systeme (z.B. Webserver, VPN-Gateways) sollten zwingend über eine separate DMZ geführt werden.

Eine beispielhafte Zoneneinteilung könnte auf Basis davon in einem KMU wie folgt gestaltet werden:

- Produktivnetz (z.B. ERP- und Fileserver, produktive Anwendungen)
- Managementnetz (z.B. Administrator:innen zugänge auf Firewalls und Router; wie gefordert in Kapitel 5.8.3)
- Entwicklungs- und Testnetz (z.B. Testserver, Entwicklungssysteme; wie gefordert in Kapitel 5.9.7)
- DMZ (z.B. Webserver, VPN-Gateways)
- Backupnetz (z.B. isolierte Speicher für Sicherungen)

Nach der grundlegenden Definition der Zonen sollte die technische Umsetzung der Segmentierung durch die IT-Abteilung erfolgen. Hierbei empfiehlt es sich insbesondere für KMUs, die Trennung pragmatisch und ressourcenschonend über Virtual Local Area Networks (VLANs) sowie ergänzende Firewalls mit Firewall-Regeln umzusetzen. VLANs ermöglichen eine logische Trennung innerhalb einer bestehenden Netzwerkinfrastruktur, ohne zusätzlicher Hardware. Firewalls kontrollieren ergänzend den Datenverkehr zwischen den VLANs mithilfe von Regeln. Dabei ist der Fokus auf ein Mindestmaß an Sicherheitsanforderungen zu legen. Beispielsweise sollte verhindert werden, dass Systeme innerhalb einer DMZ direkt mit dem internen Produktivnetz kommunizieren können. Eine solche Isolation reduziert das Risiko, dass ein erfolgreich kompromittiertes System in der DMZ auf kritische interne Systeme zugreifen kann.

Eine konkrete Kommunikationsmatrix zwischen den Zonen sollte klar definiert und dokumentiert werden. Diese Matrix kann auf Basis des Whitepapers wie in der folgenden Tabelle 5.8 aufgebaut sein:

Quelle (Zone)	**Ziel (Zone)**	**Erlaubte Protokolle/Ports**	**Zweck**	**Kommentar**
Management-Netz	Produktivnetz (Server)	SSH (Port 22)	Administration von Servern	Nur Admin-Nutzer erlaubt
DMZ (Webserver)	Produktivnetz (Datenbank)	MySQL (Port 3306)	Webserver-Abfragen an Datenbank	Eingeschränkter Zugriff
Clients (Büro-Netz)	Internet	HTTPS (Port 443)	Webnutzung	Gefiltert über Proxy

Tabelle 5.8: Beispielhafte Kommunikationsmatrix

Entscheidend laut dem Whitepaper von NIST ist, dass die Kommunikation zwischen Zonen auf das absolut notwendige Maß beschränkt wird („least privilege communication“) und kritische Systeme so weit wie möglich isoliert bleiben, um die Auswirkungen eines potentiellen Angriffs zu minimieren. [61, pp. 5-14] Hierfür sollte operativ jeder definierten Zone eine eigene VLAN-ID (z.B. 10/20/20/40) zugewiesen werden. Je VLAN wird dann ein eigenes Firewall-Interface angelegt, wobei die Default-Policy auf „deny all“ sichergestellt werden muss. Für erforderliche Netzwerkverkehre müssen explizite Regeln freigeschalten werden. Sollten Änderungen an den Firewall-Regeln nötig sein, ist hierfür der Änderungsprozess (siehe Kapitel 5.9.2) inklusive nötiger Freigaben zu initiieren, um einen formalen und sicheren Vorgang sicherzustellen.

Wie beispielsweise schon in Kapitel 5.9.6 erwähnt, sind Entwicklungs-, Produktiv und Testumgebungen zu trennen. Hierfür empfiehlt es sich, die Systeme, welche für die Entwicklung und Testung verwendet werden (z.B. bei Tests von Patches oder Entwicklungen von Anwendungen) in ein separates VLAN mit Internetzugang zu geben, wobei sichergestellt werden muss, dass die Netzwerkkommunikation zu Produktivdatenbanken blockiert ist.

Im Rahmen einer jährlichen sowie anlassbezogenen (z.B. bei Änderungen in der Netzwerkinfrastruktur oder neuen Servern) Überprüfung wird das Zonenkonzept sowie die umgesetzten Segmentierungen im Netzwerk durch die IT-Abteilung unter der Initiierung und Kontrolle des:der ISB überprüft. Die Ergebnisse werden dokumentiert und fließen in die kontinuierliche Verbesserung ein.

5.9.9 Netzwerksicherheit

Mapping - NIS2 Durchführungsverordnung (Punkt 6.7.): Abschnitt 6.7 verpflichtet Einrichtungen, angemessene Maßnahmen zum Schutz ihrer Netz- und Informationssysteme vor Cyberbedrohungen zu ergreifen (6.7.1). Diese Maßnahmen müssen umfassend und technisch fundiert umgesetzt werden. Konkret fordert die Verordnung (6.7.2):

- Eine aktuelle und verständliche Dokumentation der Netzarchitektur (a),
- Technische Zugriffs- und Kommunikationskontrollen, unter anderem zur Abschottung interner Netze, Verhinderung unnötiger Verbindungen und Sicherung von Fernzugriffen (b-d),
- Strikte Ressourcenzuordnung und Trennung sicherheitsrelevanter Systeme (e-g),
- Temporäre und kontrollierte Freigaben für Dienstleister:innenzugriffe (h),
- Sichere Kommunikation zwischen Systemen über abgesicherte, vertrauenswürdige Kanäle (i),
- Strategien zur Einführung moderner Netzwerk- und E-Mail-Protokolle sowie DNS- und Routing-Sicherheitsstandards (j-l).

Alle Maßnahmen sind regelmäßig zu überprüfen und bei Bedarf zu aktualisieren (6.7.3).

Interpretation der Anforderungen: Die Anforderung adressiert die grundlegenden technischen Schutzmaßnahmen zur Vermeidung, Erkennung und Abwehr netzwerkbasierter Angriffe. Die Anforderungen verdeutlichen, dass Netzwerksicherheit nicht punktuell, sondern ganzheitlich und kontinuierlich umzusetzen ist. Es braucht eine klare Netzarchitektur mit definierten Schutzmaßnahmen, insbesondere zur Segmentierung interner Netze (siehe vorheriges Kapitel 5.9.8), Steuerung von Remote-Zugriffen und Abschaltung

unnötiger Dienste. Fernzugriffe z.B. durch Dienstleister:innen dürfen nur autorisiert und zeitlich begrenzt erfolgen (siehe Kapitel 5.8.2). Datenflüsse zwischen Systemen müssen verschlüsselt, logisch getrennt und manipulationssicher sein. Darüber hinaus verlangt die Verordnung die Einführung aktueller Standards (z.B. DNSSEC, IPv6, sichere E-Mail-Protokolle).

Umsetzung im NIS2-ISMS-Framework: Als Grundvoraussetzung für diese Anforderungen dient das erstellte Asset-Inventar (siehe Kapitel 5.4.1) inklusive der festgelegten Asset-Kritikalität (siehe Kapitel 5.3.1). Zu Beginn wird seitens der IT-Abteilung eine Übersicht des Netzwerkes erstellt, um Transparenz über die Netzwerkarchitektur zu bekommen. KMUs können zur Darstellung einfache Tools wie Microsoft Visio, draw.io oder PowerPoint verwenden. Entscheidend bei der Darstellung ist, dass die logische Struktur und die Kommunikationsflüsse verständlich dargestellt werden. Die Darstellung umfasst insbesondere:

- Hauptnetzwerke nach den definierten Sicherheitszonen (siehe Kapitel 5.9.8)
- Zentral eingebundenen Systeme (z.B. Clients, Server, Firewalls, Switches, Router, etc.)
- Verbindungen (z.B. Ethernet)
- Verbindungen zu externen Dienstleistenden oder in das Internet (z.B. via DSL)

Zur besseren Übersichtlichkeit können im Netzplan Systeme gruppiert dargestellt werden. [62] Die zugrundeliegende Gruppierungslogik orientiert sich dabei sinnvollerweise an den Asset-Klassen aus dem Asset-Inventar (siehe Kapitel 5.4.1), da diese bereits nach Funktion, Schutzbedarf und Kritikalität strukturiert sind. Während das Asset-Inventar vorrangig Verwaltungs- und Schutzinformationen enthält, dient der Netzplan der Visualisierung der physischen oder logischen Netzwerkstruktur und der Kommunikationsflüsse. Der Netzwerkplan ist im Rahmen einer jährlichen sowie anlassbezogenen (z.B. Änderungen in der Netzwerkinfrastruktur) Prüfung von der IT-Abteilung unter Initiierung und Kontrolle des:der ISB zu prüfen. Die Ergebnisse werden dokumentiert und fließen in die kontinuierliche Verbesserung ein. Nach Erstellung und Dokumentation des aktuellen Netzwerkplans sowie der operativen Umsetzung der grundlegenden Sicherheitszonen (siehe Kapitel 5.9.8) ergibt sich im nächsten Schritt die Notwendigkeit, spezifische Schutzmaßnahmen innerhalb des Netzwerkes umzusetzen. Die Umsetzung der nachfolgenden Netzwerksicherheitsmaßnahmen erfolgt risikobasiert. Auf Grundlage der Asset-Kritikalität sowie der Ergebnisse der Risikoanalyse (siehe Kapitel 5.3.1) sollten die Maßnahmen priorisiert und sukzessive eingeführt werden. Sollte die technische Umsetzung einer Maßnahme im spezifischen KMU-Umfeld nicht möglich oder wirtschaftlich unverhältnismäßig sein, ist dies nachvollziehbar zu begründen und in eine formale Risikoanalyse (siehe Kapitel 5.3.1) aufzunehmen. In diesen Fällen sind alternative technische oder organisatorische Er-

satzmaßnahmen zu definieren, um ein vergleichbares Schutzniveau sicherzustellen.

Die Schutzmaßnahmen umfassen insbesondere:

- **Absicherung des Fernzugriffs:** Um den Fernzugriff auf Assets sicher zu gestalten, müssen externe Verbindungen ausschließlich über eine zentrale VPN-Lösung (z.B. Wireguard) erfolgen, welcher nur autorisierten Nutzer:innen den Zugriff ermöglicht. Organisatorisch wird in einer verbindlichen Richtlinie festgelegt, dass Fernzugriffe nur mit MFA (siehe Kapitel 5.8.7) zugelassen sind und ausschließlich auf explizit autorisierte Systeme erfolgen dürfen. Zudem wird organisatorisch ein Prozess eingeführt, wonach jeder externe Zugriff zeitlich befristet, formal beantragt und freigegeben werden muss. Technisch erfolgt dies durch temporäre VPN-Nutzer:innenkonten mit automatisiertem Ablaufdatum. Der Zugang wird zusätzlich auf das unbedingt notwendige System oder Netzwerksegment begrenzt und nach Ablauf automatisch deaktiviert. Nähere Informationen hierzu werden in Kapitel 5.8 thematisiert.
- **Absicherung von Administrationssystemen:** Die Administration von Systemen erfolgt ausschließlich über dedizierte, speziell geschützte Admin-PCs. [63] Diese Admin-Systeme dürfen weder für E-Mail-Verkehr noch für allgemeines Internet-Surfen verwendet werden. Technisch kann hierfür ein separates Netzwerksegment für Admin-Systeme eingerichtet werden (siehe Kapitel 5.9.8).
- **Blockieren nicht benötigter Verbindungen und Dienste:** VLANs sollten in Kombination mit Firewalls eingerichtet werden, deren Default-Policy den Datenverkehr blockiert. Notwendige Verbindungen werden explizit freigeschaltet und dokumentiert. Zusätzlich sollten regelmäßige Überprüfung aktiver Dienste mittels Discovery-Scan-Tools (z.B. Nmap) und Abschaltung nicht benötigter Dienste auf Servern und Netzwerkkomponenten durchgeführt werden. [64, p. 24]
- **Zulassung autorisierter Geräte:** Um sicherzustellen, dass nur vertrauenswürdige Endgeräte Zugang zum Netzwerk erhalten, sollten ausschließlich die im zentralen Asset-Inventar erfassten Geräte zugelassen werden. Technisch erfolgt die Absicherung kabelgebundener Zugänge durch MAC-Sticky-Listen auf Switchports sowie WLAN-Zugänge über 802.1X-Authentifizierung mit WPA2-Enterprise und zentraler Benutzerkontrolle. Organisatorisch wird ein Freigabeprozess etabliert, bei dem neue Geräte nur nach formaler Genehmigung und Inventareintrag aktiviert werden dürfen. [65], [66]
- **Modernisierung der Netzwerkprotokolle:** Es wird geraten, den schrittweisen Umstieg auf IPv6 zu planen. Dabei empfiehlt sich ein stufenweises Vorgehen gemäß dem ISi-L-IPv6-Leitfaden: zunächst Dual-Stack-Betrieb, anschließend flächendeckende Aktivierung und schrittweise Abschaltung veralteter IPv4-Dienste. [67, pp. 16-18]

- **Sichere Kommunikationskanäle:** Die Kommunikation zwischen Systemen sollte ausschließlich über vertrauenswürdige, kryptographisch gesicherte Kanäle (z.B. TLS 1.3 oder IPsec) erfolgen. Hierbei können die Empfehlungen der TR-02102-1 bezüglich verwendeter Algorithmen und Schlüssellängen als Basis verwendet werden. [41, pp. 28-30]
- **Absicherung der E-Mail-Kommunikation:** Um die Sicherheit der E-Mail-Kommunikation zu gewährleisten, sollte ein MTA-STS-fähiger Mailserver eingerichtet werden. Die E-Mail-Infrastruktur ist zusätzlich mit SPF, DKIM und DMARC abzusichern und regelmäßig durch externe Tools auf ihre Wirksamkeit hin zu überprüfen. [68, pp. 9-11]

Im Rahmen einer jährlichen sowie anlassbezogenen Prüfung werden durch die IT-Abteilung unter der Initiierung und Kontrolle des:der ISB die Schutzmaßnahmen auf die Aktualität und Wirksamkeit überprüft. Die Ergebnisse der Überprüfung werden dokumentiert und fließen in die kontinuierliche Verbesserung ein.

5.9.10 Schutz vor bösartiger und unautorisierter Software

Mapping - NIS2 Durchführungsverordnung (Punkt 6.9.): Abschnitt 6.9 verpflichtet Einrichtungen dazu, geeignete Schutzmaßnahmen gegen bösartige und nicht autorisierte Software zu implementieren, um die Integrität und Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten (6.9.1). Konkret müssen Maßnahmen zur Erkennung und Verhinderung der Nutzung solcher Software umgesetzt werden (6.9.2). Darüber hinaus ist sicherzustellen, dass (soweit angemessen) aktuelle Erkennungs- und Reaktionslösungen eingesetzt werden, deren Pflege sich an der Risikoanalyse (siehe Punkt 2.1 der Verordnung) und den vertraglichen Vereinbarungen mit Anbieter:innen orientiert.

Interpretation der Anforderungen: Die Anforderung macht deutlich, dass dieser Schutz vor Schadsoftware und nicht autorisierten Anwendungen nicht allein durch klassische Antivirenlösungen, sondern durch aktuelle, risikoorientierte Sicherheitslösungen sichergestellt werden muss. Hierfür sollten zentrale Schutzmechanismen wie Malware-Scanner, Applikationskontrollen oder Endpoint Detection & Response (EDR) etabliert sein. Entscheidend ist dabei, dass der Einsatz dieser Lösungen am tatsächlichen Risiko ausgerichtet und durch eine vorherige Analyse (siehe 5.3.1) begründet ist.

Umsetzung im NIS2-ISMS-Framework: Zu Beginn sollte eine zentrale Antivirus- und Endpoint-Protection-Lösung auf allen Endgeräten (unter anderem Notebooks, PCs, Servern) installiert werden. Als Basis gilt hier wieder das Asset-Inventar (siehe Kapitel 5.4.1), welches einen Überblick über die eingesetzten Betriebssys-

teme (z.B. Windows, Linux, etc.) gibt.

Eine geeignete Anti-Malware-Lösungen für KMUs bei einer vorhandenen Microsoft 365 Umgebung (z.B. Windows Clients) ist beispielsweise „Microsoft Defender for Business“, welche Schutz vor Bedrohungen wie Ransomware, Malware und Phishing bietet. Die Lösung ist eigenständig als auch im Rahmen von Microsoft 365 Business Premium verfügbar. [69] Alternativ kann hier auch der standardmäßige Windows Defender Antivirus zentral über GPOs konfiguriert werden. Zusätzlich empfiehlt sich für hybride Umgebungen (z.B. Windows und Linux) das Tool „Bitdefender GravityZone Business Security“. Für Linux-Server könnte auch beispielsweise das Tool „ClamAV“ eingesetzt werden. [70] Sobald ein passendes und zuverlässiges Tool ausgewählt und implementiert wurde, sollte im nächsten Schritt das Tool so konfiguriert werden, dass es automatisiert und mehrmals täglich die neuesten Informationen über Bedrohungen („Malware-Signature-Updates“) bezieht. Auch die Anti-Malware-Lösung selbst sollte mittels regelmäßiger Patches (siehe Kapitel 5.9.5) auf dem aktuellsten Stand gehalten werden. Zusätzlich sollte sichergestellt werden, dass der „Echtzeitschutz“ immer aktiviert ist, sodass Bedrohungen proaktiv erkannt werden können.

Neben einem Anti-Malware-Tool sollte auf den Endgeräten die eigenwillige Installation von Softwares eingeschränkt und blockiert werden, sodass nur Administrator:innen dazu berechtigt sind. Sollte es Anforderungen bezüglich neuer Software in einzelnen Fachbereichen ergeben ist dies mittel des Änderungsmanagementprozesses (siehe Kapitel 5.9.2) formal zu beantragen und nach einer Freigabe umzusetzen. Außerdem kann mittels Windows-Applocker geregelt werden, welche Anwendungen auf den Endgeräten ausgeführt werden dürfen. [71] Zudem sollten mithilfe Schwachstellenscans kritische Endgeräte regelmäßig überprüft werden. Für nähere Informationen siehe Kapitel 5.9.4 Im Kapitel 5.11.2 wird des Weiteren das Thema „Überwachung und Protokollierung“ behandelt, welches für die proaktive Erkennung von Malware sowie Bedrohungen ebenso relevant ist.

5.10 Kryptographie

Kryptographische Maßnahmen sind ein essenzieller Bestandteil der Informationssicherheit und schützen die Vertraulichkeit, Integrität und Authentizität sensibler Daten. Dieses Kapitel zeigt auf, wie KMUs eine konsistente Kryptographierichtlinie entwickeln und umsetzen können, um sensible Daten sowohl bei der Übertragung als auch in der Speicherung zu schützen. Dabei werden Anforderungen an den Einsatz geeigneter kryptographischer Verfahren, die Auswahl von Algorithmen und Protokollen sowie ein sicheres

Schlüsselmanagement behandelt.

5.10.1 Kryptographierichtlinie

Mapping - NIS2 Durchführungsverordnung (Punkt 9.): Abschnitt 9 verpflichtet Einrichtungen zur Einführung und Anwendung eines Konzeptes zur sicheren Nutzung kryptographischer Verfahren, um die Vertraulichkeit, Integrität und Authentizität von Informationen sicherzustellen (9.1). Die Umsetzung hat risikobasiert und unter Berücksichtigung der Asset-Klassifizierung zu erfolgen. Konkret fordert die Verordnung (9.2):

- Die Definition kryptographischer Schutzmaßnahmen entsprechend der Kritikalität der betroffenen Systeme und Daten, sowohl für ruhende Daten (at rest) als auch für Daten in Übertragung (in transit) (a),
- Die verbindliche Festlegung zulässiger Protokolle, Algorithmen, Schlüssellängen und kryptographischer Lösungen unter Berücksichtigung kryptographischer Agilität (b),
- Einen strukturierten Ansatz zum Schlüsselmanagement, einschließlich Verfahren zur Schlüsselgenerierung, Zertifikatsverwaltung, Schlüsselverteilung und -speicherung, Schlüsselwechsel, Umgang mit kompromittierten oder verlorenen Schlüsseln, Archivierung, Zerstörung sowie Protokollierung aller Schlüsselaktivitäten (c),
- Eine zeitliche Begrenzung der Schlüsselverwendung durch Aktivierungs- und Deaktivierungsregeln (c.xii).

Das Konzept sowie die Verfahren sind regelmäßig zu überprüfen und bei Bedarf unter Berücksichtigung des Stands der Technik zu aktualisieren (9.3).

Interpretation der Anforderungen: Die Anforderung an eine umfassende themenspezifische Kryptographierichtlinie soll sicherstellen, dass der Einsatz von Verschlüsselung nicht beliebig oder punktuell erfolgt, sondern systematisch auf die Asset-Kritikalität (siehe 5.3) abgestimmt ist. Kryptographische Maßnahmen müssen gezielt dort eingesetzt werden, wo sie aus Risiko- und Klassifikationssicht erforderlich sind. KMUs müssen hierfür klare Standards für Algorithmen, Protokolle und Schlüssellängen definieren und gleichzeitig Prozesse etablieren, die den gesamten Lebenszyklus von Schlüsseln, von der Generierung über die Nutzung bis hin zur sicheren Löschung, steuern und dokumentieren. Zusätzlich fordert die Verordnung, dass Unternehmen kryptographische Entwicklungen aktiv beobachten und ihre Verfahren bei Bedarf an neue Bedrohungen anpassen.

Umsetzung im NIS2-ISMS-Framework: KMUs sollten hier mit der Erstellung einer kompakten themenspezifischen Richtlinie zum Thema „Kryptographie“ beginnen. Als Basis zur Definition der Vorgaben kann hierfür von KMUs die technische Richtlinie „TR-021-02-1“ von BSI verwendet werden. Im Zuge dieser Arbeit wurde eine Kryptographie-Richtlinienvorlage erstellt, welche von KMUs als Basis verwendet werden kann, und an die eigenen Bedürfnisse angepasst werden muss. Zugehörige Verfahren enthalten insbesondere kryptographische Vorgaben zu den folgenden Themen:

- **Algorithmus- und Protokoll-Baseline:** Auf Basis der Kritikalität der Assets (siehe Kapitel 5.3.1) werden passende Baselines für die Auswahl kryptographischer Verfahren festgelegt.
  - **Datenübertragung (Daten in Transit):** Für KMUs ist es entscheidend, bei der Übertragung sensibler Daten auf anerkannte Sicherheitsstandards zu setzen. Das BSI empfiehlt, ausschließlich Transport Layer Security („TLS“) ab Version 1.2 zu verwenden. Um zusätzliche Angriffe zu verhindern, sollte HTTP Strict Transport Security („HSTS“) genutzt werden. Für die Praxis bedeutet dies: KMUs können sich darauf verlassen, dass moderne Standardkonfigurationen (z.B. TLS 1.3 bei Cloud-Diensten) bereits ein sehr hohes Schutzniveau bieten. [41, p. 18]
  - **Datenspeicherung (Daten at Rest):** Zur Absicherung ruhender Daten rät das BSI, symmetrische Verschlüsselungsverfahren wie AES mit einer Schlüssellänge von 256 Bit einzusetzen. [41, p. 42] Besonders zu empfehlen ist der Galois/Counter Mode („GCM“), der neben der Verschlüsselung auch die Integrität der Daten absichert. Die Festplattenverschlüsselung auf Servern oder Endgeräten sollte mit bewährten Technologien wie BitLocker oder LUKS erfolgen. Datenbanken sollten, falls möglich, „Transparent Data Encryption“ („TDE“) verwenden.
  - **Schlüsselalgorithmen:** Zur Authentifizierung und Absicherung sensibler Daten empfiehlt das BSI klassische asymmetrische Verfahren wie RSA mit mindestens 2048 Bit Schlüssellänge oder moderne ECC-Verfahren mit 250 Bit (z.B. P-256). [41, pp. 32-34] Für KMUs ist es pragmatisch, sich an den Empfehlungen der jeweiligen Cloud- oder Softwareanbieter zu orientieren, da diese in der Regel konforme Zertifikate und Schlüssel einsetzen.
- **Schlüsselmanagement:** Ein wirksames Schlüsselmanagement ist für KMUs essenziell, insbesondere wenn sensible Unternehmensdaten oder personenbezogene Informationen verarbeitet werden. Das BSI empfiehlt, kryptographische Schlüssel entweder in professionellen Cloud Key Management Services („KMS“) oder in Hardware Security Modules („HSM“) sicher zu erzeugen und zu verwalten. [41, p. 79]
  - Wesentliche Anforderungen sind:
    - **Keine Speicherung im Klartext:** Schlüssel dürfen nicht offen auf Servern oder Arbeitsplät-

zen abgelegt werden.

* **Kontrollierte Verteilung:** Zugriff auf Schlüssel muss rollenbasiert beschränkt und regelmäßig überprüft werden.
* **Regelmäßige Rotation:** Schlüssel sollten spätestens alle zwölf Monate erneuert werden oder sofort bei Verdacht auf eine Kompromittierung. [41, p. 79]

– Darüber hinaus empfiehlt das BSI für die Verwaltung asymmetrischer Schlüssel den Einsatz einer vertrauenswürdigen Public Key Infrastruktur („PKI“), um Zertifikate sicher auszustellen, zu verteilen und deren Gültigkeit zu überwachen. [41, p. 38] Zur Erhöhung der Verfügbarkeit und Sicherheit sind Sicherheitskopien kryptographischer Schlüssel verschlüsselt aufzubewahren, damit eine Wiederherstellung bei Verlust oder Beschädigung möglich bleibt. [41, p. 79] Im Falle einer Kompromittierung müssen Prozesse zur sofortigen Sperrung, Erneuerung sowie Protokollierung aller Maßnahmen etabliert sein. Weiterhin sind für alle Schlüssel klare Aktivierungs- und Deaktivierungszeiträume festzulegen, sodass diese ausschließlich während ihrer vorgesehenen Nutzungsdauer gültig bleiben. [41, p. 79]

- **Kryptographische Agilität:** Im Hinblick auf die zukünftige Entwicklung von Bedrohungen, insbesondere durch Quantencomputer, fordert das BSI die Fähigkeit, kryptographische Verfahren flexibel auszutauschen. [41, pp. 30-31] Für KMUs bedeutet dies jedoch nicht, dass sofort Post-Quantum-Verfahren eingeführt werden müssen. Vielmehr sollten Systeme und Verträge so gestaltet sein, dass ein Wechsel auf neue, sichere Algorithmen ohne größere Systemabbrüche möglich ist.
  – Empfohlene praktische Schritte:
    * Nutzung standardisierter Schnittstellen (z.B. PKCS#11 für Schlüsselzugriff)
    * Auswahl von Software- und Cloud-Lösungen, die aktiv an Post-Quantum-Initiativen teilnehmen (z.B. TLS-Anbieter, die PQC-Optionen anbieten). [41, pp. 30-31]
    * Regelmäßige Überprüfung der eingesetzten Algorithmen im Rahmen der jährlichen Überprüfungen.

Im Rahmen einer jährlichen sowie anlassbezogenen Prüfung muss die Richtlinie und die dazugehörigen Prozesse seitens der IT-Abteilung unter Initiierung und Kontrolle des:der ISB überprüft werden. Die Ergebnisse fließen in die Anpassung sowie kontinuierliche Verbesserung ein.

5.11 Umgang mit Cybersicherheitsvorfällen

Ein effektiver und strukturierter Umgang mit Cybersicherheitsvorfällen ist essenziell, um Schäden für Unternehmen zu begrenzen und regulatorische Anforderungen zu erfüllen. Im Mittelpunkt dieses Themenbereichs steht die Etablierung eines ganzheitlichen Vorfallmanagementprozesses, von der Erkennung über die Klassifikation und Reaktion bis hin zur Nachbereitung. Die NIS2-Durchführungsverordnung macht deutlich, dass Vorfälle nicht isoliert betrachtet werden dürfen, sondern eingebettet in bestehende Notfall- und Krisenprozesse behandelt werden müssen. Für KMUs bedeutet dies, mit begrenzten Ressourcen ein praxistaugliches System zu schaffen, das klare Rollen, nachvollziehbare Abläufe und eine belastbare Dokumentation sicherstellt. Das Kapitel zeigt auf, wie diese Anforderungen schrittweise in einem praxisnahen ISMS für KMUs umgesetzt werden können.

5.11.1 Richtlinie zum Umgang mit Cybersicherheitsvorfällen

Mapping - NIS2 Durchführungsverordnung (Punkt 3.1.): Abschnitt 3.1 verpflichtet Einrichtungen, ein formelles Konzept für die Behandlung von Vorfällen zu etablieren, die die Rollen, Verantwortlichkeiten und Verfahren für das rechtzeitige Erkennen, Analysieren, Eindämmen, Beheben, Dokumentieren und Melden von Sicherheitsvorfällen klar definiert (3.1.1). Diese Richtlinie muss kohärent mit dem Notfall- und Wiederherstellungsplan des Unternehmens abgestimmt sein (3.1.2). Konkret fordert die Verordnung (3.1.2):

- Eine verbindliche Kategorisierungsmatrix zur Priorisierung von Vorfällen (a),
- Kommunikations- und Eskalationspläne für interne und externe Meldungen (b),
- Eindeutige Zuweisung von Verantwortlichkeiten an geschulte Mitarbeitende (c),
- Standardisierte Vorlagen und Hilfsmittel zur strukturierten Vorfallbearbeitung (d).

Alle festgelegten Rollen, Verantwortlichkeiten und Verfahren sind regelmäßig zu testen, zu überprüfen und bei Bedarf zu aktualisieren, insbesondere nach erheblichen Vorfällen oder wesentlichen Änderungen der Rahmenbedingungen (3.1.3).

Interpretation der Anforderungen: Die Vorgabe betont, dass die Behandlung von Sicherheitsvorfällen nicht situativ oder improvisiert erfolgen darf, sondern als definierter, dokumentierter und strukturierter Prozess im Unternehmen verankert sein muss. Ziel ist es, bei Auftreten eines Vorfalls schnell und geordnet reagieren zu können, um Schäden zu minimieren und regulatorische Meldepflichten fristgerecht zu erfüllen. KMUs müssen im Voraus klare Prozesse und Verantwortlichkeiten festlegen, wer Vorfälle erkennt, wer sie

analysiert, wer sie eindämmt und wer über den weiteren Umgang entscheidet. Besonders wichtig ist dabei die Abstimmung mit bestehenden Notfall- und Wiederherstellungsplänen, um eine nahtlose Reaktion sicherzustellen. Die Einführung standardisierter Dokumente wie Playbooks und Eskalationspläne ermöglicht eine transparente und geordnete Vorfallbearbeitung, während regelmäßige Tests sicherstellen, dass Prozess kontinuierlich verbessert und an neue Bedrohungslagen angepasst wird.

Umsetzung im NIS2-ISMS-Framework: Zu Beginn müssen KMUs eine kompakte themenspezifische Richtline zum Thema Behandlung von Sicherheitsvorfällen erstellen. Hierfür muss vorab festgelegt werden, wo die Verantwortlichkeiten innerhalb des Managements von Sicherheitsvorfällen liegen. Für KMUs empfiehlt es sich hierbei, eine schlanke, klar strukturierte Rollenverteilung zu wählen, welche sich an den tatsächlichen personellen und organisatorischen Gegebenheiten orientiert. Im Regelfall sollte der:die ISB für die Erstellung, Pflege und Steuerung der Richtlinie verantwortlich sein. Die IT-Abteilung übernimmt hierbei die operative Rolle in der technischen Erkennung, Bearbeitung und Wiederherstellung, während die oberste Leitungsebene für Eskalationsentscheidungen bei Vorfällen mit hoher Kritikalität zuständig ist. Darüber hinaus sollten auch die Fachabteilungen eingebunden werden. Insbesondere im Hinblick auf die zeitnahe Meldung verdächtiger Vorkommnisse sowie die Unterstützung bei Recovery-Maßnahmen und der internen Kommunikation.

Im Rahmen dieser Arbeit wurde eine Richtlinien-Vorlage für die Behandlung von Sicherheitsvorfällen erstellt, welche von KMUs als Basis verwendet werden kann, und auf die eigenen Bedürfnisse angepasst werden muss. Die Vorlage beschreibt ein strukturiertes und praxisorientiertes Vorgehen für den Umgang mit Sicherheitsvorfällen in einem KMU, einschließlich der Erkennung, Bewertung, Eindämmung, Analyse, Meldung, Wiederherstellung und Nachbearbeitung. Zudem legt sie klare Verantwortlichkeiten, Meldewege, Eskalationsstufen und Dokumentationspflichten fest und stellt sicher, dass Sicherheitsvorfälle nachvollziehbar, rechtskonform und effizient bearbeitet werden. Die inhaltlichen Punkte der Richtlinie sowie die genauen operativen Schritte zur Behandlung von Sicherheitsvorfällen (Überwachung und Protokollierung, Meldung, Klassifikation, Reaktion sowie Lessons Learned und Testungen) werden in den folgenden Kapiteln näher thematisiert.

5.11.2 Überwachung und Protokollierung

Mapping - NIS2 Durchführungsverordnung (Punkt 3.2.): Abschnitt 3.2 verpflichtet Einrichtungen dazu, Verfahren und technische Lösungen zur Überwachung und Protokollierung aller sicherheitsrelevanten

Aktivitäten innerhalb der Netzwerk- und Informationssysteme zu etablieren (3.2.1). Ziel ist es, sicherheitsrelevante Ereignisse frühzeitig zu erkennen und geeignete Reaktionen einzuleiten. Konkret fordert die Verordnung (3.2.2-3.2.7):

- Automatisierte und kontinuierliche bzw. regelmäßig durchgeführte Überwachungsmaßnahmen, die möglichst fehlerfrei arbeiten (3.2.2),
- Pflege eines Asset-Verzeichnisses mit definierter Logging-Priorität je nach Risikoanalyse (3.2.3),
- Protokollierung sicherheitskritischer Ereignisse, wie z.B. Logins, Konfigurationsänderungen, Datenzugriffe oder Netzwerkverkehr (3.2.3 a-l),
- Regelmäßige Prüfung von Logdaten auf Auffälligkeiten und Definition von Schwellwerten mit automatisierter Alarmierung (3.2.4),
- Sicherung, Integritätsschutz und zeitlich definierte Aufbewahrung der Logdaten (3.2.5),
- Zeitsynchronisation aller Systeme sowie redundante Auslegung der Logging-Infrastruktur (3.2.6),
- Regelmäßige Überprüfung und Aktualisierung der Logging-Verfahren sowie der Asset-Logliste (3.2.7).

Interpretation der Anforderungen: Logging und Monitoring bilden die operative Grundlage für die Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen. Ein zentraler Punkt ist die Qualität der Logs, zwar muss nicht alles geloggt werden, jedoch muss das Relevante verfügbar, vollständig und fälschungssicher sein. Zudem muss gewährleistet sein, dass bei Abweichungen (z.B. ungewöhnlichem Loginverhalten) automatisch reagiert wird. Dies erfordert keine teure SIEM-Lösung und es kann auch mittels einfacher Syslog-Server, gut definierten Regeln und Open-Source-Werkzeugen ein belastbares Logging und Monitoring aufgebaut werden. Für die spätere forensische Auswertung, aber auch zur Einhaltung regulatorischer Fristen (z.B. Nachweispflichten bei Behördenmeldungen), ist es essenziell, dass Logs nicht nur erzeugt, sondern auch manipulationssicher gespeichert, regelmäßig geprüft und zentral ausgewertet werden.

Umsetzung im NIS2-ISMS-Framework: Als Grundvoraussetzung sollten alle sicherheitsrelevanten Assets in einem Inventar kategorisiert (siehe Kapitel 5.4.1) und mit einer Kritikalität eingestuft sein (siehe Kapitel 5.3.1) Auf Basis davon muss im nächsten Schritt festgelegt werden, welche Systeme mindestens überwacht werden müssen und was genau geloggt werden muss. Für die Auswahl der zu überwachenden Systeme sollten zuerst die Assets mit höherer Kritikalität gemäß BIA priorisiert werden. Je Asset-Klasse wird im nächsten Schritt definiert, welche Ereignisse mindestens protokolliert werden müssen. Als Basis kann hierfür beispielsweise das Dokument „Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen“ [72] verwendet werden. Durch die detaillierte Aufschlüsselung des Mindeststandards nach

IT-System-Sicht und Netz-Sicht sowie klar formulierte Anforderungen gibt das Dokument konkrete Anhaltspunkte, welche Ereignisse je Systemart mindestens protokolliert werden sollten. Dazu zählen Anmeldeversuche, Konfigurationsänderungen, Netzwerkkommunikation oder Systemstarts. Im nächsten Schritt werden relevante Ereigniskategorien definiert, welche festlegen welche Ereignisse prinzipiell geloggt werden müssen. In der folgenden Tabelle 5.9 ist dies beispielhaft dargestellt:

Ereigniskategorie	**Beispiele**
Authentifizierung	Anmeldung, fehlgeschlagene Anmeldung, Passwortänderung, etc.
Benutzer:innen- und Rollenänderungen	Erstellung, Löschung und Rechtänderung von Benutzer:innen, etc. (wie in Kapitel 5.8.2 gefordert)
Zugriffe	(privilegierte) Zugriffe auf Systeme und Anwendungen, physischer Zugang, etc.
Systemereignisse	Start, Stopp und Neustart von Systemen und Protokollen, Aktivitäten von Verwaltungskonten, Nutzung von Systemressourcen und deren Leistungen, etc.
Sicherheitsereignisse	Malwarefund, Policy-Verletzung, IDS/IPS-Alarm, etc.
Konfigurationsänderungen	Firewall-Regeländerungen, Update-Installation, Backup-Änderungen, etc.
Netzwerkkommunikation	Ausgehender und eingehender Netzwerkverkehr, Verbindungen über VPN, neue externe Session, etc.

Tabelle 5.9: Beispielhafte Ereigniskategorien zum Loggen

Bei Assets mit hoher Kritikalität ist es empfehlenswert alle definierten Ereigniskategorien zu protokollieren. Zudem sollte eine Aufbewahrungsdauer der Logs je nach Asset-Kritikalität festgelegt werden. Eine Broschüre des BMI zum Thema Log-Daten als Grundlage für Incident Response empfiehlt hierbei standardmäßig drei Monate, wobei bei kritischeren Assets eine Aufbewahrungsdauer von 6 Monaten oder mehr eingehalten werden sollte. [73]

Für eine gute Übersicht sollten die einzelnen Aspekte zusammengefasst in einer Logging-Matrix strukturiert und dargestellt werden. Eine beispielhafte Matrix ist in der folgenden Tabelle 5.10 dargestellt:

Asset-Klasse	**Asset-Kritikalität**	**Ereignisse protokollieren**	**Aufbewahrungsdauer**
Firewall	Hoch	Alle Ereigniskategorien	12 Monate
Server (z.B. Active Directory)	Hoch	Alle Ereigniskategorien	12 Monate
Clients	Mittel	Authentifizierung, Zugriffe, Systemereignisse, Sicherheitsereignisse	3 Monate

Tabelle 5.10: Beispielhafte Logging-Matrix

Um die Integrität und Verfügbarkeit der erfassten Logdaten sicherzustellen, müssen alle Logdateien manipulationssicher gespeichert und gegen unbefugte Zugriffe geschützt werden. Der Zugriff auf zentrale Logserver sowie auf gespeicherte Logdaten ist ausschließlich autorisierten Administrator:innen vorbehalten (siehe Kapitel 5.8). Eine weitere technische Grundvoraussetzung für eine konsistente und verwertbare Loganalyse ist die zentrale Zeitsynchronisation aller Systeme. Sämtliche Clients, Server und Netzwerkgeräte müssen eine einheitliche Zeitquelle (z.B. NTP-Server) verwenden, um eine korrekte zeitliche Korrelation von Ereignissen aus verschiedenen Systemen zu gewährleisten. Dies ist insbesondere bei der forensischen Auswertung und der Rekonstruktion von Vorfällen (als Basis für die schnelle Vorfallserkennung sowie forensische Aufklärung; siehe Kapitel 5.11.5) von entscheidender Bedeutung. In der praktischen Umsetzung empfiehlt es sich hierzu einen zentralen NTP-Server („Network Time Protocol“) innerhalb der Netzwerkinfrastruktur zu definieren. Dies kann beispielsweise ein bestehender Domain Controller sein, welcher sich mit vertrauenswürdigen externen Zeitquellen synchronisiert (z.B. „time.cloudflare.com“) und diese Zeit an alle internen Systeme verteilt. Hierzu können Windows-Clients mittels GPO und Linux-Systeme sowie Netzwerkgeräte mithilfe der Systemkonfiguration auf die interne Zeitquelle eingestellt werden. [74]

Im Anschluss stellt sich die Frage, wie die erfassten Log-Daten in der Praxis zentral gesammelt, überwacht und ausgewertet werden können, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen. Für KMUs empfiehlt sich hierbei ein pragmatischer Ansatz, der eine zentrale Sammlung und Überwachung der wichtigsten Logs ermöglicht, ohne unverhältnismäßig hohe Investitionen oder komplexe Systemarchitekturen zu erfordern. Ziel hierbei ist es, sicherheitsrelevante Aktivitäten über alle kritischen Systeme hinweg nachvollziehbar zu dokumentieren, Anomalien zu erkennen und die Daten manipulationssicher für einen definierten

Zeitraum aufzubewahren.

Als Einstieg bietet sich die Implementierung eines zentralen Logservers an, auf dem alle sicherheitsrelevanten Systeme ihre Ereignisdaten konsolidiert ablegen. Dabei können beispielsweise Windows-Server und -Clients über „Windows Event Forwarding“ ihre Logs zentral bereitstellen, während Netzwerkgeräte und Firewalls Syslog-Protokolle an einen dedizierten Syslog-Server senden. Statt eine separate Windows-Event-Forwarding-Infrastruktur aufzubauen und einen dezidierten Syslog-Server zu betreiben, empfiehlt sich eine direkte Sammlung aller Logs auf einem universellen Syslog-Server wie beispielsweise „rsyslog“ auf Basis von Linux-Systemen. Mithilfe von „NXLog Community Edition“ oder „Snare“ auf den Windows-Clients und -Servern können Windows-Eventlogs in Syslog-Format konvertiert werden und direkt an den zentralen Syslog-Server geschickt werden. [75] Ebenso sind Netzwerkgeräte und Firewalls in der Lage die Syslogs direkt an den zentralen Server zu senden. Um das Erkennen von Anomalien in Logs automatisiert sicherzustellen, können beispielsweise mit „rsyslog“ einfache Regeln mit Schwellwerten definiert werden, welche beim Erkennen bestimmter Log-Ereignisse automatisierte Aktionen auslösen können (z.B. Alarmierung durch das Senden von E-Mails an die IT-Abteilung). [76] Alternativ gibt es auch empfehlenswerte Tool-Lösungen, welche all diese Funktionalitäten in einem vereinen. Diese sollten von KMUs in Betracht gezogen werden. Die Lösung „Wazuh“ ist als kostenlose Open-Source-Lösung beispielsweise mit deutlich mehr Funktionalitäten als reine Syslog-Server ausgestattet und bieten dadurch einen großen Vorteil für Unternehmen. Neben der klassischen zentralen Sammlung von Log-Daten kann die Lösung auch als Analyse- und Security-Monitoring-Plattform eingesetzt werden, die Log-Daten auswertet, korreliert, alarmiert und aktive Gegenmaßnahmen einleitet. [77] Dabei sammeln die „Wazuh-Agents“ auf den zu überwachenden Systemen (Windows-Clients, Servern, etc.) sicherheitsrelevante Ereignisse, der „Wazuh-Manager“ analysiert diese regelbasiert, und das Dashboard stellt die Ergebnisse übersichtlich dar. Die Lösung kann sowohl On-premise auf eigenen Servern als auch in der Cloud (kostenpflichtig) betrieben werden. Zusätzlich können auch sicherheitsrelevante Ereignisse aus Anti-Malware-Lösungen (siehe Kapitel 5.9.10) wie „Windows Microsoft Defender“ und „ClamAV“ in die zentrale Lösung zur Sammlung, Auswertung und Alarmierung integriert werden. [78], [79]

Im Rahmen einer jährlichen und anlassbezogenen Überprüfung muss von der IT-Abteilung unter Initiierung und Koordination des:der ISB das Thema Protokollierung und Überwachung inklusive der Prozesse kontrolliert werden. Die Ergebnisse fließen in die Anpassung sowie kontinuierliche Verbesserung ein.

5.11.3 Meldung von Ereignissen

Mapping - NIS2 Durchführungsverordnung (Punkt 3.3.): Abschnitt 3.3 der Verordnung verpflichtet Einrichtungen, ein einfaches und zugängliches Verfahren zur Meldung sicherheitsrelevanter Ereignisse bereitzustellen, welches es Mitarbeitenden, Lieferant:innen und (soweit relevant) Kund:innen ermöglicht, verdächtige Ereignisse unkompliziert zu melden (3.3.1). Konkret fordert die Verordnung (3.3.2):

- Eine transparente Kommunikation des Meldeverfahrens an interne und externe Stakeholder,
- Eine regelmäßige Schulung der Mitarbeitenden, um die Nutzung des Meldewegs sicherzustellen.

Das eingerichtete Meldesystem soll die frühzeitige Erkennung von sicherheitsrelevanten Vorfällen unterstützen und als integraler Bestandteil des Vorfallsmanagement-Prozesses etabliert sein.

Interpretation der Anforderungen: Das Ziel dieser Anforderung ist es, einen Meldeweg bereitzustellen, der von allen Mitarbeitenden sowie anderen relevanten Stakeholdern ohne große Hürden genutzt werden kann und im Notfall auch unter Stressbedingungen funktioniert. Gleichzeitig müssen die Meldekanäle aktiv durch Awareness-Schulungen und -Maßnahmen bekanntgemacht und durch regelmäßige Sensibilisierung gefestigt werden.

Umsetzung im NIS2-ISMS-Framework: Zu Beginn sollten KMUs einen unkomplizierten Meldekanal festlegen, über welche Vorfalls-Meldungen an eine zentrale Stelle geschickt werden. In der Praxis kann hierfür eine E-Mail-Adresse (z.B. „vorfall@kmu.at“) oder ein Online-Formular im Intranet oder einer internen Seite sein. Bei Online-Formularen sollte beachtet werden, diese mit den wichtigsten Feldern zu konfigurieren, beispielsweise: [80]

- Was ist passiert?
- Wann wurde es bemerkt?
- Wer meldet?
- Welche Systeme könnten betroffen sein?
- Sind sensible Daten (z.B. personenbezogene Daten) betroffen? Welche genau?

Dies stellt sicher, dass alle nötigen Informationen direkt bereitgestellt werden können. Auch eine telefonische Notfall-Hotline, welche innerhalb der Geschäftszeiten beispielsweise direkt an die IT-Abteilung weiterleitet, falls Systeme ausfallen, ist für KMUs empfehlenswert. Damit der eingerichtete Meldekanal auch effektiv funktioniert, muss dieser an alle relevanten Personen und Stakeholder kommuniziert werden. Daher

müssen insbesondere:

- **Mitarbeitende** über die verfügbaren Meldekanäle informiert werden. Dies kann im Zuge des Onboardings, der Schulungen (siehe Kapitel 5.6), einer Informations-Mail sowie eines Eintrags im Intranet erfolgen.
- **Lieferant:innen und Dienstleister:innen** spätestens bei Vertragsabschluss oder im Onboarding über die Meldepflicht und den Meldeweg informiert werden (siehe Kapitel 5.7.1).
- **Kund:innen** (nur wenn sicherheitsrelevant) beispielsweise auf der Unternehmenswebseite einen klaren Hinweis erhalten, wie sie sicherheitsrelevante Beobachtungen melden können.

Um sicherzustellen, dass Meldungen qualitativ hochwertig sind und echte Sicherheitsvorfälle nicht übersehen werden, sollen Mitarbeitende in den regelmäßigen Awareness-Schulungen und -Maßnahmen (siehe Kapitel 5.6) zumindest über folgende Themen aufgeklärt werden:

- Woran erkenne ich einen sicherheitsrelevanten Vorfall? (z.B. verdächtige E-Mails, ungewöhnliches Verhalten von Systemen, Verlust von Notebook, etc.)
- Wie melde ich richtig?
- Warum ist eine schnelle Meldung wichtig?

5.11.4 Erhebung und Klassifikation von Ereignissen

Mapping - NIS2 Durchführungsverordnung (Punkt 3.4.): Abschnitt 3.4 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen zur systematischen Bewertung sicherheitsrelevanter Ereignisse mit dem Ziel, deren Einstufung als Sicherheitsvorfall sowie deren Art und Schweregrad eindeutig festzustellen (3.4.1). Konkret müssen folgende Anforderungen umgesetzt werden (3.4.2):

- Die Bewertung muss auf vorab definierten, dokumentierten Kriterien basieren und eine Priorisierung der Maßnahmen (Triage) ermöglichen (3.4.2 a),
- Quartalsweise Analyse, ob bestimmte Vorfallmuster wiederkehren oder systemische Schwächen bestehen (3.4.2 b),
- Sichtung und Auswertung relevanter Logdaten zur fundierten Beurteilung von Ereignissen (3.4.2 c),
- Einführung eines standardisierten Verfahrens zur Korrelation und Analyse mehrerer Logquellen (3.4.2 d),
- Möglichkeit zur nachträglichen Neubewertung und Re-Klassifikation von Vorfällen bei neuen Erkenntnissen oder veränderten Lagebildern (3.4.2 e).

Diese Prozesse dienen als Grundlage für eine fundierte Eskalationsentscheidung (z.B. Vorfall, Notfall, Krise) und sind eng mit dem Behandeln von Sicherheitsvorfällen, dem BCM sowie der internen Risikosteuerung zu verzahnen.

Interpretation der Anforderungen: Die Anforderungen aus Abschnitt 3.4 betonen, dass eine strukturierte Bewertung und Klassifikation sicherheitsrelevanter Ereignisse kein Selbstzweck, sondern Grundlage für jede angemessene Reaktion ist. Gerade für KMUs, welche über keine dedizierte SOC-Struktur („Security Operation Center“) verfügen, ist es entscheidend, durch vordefinierte Kriterien und einfache Bewertungsmethoden Klarheit zu schaffen: Was ist nur auffällig, was ist ein Vorfall und wann sprechen wir von einem Notfall oder gar einer Krise? Ein übersichtliches Klassifikationsschema hilft nicht nur bei der Priorisierung und Meldeentscheidung, sondern schafft auch Transparenz gegenüber Behörden und der obersten Leitungsebene. Entscheidend ist, dass KMUs keine komplexen Bewertungssysteme einführen, sondern einfache, nachvollziehbare Prozesse etablieren, die regelmäßig überprüft und angepasst werden.

Umsetzung im NIS2-ISMS-Framework: Sicherheitsrelevante Vorfälle können über mehrere Quellen (z.B. E-Mail, Ticketsystem, Überwachungssystem) an die definierte verantwortliche Stelle (z.B. IT-Abteilung) gemeldet werden. Vorab ist zu klären, welche grundsätzlichen Kategorien und Definitionen von Schadensereignissen existieren. Das BSI definiert im Rahmen des Standards 200-4 drei Eskalationsstufen (Sicherheitsvorfall, Notfall und Krise), zwischen denen unterschieden werden muss:

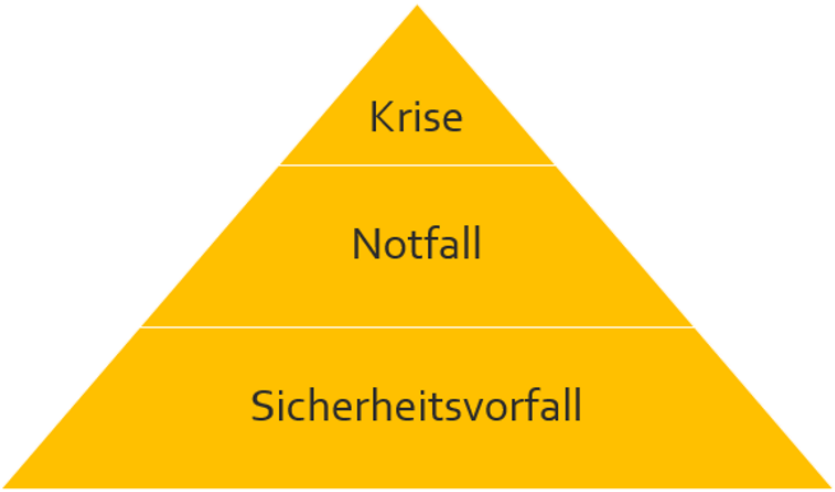

Abbildung 5.3: Eskalationsstufen Sicherheitsvorfall - Notfall - Krise

- **Sicherheitsvorfall:** Ein Sicherheitsvorfall ist ein Ereignis mit sicherheitsrelevanter Bedeutung, wel-

cher eine Abweichung vom normalen Betrieb darstellt und potenziell oder tatsächlich Auswirkungen auf die Vertraulichkeit, Integrität, Authentizität und/oder Verfügbarkeit von Assets hat. Zudem müssen Sicherheitsvorfälle nicht zwangsläufig einen Schaden verursachen, aber sind ein Indikator für eine Bedrohung oder eine Schwachstelle.
  - **Beispiel:** Erkennung von Malware oder mehrfach fehlgeschlagene Login-Versuche.
- **Notfall:** Ein Notfall ist, wenn ein schwerwiegendes Ereignis oder eine Störung eintritt, wodurch die Fortführung kritischer Geschäftsprozesse und Dienstleistungen erheblich beeinträchtigt sind und eine koordinierte Reaktion gemäß Business Continuity Management (siehe Kapitel 5.12) notwendig wird.
  - **Beispiel:** Ausfall eines Rechenzentrums oder großflächiger Ransomware-Befall.
- Krise: Eine Krise ist ein komplexer, oft eskalierter Notfall, welcher mehrere Geschäftsbereiche betrifft oder organisationsweite Auswirkungen hat. Außerdem stellt eine Krise eine erhebliche Gefährdung für die Assets, Reputation oder die Existenz dar, wodurch eine strategische Entscheidung auf oberster Ebene (oberste Leitungsebene) erfordert ist. [81, pp. 20-21]
  - **Beispiel:** Öffentlich gewordener Datenabfluss mit regulatorischen und reputativen Folgen.

Um Sicherheitsvorfälle vor der Eskalation zum Notfall weiter unterteilen und für die Triage priorisieren zu können, empfiehlt es sich, standardisierte Kategorisierungen nach Schweregrad einzuführen. Dies kann mithilfe einer kompakten Kategorisierungsmatrix anhand der Schutzziele sowie der Auswertung und Korrelation vorhandener Logs (siehe Kapitel 5.11.2) durchgeführt werden. Zur strukturierten Bewertung von Sicherheitsvorfällen wurde eine praxistaugliche Matrix im Rahmen dieser Arbeit (Tabelle 5.11) entwickelt, welche anhand von sechs zentralen Bewertungskriterien (z.B. Systemauswirkung, Datenbezug, Außenwirkung) eine Punktevergabe ermöglicht.

Kriterium	**Gering (1 Punkt)**	**Mittel (2 Punkte)**	**Hoch (3 Punkte)**
Systemauswirkung	Kein Systemausfall	Einzelnes System gestört	Mehrere/kritische Systeme ausfallend
Datenschutzrelevanz	Keine Daten betroffen	Verdacht auf Datenverlust	Sensible Daten tatsächlich kompromittiert
Geschäftsprozess	Kein Einfluss	Eingeschränkte Abläufe	Kritische Prozesse unterbrochen
Betroffene Bereiche	Ein Arbeitsplatz / System	Einzelner Fachbereich	Mehrere Abteilungen / Standorte betroffen

Kriterium	Gering (1 Punkt)	Mittel (2 Punkte)	Hoch (3 Punkte)
Außenwirkung	Intern gehalten	Kund:innen betroffen	Öffentlichkeit / Medien involviert
Angriffscharakter	Kein aktiver Angriff (z.B. Spam-Mail)	Technische Auffälligkeit (z.B. Malware, Phishing)	Aktive Bedrohung (z.B. Ransomware, externes Einwirken)

Tabelle 5.11: Bewertungskriterien zur Klassifikation von Sicherheitsvorfällen

Die daraus resultierende Punktesumme führt zur Zuordnung in fünf definierte Kritikalitätsstufen (Tabelle 5.12), welche wiederum konkrete Eskalations- und Meldewege auslösen. Diese standardisierte Einstufung erleichtert KMUs eine konsistente, nachvollziehbare und regelbasierte Entscheidungsfindung im Sicherheitsvorfallprozess.

Punktesumme (von 6-18)	Klassifikation	Eskalation an	Hinweis
6-7 Punkte	**Stufe 1 - Geringer Vorfall**	IT-Abteilung	Beobachten, dokumentieren
8-10 Punkte	**Stufe 2 - Erheblicher Vorfall**	ISB und IT-Abteilung	Maßnahmen starten, Meldepflicht prüfen
11-13 Punkte	**Stufe 3 - Kritischer Vorfall / Notfall**	Oberste Leitungsebene, ISB	Sofortmaßnahmen, Behördenmeldung vorbereiten
14-18 Punkte	Stufe 4 - Krise	Oberste Leitungsebene	Externe Kommunikation, strategische Reaktion nötig

Tabelle 5.12: Zuordnung der Kritikalität bei Sicherheitsvorfällen

Zusätzlich zur Einzelfallbewertung muss quartalsweise eine Analyse erfolgen, ob sicherheitsrelevante Vorfälle systematisch wiederkehren oder sich häufen. Hierzu kann ein einfaches Sicherheitsvorfallregister (z.B. in Excel-Format) verwendet werden, in welchem Datum, Ursache, betroffene Systeme und Klassifikation aller Sicherheitsvorfälle dokumentiert werden. Der:die ISB sollte mithilfe der IT-Abteilung dieses Register regelmäßig auswerten, um Muster zu erkennen (z.B. wiederholte Phishing-Erfolge, immer wieder betroffe-

ne Dienste) und daraus gezielte Präventionsmaßnahmen abzuleiten. Im Rahmen dieser Arbeit wurde eine Vorlage für Sicherheitsvorfallsregister erstellt, welche von KMUs als Basis verwendet werden kann, und auf die eigenen Bedürfnisse angepasst werden muss.

Wird im Verlauf der Analyse (z.B. durch forensische Maßnahmen oder nachträgliche Logauswertung) deutlich, dass ein Sicherheitsvorfall schwerwiegender war als zunächst angenommen, muss eine Re-Klassifikation erfolgen. Der geänderte Status (z.B. von „Stufe 2 - Erheblicher Vorfall“ auf „Stufe 3 - Kritischer Vorfall / Notfall“) ist beispielsweise im Sicherheitsvorfallsregister zu dokumentieren und die entsprechende Eskalation (z.B. Behördenmeldung bzgl. NIS2) nachzuholen. Auch umgekehrt ist eine Herabstufung möglich, wenn sich erste Hinweise nicht bestätigen. Im folgenden Kapitel wird dann die Reaktion auf Sicherheitsvorfälle thematisiert.

5.11.5 Reaktion auf Cybersicherheitsvorfälle

Mapping - NIS2 Durchführungsverordnung (Punkt 3.5.): Abschnitt 3.5 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen dazu, auf Sicherheitsvorfälle zeitnah und auf Basis dokumentierter Verfahren zu reagieren (3.5.1). Die Incident-Response-Prozesse müssen dabei mindestens drei zentrale Phasen abdecken: Eindämmung der Auswirkungen, vollständige Beseitigung der Ursache sowie gegebenenfalls die Wiederherstellung betroffener Systeme (3.5.2). Zudem müssen Kommunikationswege mit externen Stellen wie CSIRTs oder Behörden sowie für die interne Koordination klar geregelt sein (3.5.3). Alle Reaktionsmaßnahmen sind zu protokollieren und beweissicher zu dokumentieren (3.5.4). Die Verfahren sind regelmäßig zu testen, um ihre Wirksamkeit sicherzustellen (3.5.5).

Interpretation der Anforderungen: Ein dokumentierter und eingeübter Incident-Response-Prozess ist das Rückgrat jeder Sicherheitsorganisation, insbesondere in KMUs. Die Anforderungen verdeutlichen, dass bei einem Vorfall nicht improvisiert, sondern nach einem klaren Ablauf reagiert werden muss. Dabei sind die Eindämmung (Containment) und Beseitigung (Eradication) entscheidend und müssen sofort greifen, um Schäden zu minimieren. Die Wiederherstellung (Recovery) darf erst nach vollständiger Ursachenbeseitigung erfolgen. Für KMUs heißt es, dass einfache, klar beschriebene Prozesse und klar definierte Kommunikationsketten (intern sowie extern) unerlässlich sind. Die Dokumentation und Nachvollziehbarkeit der Maßnahmen schützen dabei nicht nur technisch, sondern sind auch regulatorisch und haftungsrechtlich essenziell.

Umsetzung im NIS2-ISMS-Framework: Um angemessen und zeitnah auf Sicherheitsvorfälle reagieren zu können empfiehlt sich die Strukturierung in drei Reaktionsphasen:

- **Eindämmung:** Hierbei handelt es sich um sofortige Maßnahmen zur Eindämmung des Sicherheitsvorfalls. Dies kann beispielsweise durch die Isolierung betroffener Systeme, die Sperrung von Benutzer:innenkonten sowie das Abschalten kompromittierter Netzwerksegmente geschehen
- **Beseitigung:** Hierbei handelt es sich um die Beseitigung der Ursache des Sicherheitsvorfalls. Dies kann beispielsweise durch die Entfernung von Schadsoftware, das Schließen von Schwachstellen (siehe Kapitel 5.9.3) sowie den Austausch betroffener Komponenten sichergestellt werden.
- **Wiederherstellung:** Hierbei handelt es sich um die Wiederherstellung des Betriebs nach einem Sicherheitsvorfall. Dies kann durch das Rückspielen von geprüften Backups (siehe Kapitel 5.12.2) sowie das Testen der Systeme und Funktionen geschehen.

Je nach Art und Klassifizierung des Sicherheitsvorfalls (siehe Kapitel 5.11.4) unterscheiden sich die Anforderungen an diese Phasen maßgeblich. Ein breitflächiger Ransomware-Befall erfordert unmittelbar das Trennen betroffener Systeme vom Netz, die forensisch gesicherte Ursachenanalyse und das Neuaufsetzen kompromittierter Systeme, sowie eine kontrollierte Wiederanbindung mittels geprüfter Backups. [82] Im Gegensatz dazu liegt der Fokus bei Phishing-Angriffen auf der raschen Sperrung kompromittierter Benutzer:innenkonten und der systemweiten E-Mail-Bereinigung. [83] Auch verlorene Geräte oder interne Missbrauchsfälle müssen spezifisch behandelt werden. Beispielsweise durch die Löschung der Zugriffrechte und anschließender forensischer Prüfung. [84] Bei verdächtigen Login-Versuchen hingegen sind risikobasierte Zugriffskontrollen, Token-Widerrufe und Verifikation von Identitäten zentrale Maßnahmen, welche der Eskalation vorbeugen. [85]

Um auf unterschiedlichste Sicherheitsvorfälle vorbereitet zu sein, empfiehlt es sich die wesentlichsten Arten von Vorfällen für das KMU zu definieren und hierfür verschiedene Herangehensweisen und Maßnahmen der drei Reaktionsphasen vorab zu definieren. Durch die Anwendung von Checklisten kann diese Vorgehensweise strukturiert von den verantwortlichen Stellen sichergestellt werden. Die WKO definiert eine organisatorische Checkliste für das Eintreten eines Sicherheitsvorfalles, welche als Grundlage für die Erstellung einer eigenen Checkliste dienen kann. [86] Eine technische Checkliste wird vom BSI definiert. [87]

Weiters ist ein Kommunikationsplan festzulegen welcher nicht nur interne, sondern auch externe Kommunikationen (z.B. Erstmeldung an eine Behörde) berücksichtigt. Hierfür ist es zu empfehlen eine kompakte

Notfallkontaktliste zu erstellen, welche alle wesentlichen internen Rollen (beispielsweise ISB, IT-Leitung sowie gegebenenfalls externe Dienstleistende) inklusive ihrer Kontaktdaten auflistet. Sicherheitsvorfälle ab „Stufe 3 - Kritischer Vorfall / Notfall“ anhand der definierten Kategorisierungsmatrix (siehe Kapitel 5.11.4) sind gemäß NISG 2024 als „erheblich“ einzustufen und an die Behörden zu melden.

Nach aktueller Rechtslage (NISG 2018) müssen Sicherheitsvorfälle in Österreich an das zuständige sektorspezifische Computer-Notfallteam („CERT“) gemeldet werden. Betreiber wesentlicher Dienste und Anbieter digitaler Dienste nutzen hierfür in der Praxis das zentrale NIS-Meldeportal von CERT.at [88], das sowohl verpflichtende als auch freiwillige Meldungen entgegennimmt. Über dieses Portal werden die Eingaben automatisch an das jeweils zuständige CERT weitergeleitet:

- GovCERT Austria - Einrichtungen des öffentlichen Sektors
- Austrian Energy-CERT - Energieunternehmen
- Austrian HealthCERT - Gesundheits- und Pflegeeinrichtungen

Der Ministerialentwurf zum NISG 2024 sieht in § 18 vor, dass Meldungen künftig elektronisch an die Cybersicherheitsbehörde im BMI über ein Melde- und Analysesystem übermittelt werden. § 34 Abs. 2 des Entwurfs nennt als verpflichtende Mindestangaben:

- Vorfallsart
- Betroffene Systeme
- Erste Abwehrmaßnahmen
- Vorläufige Schadensschätzung
- Kontaktdaten der verantwortlichen Incident-Response-Person (NISG 2024 [9])

Die Meldung muss gemäß NISG 2024 § 34 nach den folgenden Meldestufen und Fristen, wie in Tabelle 5.13 dargestellt, erfolgen:

Stufe	Frist ab Kenntnisnahme	Inhalt laut § 34	Zweck
1 - Frühwarnung	Innerhalb von 24 Stunden	• Vermutete Ursache • Hinweis auf eventuelle rechtswidrige Handlung • Hinweis auf eventuelle grenzüberschreitende Auswirkungen	Sofortiges Lagebild für CSIRT / BMI
2 - Meldung	Innerhalb von 72 Stunden (bei Vertrauensdienst-Anbieter innerhalb 24 Stunden)	• Aktualisierte Anhaben aus Stufe 1 • Erste Bewertung von Schweregrad und Auswirkung • (falls bekannt) Indicator of Compromise	Basis für operative Unterstützung und EU-Weitermeldung
3 - Zwischenbericht	Auf Anforderung von CSIRT / BMI	• Status-Updates und Fortschritt der Abwehrarbeiten	Fortlaufende Lagebeurteilung

Stufe	Frist ab Kenntnisnahme	Inhalt laut § 34	Zweck
4 - Abschlussbericht	Spätestens nach einem Monat nach der 72-Stunden-Meldung. Sollte der Sicherheitsvorfall noch laufen, muss zunächst ein Fortschrittsbericht eingereicht werden und der Abschlussbericht wird spätestens ein Monat nach Beendigung des Vorfalls nachgereicht.	• Detaillierte Beschreibung • Wahrscheinliche Ursachen • Getroffene und laufende Maßnahmen • Grenzüberschreitende Auswirkungen	Lessons Learned und Compliance-Nachweis

Tabelle 5.13: Meldestufen und Firsten nach NISG 2024 [9]

Da sich das NISG 2024 noch im parlamentarischen Verfahren befindet, gilt bis zu dessen Kundmachung weiterhin das Meldeverfahren nach NISG 2018. Sicherheitsvorfälle sind daher unverändert über das NIS-Meldeportal beziehungsweise direkt an das zuständige sektorspezifische CERT zu übermitteln. Hierfür sollte sichergestellt werden, dass die relevanten Kontaktinformationen sowie relevanten Webseiten zur Meldung an die Behörden definiert, zentral abgelegt (z.B. Intranet) und an die relevanten Stakeholder kommuniziert sind.

Wie in Kapitel 5.11.4 erwähnt, wird jeder Sicherheitsvorfall zentral in einem Sicherheitsvorfallsregister (unter anderem inklusive Datum, betroffene Systeme sowie Maßnahmen) dokumentiert. Zusätzlich müssen relevante Logs, Screenshots sowie E-Mails als Beweismittel gesichert werden, um die Nachvollziehbarkeit und Dokumentation zu gewährleisten.

Um im Ernstfall sicherstellen zu können, dass die definierten Prozesse funktionieren und jede verantwortliche Rolle weiß, was zu tun ist, müssen diese regelmäßig getestet werden. Hierfür empfiehlt sich im definierten Prüfprogramm (siehe Kapitel 5.3.4) einen Zyklus festzulegen, an welchen Übungen und Tests hierzu durchgeführt werden. Für KMUs empfiehlt sich hier die kompakte Durchführung eines Planspiels („Table-Top-Exercise“), bei welcher beispielsweise alle drei Jahre auch der Notfallplan (siehe Kapitel 5.12) sowie die Krisenkommunikation (siehe Kapitel 5.12.3) mitbetrachtet werden. So können durch die Mitbetrach-

tung mehrerer Themen Synergien genutzt werden und ressourcensparend sowie effektiv die Anforderungen umgesetzt werden. Eine solche Table-Top-Exercise hat beispielsweise dann als Zielsetzung die Reaktionsfähigkeit auf Sicherheitsvorfälle, Notfälle und Krisen sowie die definierten Zuständigkeiten und Aufgaben zu testen sowie den bestehenden Notfallplan, Wiederanlaufstrategien und Meldeverfahren zu überprüfen. Auch wird hierbei die interne sowie externe Kommunikation (z.B. Kund:innen, Behörden sowie Medien) geübt. Üblicherweise empfiehlt sich hierbei die Teilnahme der wesentlichsten Rollen wie beispielsweise der:die ISB, die IT-Leitung, Verantwortliche der IT-Abteilung, die oberste Leitungsebene, die jeweiligen Fachabteilungen der betroffenen Prozesse (z.B. Einkauf, HR, Buchhaltung, etc.) sowie gegebenenfalls IT-Dienstleister:innen. Nähere Informationen zu einer solchen Planübung sind in Kapitel 5.12 beschrieben. Wie die Erkenntnisse der Übungen und Tests in die kontinuierliche Verbesserung und Anpassung der Prozesse einfließen wird im nächsten Kapitel behandelt.

5.11.6 Erkenntnisse nach Cybersicherheitsvorfällen

Mapping - NIS2 Durchführungsverordnung (Punkt 3.6.): Abschnitt 3.6 der Verordnung verpflichtet Einrichtungen dazu, nach erfolgter Wiederherstellung eines Sicherheitsvorfalls eine strukturierte Nachbereitung durchzuführen (3.6.1). Ziel dieser sogenannten Post-Incident Reviews ist die Ursachenanalyse und die Ableitung dokumentierter Lessons Learned zur Vermeidung zukünftiger Vorfälle. Konkret fordert die Verordnung:

- Analyse der Ursachen des Vorfalls und Dokumentation der Erkenntnisse (3.6.1),
- Nutzung der Erkenntnisse zur Weiterentwicklung von Sicherheitsmaßnahmen, Risikoanalysen und Vorfallsmanagementprozessen (3.6.2),
- Regelmäßige Überprüfung, ob Vorfälle zu einer Nachbereitung geführt haben (3.6.3).

Interpretation der Anforderungen: Die Anforderung unterstreicht, dass die Behandlung von Sicherheitsvorfällen nicht mit der technischen Behebung enden darf. Gerade in KMUs bietet eine strukturierte und pragmatische Nachbereitung eine wichtige Gelegenheit zur kontinuierlichen Verbesserung. Dabei geht es nicht um Schuldzuweisungen, sondern um das systematische Lernen aus Fehlern und Schwachstellen. Dies kann beispielsweise durch die Überarbeitung von Prozessen, Anpassung technischer Maßnahmen oder gezielte Awareness-Maßnahmen erzielt werden. Um wirksam zu sein, müssen diese Erkenntnisse dokumentiert, nachvollziehbar kommuniziert und in bestehende Richtlinien, Prozesse und Schulungen überführt werden.

Umsetzung im NIS2-ISMS-Framework: KMUs sollten hierfür einen Schwellwert definieren, ab wann bei

Sicherheitsvorfällen ein Termin zur Nachüberprüfung („Post-Incident-Review“) durchgeführt werden muss. Dies kann gemäß der Kategorisierungsmatrix beispielsweise ab Stufe 2 oder höher geschehen. Die Verantwortung für die Durchführung kann primär bei der IT-Abteilung liegen, wobei je nach Schweregrad und Umfang weitere Beteiligte (z.B. ISB, oberste Leitungsebene, betroffene Fachbereiche, etc.) hinzugezogen werden sollten. Zur Vorbereitung des Termins müssen alle relevanten Dokumente, wie beispielsweise Logs und forensische Daten (sofern vorhanden), die Dokumentation des Sicherheitsvorfalls, der Kommunikationsverlauf sowie eingesetzte Maßnahmen, zusammengestellt werden. Bei der Durchführung der Nachüberprüfung sollen dann standardisierte Fragen beantwortet werden, um die Schwachstellen sowie Verbesserungspotenziale und somit die kontinuierliche Verbesserung sicherzustellen. Dies kann beispielsweise nach dem PDCA-Zyklus (siehe Kapitel 2.2.2) strukturiert gestaltet werden, wie in der folgenden Tabelle 5.14 beispielhaft dargestellt:

Phase	**Fragebereich**	**Beispielfragen**
Plan	Vorbereitung, Planung und Prävention	• Gab es im Vorfeld bekannte Schwachstellen? • Gab es klare Prozesse und Richtlinien für diesen Fall? • Waren alle Rollen und Eskalationsstufen dokumentiert und bekannt?
Do	Ablauf und Maßnahmen während des Sicherheitsvorfalls	• Wie wurde der Vorfall entdeckt? • Wer war beteiligt? • Welche Sofortmaßnahmen wurden umgesetzt? • War die Kommunikation effektiv (intern/extern)?
Check	Bewertung und Analyse der Wirksamkeit	• Welche Maßnahmen waren erfolgreich? • Wo gab es Verzögerungen oder Fehleinschätzungen? • Welche Schwächen wurden sichtbar (technisch, organisatorisch)?

Phase	Fragebereich	Beispielfragen
Act	Ableitung von Verbesserungen / Lessons Learned	• Was muss geändert werden (Prozesse, Rollen, Technik)? • Welche Maßnahmen wurden beschlossen? • Welche Schulungen oder Sensibilisierungen sind nötig? • Müssen Richtlinien angepasst werden?

Tabelle 5.14: Lessons-Learned-Fragen zu Sicherheitsvorfällen

Die Anwendung des PDCA-Zyklus im Rahmen von Post-Incident-Reviews bietet KMUs eine praxisnahe und gleichzeitig normgerechte Vorgehensweise zur strukturierten Analyse von Sicherheitsvorfällen. Durch die klare Trennung in Planungs-, Durchführungs-, Bewertungs- und Verbesserungsphase lassen sich Schwachstellen gezielt identifizieren und Maßnahmen ableiten, welche zu einer messbaren Erhöhung der Resilienz beitragen. Mithilfe eines Protokolls muss die Dokumentation dieser Post-Incident-Review-Termine sichergestellt werden. Anschließend sind anhand der Erkenntnisse Maßnahmen abzuleiten. Diese können beispielsweise die Anpassung von Prozessen, die Durchführung von Awareness-Schulungen oder technische Konfigurationen umfassen. Die Maßnahmen werden dann je nach Art im jeweiligen Register der betroffenen Prozesse (insbesondere Änderungsmanagement, Schwachstellenmanagement, etc.) aufgenommen und nachverfolgt.

Im Rahmen einer regelmäßigen Überprüfung wird seitens des:der ISB die Durchführung der Post-Incidents-Reviews stichprobenartig überprüft (siehe Kapitel 5.3.3). Erkenntnisse sowie Abweichungen fließen in das Risikomanagement, der Anpassung sowie der kontinuierlichen Verbesserung des Themenbereichs ein.

5.12 Betriebskontinuitäts- und Krisenmanagement

Ein Betriebskontinuitäts- und Krisenmanagement ist zentraler Bestandteil eines ISMS. Ziel ist es, auch bei gravierenden Störungen die Handlungsfähigkeit und kritische Geschäftsprozesse sicherzustellen. Dieses Kapitel zeigt basierend auf klaren Zuständigkeiten, dokumentierten Prozessen und regelmäßigen Tests, wie KMUs mit pragmatischen Mitteln Notfallplanung, Wiederherstellung und Krisensteuerung umsetzen

können.

5.12.1 Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne

Mapping - NIS2 Durchführungsverordnung (Punkt 4.1.): Abschnitt 4.1 der NIS2-Durchführungsverordnung verpflichtet Unternehmen zur Erstellung, Pflege und regelmäßigen Überprüfung eines Notfallplans für die Aufrechterhaltung und Wiederherstellung des Betriebs im Falle von Sicherheitsvorfällen (4.1.1). Der Plan muss auf einer vorangegangenen Risikoanalyse (siehe 2.1 Verordnung) sowie einer Business Impact Analyse (BIA) basieren (4.1.3) und insbesondere folgende Inhalte abdecken (4.1.2):

- Zweck, Anwendungsbereich und Zielgruppe des Plans (a),
- Verantwortlichkeiten und interne wie externe Kontaktwege (b-c),
- Aktivierungs- und Deaktivierungsbedingungen (d),
- Wiederherstellungsreihenfolge und spezifische Wiederherstellungspläne inklusive Zielzeiten (e-f),
- Ressourcenbedarf wie Backups und Redundanzen (g),
- Maßnahmen zur Wiederaufnahme von Aktivitäten (h).

Die Pläne sind regelmäßig zu testen, zu überprüfen und auf Basis von Vorfällen oder veränderten Rahmenbedingungen anzupassen. Ergebnisse aus Tests und Vorfällen sind in die kontinuierliche Weiterentwicklung einzubeziehen (4.1.4).

Interpretation der Anforderungen: Betriebskontinuität ist kein rein technisches, sondern ein strategisches Thema, das eng mit dem Risiko- und Sicherheitsvorfallmanagement (siehe Kapitel 5.3.1 und 5.11) verzahnt ist. Die Anforderung unterstreicht, dass Organisationen im Falle gravierender Störungen, egal ob durch Cyberangriffe, Ausfälle oder andere Ereignisse, in der Lage sein müssen, kritische Geschäftsprozesse zeitnah wiederherzustellen. Für KMUs bedeutet es, dass es keine komplexen Pläne braucht, sondern pragmatische, gut dokumentierte und getestete Handlungsanweisungen, welche auch unter Stress funktionieren. Entscheidend ist hierbei, dass Wiederherstellungsprioritäten auf Basis einer BIA festgelegt und Ressourcen (wie Backups, Ausweichsysteme, Kontakte zu Dienstleister:innen) im Vorfeld geklärt sind. Ein regelmäßig getesteter und gelebter Notfallplan entscheidet im Ernstfall über wirtschaftliches Überleben. Dies gilt insbesondere bei KMUs mit begrenzten Ressourcen.

Umsetzung im NIS2-ISMS-Framework: Zu Beginn ist die Aufbauorganisation des BCM festzulegen, einschließlich der Rollen und Verantwortlichkeiten. In einem KMU bietet es sich an, die Funktion des:der Not-

fallbeauftragten durch den:die ISB oder die IT-Leitung wahrnehmen zu lassen. Diese Rolle übernimmt die zentrale Koordination des BCM, die Pflege des Notfallplans sowie die Organisation und Durchführung von Tests und Übungen. Die IT-Abteilung (bei Auslagerung externe IT-Dienstleister:innen) trägt die operative Verantwortung für die technische Wiederherstellung, etwa durch Rücksicherung von Backups oder Neuaufsetzung von Systemen. Die oberste Leitungsebene ist für strategische Entscheidungen, die Aktivierung des Notfallplans und (im Falle einer Krise) für die externe Krisenkommunikation zuständig. Fachabteilungen sind in ihre jeweiligen Aufgabenbereiche eingebunden, etwa bei der Priorisierung kritischer Prozesse oder bei der Mitwirkung an Notfallübungen. Im weiteren Schritt wird eine BIA durchgeführt, bei welcher die kritischsten Geschäftsprozesse/Dienstleistungen (sogenannte „Kronjuwelen“ des Unternehmens) inklusive ihrer Abhängigkeiten zu Assets identifiziert, die Auswirkungen auf die Schutzziele (hierbei insbesondere Verfügbarkeit) sowie die Werte RPO und RTO je Asset festgelegt werden. Da im Rahmen dieser Arbeit das Thema BIA zur Nutzung von Synergien bereits im Themenbereich Risikomanagement thematisiert wurde, sind nähere Informationen zur Durchführung im Kapitel 5.3.1 sowie im zugehörigen beispielhaften IS-Risikomanagement-Handbuch zu finden. Sofern diese Analyse durchgeführt wurde, ist auf Basis der Ergebnisse ein Notfallplan zu erstellen. Ein Notfallplan besteht im Normalfall aus den folgenden zwei Themenbereichen:

- **Businesskontinuität:** beschreibt organisatorische Maßnahmen zur Aufrechterhaltung kritischer Geschäftsprozesse/Dienstleistungen.
- **Wiederherstellung:** beschreibt technische Wiederherstellungsmaßnahmen nach Sicherheitsvorfällen oder IT-Ausfällen.

Für die Erstellung eines Notfallplans können KMUs auf bestehende offene Praxishilfen zugreifen. Insbesondere das BSI [89] sowie die WKO [90] stellen hierfür Vorlagen und Beispieldokumente für Notfallpläne bereit, welche als Basis verwendet werden können.

Im Rahmen dieser Arbeit wurde eine Vorlage erstellt, welches von KMUs als Basis für einen Notfallplan verwendet werden kann. Die Einzelheiten müssen vor aktiver Verwendung jedoch angepasst werden. Im Wesentlichen ist bei der Erstellung folgendes zu berücksichtigen:

- **Rollen und Verantwortlichkeitsfestlegung:** Zu Beginn werden die beteiligten Rollen und ihre Verantwortlichkeiten festgelegt. In KMUs bietet es sich an, die Rolle des:der Notfallbeauftragten mit der ISB-Funktion oder der IT-Leitung zu vereinen. Die IT-Abteilung übernimmt die technische Wiederherstellung, während Fachbereiche ihre Prozesskenntnisse einbringen. Die oberste Leitungsebene

trägt die strategische Gesamtverantwortung. Diese klare Rollenverteilung ist entscheidend für eine wirksame Umsetzung und spätere Eskalation im Ernstfall.

- **Verknüpfung mit Risikoanalyse und BIA:** Der Notfallplan basiert auf einer vorgelagerten BIA im Risikomanagement (siehe Kapitel 5.3.1). Die BIA identifiziert kritische Geschäftsprozesse, klassifiziert sie hinsichtlich ihrer Kritikalität und legt RTO und RPO fest. Diese Ergebnisse bilden die Grundlage für die Wiederanlaufreihenfolge und -maßnahmen.
- **Definition von Aktivierungs- und Deaktivierungskriterien:** Ein zentrales Element ist die Festlegung von Schwellenwerten, ab wann der Notfallplan aktiviert wird. Diese Kriterien orientieren sich an der Kritikalität der betroffenen Prozesse und Systeme sowie der Dauer und dem Ausmaß des Ausfalls. Ebenso werden klare Regeln zur Rückkehr in den Normalbetrieb definiert, einschließlich der Kommunikation und Dokumentation der Deeskalation.
- **Aufbau des Kommunikationsplans:** Wie schon in Kapitel 5.11.3 erwähnt, sind interne als auch externe Kommunikationswege verbindlich festzulegen. Dies umfasst Eskalationsketten, Kontaktdaten, Kommunikationskanäle und Zuständigkeiten für die behördliche Meldung gemäß NIS2 (z.B. an CERTs). Eine aktuelle Kontaktliste bildet das Rückgrat der Notfallkommunikation und wird regelmäßig durch den:die Notfallbeauftragte:n gepflegt.
- **Entwicklung der Wiederanlaufmaßnahmen:** Basierend auf der Wiederanlaufreihenfolge und den Anforderungen aus der BIA werden technische Wiederanlaufmaßnahmen ausgearbeitet. Diese beschreiben, wie die betroffenen Assets wiederhergestellt werden, welche Backupmaßnahmen (auf Basis von Kapitel 5.12.2) zur Anwendung kommen und welche Übergangslösungen für einen Notbetrieb möglich sind. Ergänzt wird dies durch Rollenzuweisungen für Prüfungen, Kommunikation und Rückführung.

Der Notfallplan darf nicht als ein einmalig erstelltes Dokument betrachtet werden, sondern unterliegt einem definierten Prüf- und Übungszyklus. Wie bereits in Kapitel 5.11.6 erwähnt, eignen sich unter anderem Planspiele, aber auch Wiederherstellungstests und Kommunikationsprüfungen, welche regelmäßig durchgeführt und dokumentiert werden, um die Effektivität der Pläne zu testen. Diese sind im zentralen Prüfprogramm (siehe Kapitel 5.3.4) zu planen und dokumentieren. Auch der BSI-Standard 200-4 betont: Nur getestete Pläne sind belastbar und einsatzfähig. [81, pp. 253-288]

Der BSI-Standard 200-4 beschreibt hierbei wie in Tabelle 5.15 folgende Übungsarten:

Übungsart	Zielsetzung
Planbesprechung („Schreibtischtest“ oder „Tabletop-Übung“)	Plausibilitätsprüfung von Notfallplänen ohne realistische Durchführung
Funktionstest	Überprüfung technischer Maßnahmen, z.B. Wiederherstellung von Backups
Stabsübung	Simulation eines Notfalls und Koordination durch das Notfallteam
Alarmierungsübung	Test der Kommunikations- und Alarmierungswege

Tabelle 5.15: Übungsarten nach BSI 200-4 [81]

Eine „Stabsübung“ wird in KMUs in der Regel nicht benötigt, da der Aufwand in der Regel nicht im Verhältnis zum Nutzen steht. [81, pp. 253-288] Um Synergien zu nutzen und die Schonung von Ressourcen sicherzustellen, empfiehlt es sich beispielsweise Planbesprechungen mit den anderen Themenbereichen Sicherheitsvorfallsmanagement (siehe Kapitel 5.11) sowie Krisenmanagement (siehe Kapitel 5.12.3) zu verknüpfen.

Eine Planung, Durchführung und Nachbereitung einer Planbesprechung kann angelehnt auf Basis des BSI-Standards 200-4 wie folgt aussehen und zeitlich geplant werden:

1. **Vorbereitung** (zwei Wochen vorab):
    - **Definition des Ziels:** z.B. Überprüfung der Aktivierung des Notfallplans, Kommunikation bei Notfällen oder Koordination der Wiederherstellung
    - **Erstellung eines Szenarios:** z.B. Malware-Befall mit Ausfall ERP-System → Prozessstörung in der Fakturierung → kritischer Engpass → Kund:innenreklamationen → Medienanfrage
    - **Festlegung der Teilnehmenden:** ISB (Notfallbeauftragte:r), IT-Leitung, oberste Leitungsebene, Fachbereichsvertretungen, gegebenenfalls externe IT-Dienstleister:innen
    - **Verteilung von Unterlagen:** Notfallplan, Wiederanlaufpriorität, Kommunikationsplan, Meldewege, Checklisten
    - **Festlegung der Moderation:** ISB oder neutrale Person (z.B. externe Berater:innen)
2. **Durchführung** (drei bis vier Stunden):
    - **Einleitung und Zielsetzung:** Einführung und Ziele der Übung

  - Was soll getestet werden? Welche Rollen sind involviert
- **Auslöser eines Sicherheitsvorfalls:** Szenario startet beispielsweise durch verdächtige E-Mail oder Ausfall eines Systems
  - Wie wird reagiert? Wer erkennt den Sicherheitsvorfall? Wer meldet?
- **Notfalllage:** Geschäftsprozesse sind unterbrochen → Aktivierung des Notfallplans
  - Wann erfolgt die Aktivierung? Wer entscheidet?
- **Wiederanlauf und Notbetrieb:** Maßnahmen zur Überbrückung werden gesetzt
  - Wie erfolgt die Wiederherstellung? Sind Übergangslösungen nutzbar?
- **Krise und externe Kommunikation:** z.B. Medienanfrage und Kommunikation mit Kund:innen nötig
  - Wer kommuniziert? Sind Meldungen nötig?
- **Rückkehr in Normalbetrieb:** Systeme wieder verfügbar
  - Wie erfolgt die Deeskalation? Was muss dokumentiert werden?

3. **Nachbereitung** (nach einer Woche):
   - Durchführung eines Workshops zur Abstimmung der Beobachtungen und Erkenntnisse
   - Erstellung und Ableitung von Maßnahmen
   - Dokumentation der Übung inklusive Teilnehmer:innen, Datum Szenario, Ablauf, Beobachtungen und Maßnahmenempfehlungen [81, pp. 253-288]

Die daraus abgeleiteten Erkenntnisse fließen in die Anpassung des Notfallplans sowie die kontinuierliche Verbesserung ein. Die finale Verantwortung liegt bei dem:der Notfallbeauftragten, welche:r jährlich eine Überprüfung und Aktualisierung initiiert.

5.12.2 Backup-, Redundanz- und Wiederherstellungsmanagement

Mapping - NIS2 Durchführungsverordnung (Punkt 4.2.): Abschnitt 4.2 der NIS2-Durchführungsverordnung verpflichtet Unternehmen zur Umsetzung eines strukturierten Backup- und Redundanzmanagements zur Sicherstellung der Betriebsfähigkeit im Notfall (4.2.1). Auf Basis der Risikoanalyse (siehe 2.1 der Verordnung) und des Notfallplans müssen formalisierte Sicherungspläne erstellt werden, welche insbesondere folgende Anforderungen erfüllen (4.2.2):

- Festlegung von Wiederherstellungszeiten (a),
- Gewährleistung vollständiger und korrekter Backupkopien, auch in Cloudumgebungen (b),
- Sichere, netzwerkgetrennte und geographisch verteilte Speicherung der Backups (c),

- Physische und logische Zugriffskontrollen gemäß Asset-Klassifikation (d),
- Definierte Verfahren zur Datenwiederherstellung (e),
- Festgelegte Aufbewahrungsfristen auf Basis gesetzlicher und geschäftlicher Anforderungen (f).

Zusätzlich sind regelmäßige Integritätsprüfungen der Backupkopien durchzuführen (4.2.3). Auf Basis der Risikoanalyse und des BCM sind geeignete Redundanzen vorzusehen, u.a. für Systeme, Assets, Personal und Kommunikationskanäle (4.2.4). Die Ressourcenüberwachung soll sich an den Backup- und Redundanzanforderungen orientieren (4.2.5). Wiederherstellungstests sind regelmäßig durchzuführen, zu dokumentieren und bei Bedarf durch Korrekturmaßnahmen zu ergänzen (4.2.6).

Interpretation der Anforderungen: Backup- und Redundanzmanagement ist kein rein technischer Selbstzweck, sondern ein zentraler Pfeiler der betrieblichen Resilienz und Wiederherstellungsfähigkeit. Die Anforderung betont, dass Organisationen ihre Betriebsfähigkeit auch im Krisenfall aufrechterhalten oder zeitnah durch robuste, verifizierte Backupverfahren und geeignete Redundanzen wiederherstellen müssen. Für KMUs bedeutet dies, dass es keine hochkomplexen Backup-Infrastrukturen, sondern funktionierende, dokumentierte und regelmäßig getestete Prozesse, die im Ernstfall verlässlich greifen. Entscheidend ist, dass Backupziele (z.B. RPO, RTO) definiert, Speicherkonzepte von der Produktionsumgebung getrennt und Wiederherstellungen realistisch eingeübt werden. Auch personelle und infrastrukturelle Redundanzen sollten berücksichtigt werden. So wird verhindert, dass einzelne System- oder Personenausfälle den gesamten Betrieb gefährden.

Umsetzung im NIS2-ISMS-Framework: Auf Basis der definierten Werte der BIA (siehe Kapitel 5.3.1) sowie des Notfallplans muss im nächsten Schritt definiert und dokumentiert werden, wann und in welcher Form Backups bei den Assets durchzuführen sind. Gemäß dem BSI-Standards 200-4 ist insbesondere bei IT-gestützten Notfallprozessen sicherzustellen, dass eine geeignete Datenbasis für den Notbetrieb sowie für die Rückkehr in den Normalbetrieb bereitsteht. Dies umfasst insbesondere Anwendungsdaten, Konfigurationsdateien, Kommunikationsprotokolle und betriebsrelevante Metadaten. [81] Zur konkreten Umsetzung empfiehlt das Bundesamt für Sicherheit in der Informationstechnik im Beitrag „Datensicherung - wie geht das?“ die Nutzung folgender Backup-Methoden: [91]

- **Vollbackup:** Sämtliche ausgewählten Dateien werden vollständig auf ein externes Medium gesichert. Vorteilhaft ist hierbei die einfache und schnelle Wiederherstellung, jedoch ist dieses Verfahren speicherintensiv und zeitaufwendig.

- **Inkrementelles Backup:** Es werden nur die seit dem letzten Backup geänderten Dateien (Vollbackup oder Inkrementelles Backup) gesichert. Dies reduziert den Speicherbedarf und die Dauer des Sicherungsvorgangs, erfordert jedoch bei der Wiederherstellung alle inkrementellen Schritte ab dem letzten Vollbackup.
- **Differentielles Backup:** Gesichert werden alle Änderungen seit dem letzten Vollbackup. Die Wiederherstellung ist schneller als bei inkrementellen Backups, benötigt aber mehr Speicherplatz.
- **Systemabbild (Image-Backup):** Hierbei wird ein vollständiges Abbild eines Systems inklusive Betriebssystem, Konfigurationen und installierter Anwendungen erstellt. Dies erlaubt eine schnelle Wiederherstellung kompletter Systeme, ist jedoch speicherintensiv und nur für ausgewählte, besonders kritische Systeme sinnvoll.

Abgeleitet den RPO-Werten der BIA muss für jedes Asset bestimmt werden, in welchem Zyklus welche Backup-Arten durchgeführt werden müssen. Ziel ist es, durch die Durchführung von Backups, die in der BIA festgelegten Recovery Point Objectives, im Notfall einhalten zu können. Allgemein empfiehlt sich für KMUs, dass beispielsweise bei Systemen mit hoher Kritikalität tägliche inkrementelle Backups, wöchentliche Vollbackups sowie vierteljährlich ein Systemabbild zur schnellen Wiederherstellung durchgeführt werden. Bei Systeme mit mittlerer Kritikalität hingegen können wöchentliche Vollbackups sowie optional zusätzlich alle zwei bis drei Tage inkrementelle Backups erstellt werden. Für wenig kritische Systeme kann ein differentielles Backup in einem definierten Wochenrhythmus ausreichend erscheinen. Zusätzlich ist laut dem BSI-Online-Beitrag zu empfehlen, dass Konfigurationsdateien individuell angepasster Systeme separat gesichert werden (z.B. bei Firewalls), da diese bei einer Neuinstallation ansonsten verloren gehen können. [91] Die Speicherorte der Backups sind physisch oder logisch vom produktiven Netz getrennt aufzubewahren (z.B. durch „Offsite“-Speicherungen). Die Backups sollten durch entsprechende Zugangskontrollen (siehe Kapitel 5.8) nur für autorisierte Personen zugänglich sein.

Die Aufbewahrung erfolgt bestenfalls abgestuft: tägliche inkrementelle Backups werden jeweils für sieben Tage vorgehalten und dann überschrieben, wöchentliche Vollbackups verbleiben für vier bis sechs Wochen im System. Die quartalsweisen Systemabbilder hingegen werden für ein Jahr archiviert. Bei rechtlich relevanten Daten (Buchhaltungsunterlagen, Belege, Rechnungen, etc.) empfiehlt es sich zusätzlich, ein jährliches Archiv-Backup anzulegen, welches über sieben Jahre aufbewahrt wird, um den steuer- und handelsrechtlichen Vorgaben gerecht zu werden. [92]

Für KMUs stellt sich die Frage, ob für die regelmäßige Datensicherung zwingend externe Softwarelösungen benötigt werden oder ob bereits mit vorhandenen Ressourcen ausreichende Backup-Maßnahmen umgesetzt werden können. Tatsächlich bieten die gängigen Betriebssysteme sowie moderne Netzwerkspeicher („NAS“) eine Vielzahl an integrierten Funktionen, mit denen grundlegende Backup-Anforderungen bereits zuverlässig abgedeckt werden können. Im Windows-Umfeld steht mit Windows Server Backup ein integriertes Tool zur Verfügung, das vollständige Sicherungen von Systemen und Daten auf externe Laufwerke oder Netzlaufwerke ermöglicht. Für Desktop-Systeme kann der sogenannte Dateiversionsverlauf genutzt werden, um automatisch Änderungen in Benutzer:innenordnern zu sichern und bei Bedarf frühere Versionen wiederherzustellen. Unter Linux-basierten Systemen können bewährte Werkzeuge wie „rsync“ eingesetzt werden, um regelmäßige Datei- oder Systembackups zu erstellen. Kombiniert mit dem Zeitplanungsdienst „cron“ lassen sich diese Aufgaben vollständig automatisieren. Eine empfehlenswerte Lösung für KMUs sind NAS-Systeme, wie etwa von Synology.

Bezüglich Redundanz werden im BSI-Dokument „Redundanz - Modularität - Skalierbarkeit“ folgende Redundanzkonzepte beschrieben: [93]

- **Betriebsredundanz:** Ein zusätzliches System steht bereit und übernimmt im Fehlerfall die Aufgaben des ausgefallenen Systems.
- **Wartungsredundanz:** Zwei zusätzliche Systeme sichern den Betrieb auch bei gleichzeitiger Wartung und Ausfall eines weiteren Systems.
- **Georedundanz:** Systeme oder Daten werden an einem zweiten geografisch getrennten Standort gespiegelt, um bei standortweiten Ausfällen weiterarbeiten zu können.
- **Temporäre Redundanz:** Temporäre Systeme (z.B. mobile Notfall-Server) werden nur bei Wartung oder erhöhtem Risiko zugeschaltet.

Für KMUs lässt sich hieraus ableiten, dass für kritische Systeme ein N+1-Redundanzkonzept (Unterkategorie der Betriebsredundanz) eingeführt wird. Das N+1-Redundanzprinzip bezeichnet gemäß dem BSI-Dokument die Bereitstellung einer zusätzlichen Komponente („+1“) zu den für den Normalbetrieb benötigten („N“) Einheiten, um beim Ausfall einer Komponente den Betrieb ohne Unterbrechung aufrechterhalten zu können. [93] Zusätzlich empfiehlt sich bei KMUs die Verwendung von Cloud-Diensten mit Georedundanzen, um den Aufbau einer komplexen und aufwändigen Netzwerkinfrastruktur zu vermeiden. Außerdem sind nicht nur Redundanzen auf Systemebene (z.B. Netzwerk, Server), sondern auch bei Einrichtungen, Equipment, Personal und Kommunikationskanälen sicherzustellen. Der BSI-Standard verweist hier in die-

sem Zusammenhang auf die Bedeutung einer strukturierten Ressourcenplanung sowie personeller Vertretungsregelungen im Rahmen des Notfallmanagements [81] KMUs sollten hierfür zumindest:

- Für alle kritischen Systeme Notfallvertretungen zusätzlich zu den Asset-Verantwortlichen regeln
- Redundante Kommunikationsmittel vorsehen (z.B. Notfall-Smartphones)
- Externe Dienstleistende mit SLAs zur Notfallunterstützung einbinden (siehe Kapitel 5.7.1)

Zudem sind regelmäßige Wiederherstellungstests und Integritätsprüfungen verpflichtend, um die tatsächliche Nutzbarkeit der Backups im Ernstfall sicherzustellen. Bereits im Kapitel zuvor wurden dazu verschiedene Testformate beschrieben. Besonders relevant ist hierbei der sogenannte Funktionstest, wie auch im BSI-Standard 200-4 beschrieben. [81] Ein Funktionstest überprüft konkret, ob aus einem definierten Backup-Stand ein System oder eine Datei tatsächlich erfolgreich wiederhergestellt werden kann und ob diese anschließend auch funktionsfähig und konsistent ist. Ziel ist es, die vollständige und fehlerfreie Rücksicherung sowohl für Einzeldateien (z.B. bei File-Shares, etc.) als auch für komplette Systeme (z.B. ERP-Server, etc.) zu validieren.

Für KMUs empfiehlt sich dies im zentralen Prüfprogramm (siehe Kapitel 5.3.4) zu planen und dokumentieren. Dies kann beispielsweise wie folgt aussehen:

- Jährliche Wiederherstellung einzelner kritischer Daten aus Backups
- Alle zwei bis drei Jahre ein vollständiger Wiederherstellungs-Test eines kompletten kritischen Systems

5.12.3 Krisenmanagement

Mapping - NIS2 Durchführungsverordnung (Punkt 4.3.): Abschnitt 4.3 der NIS2-Durchführungsverordnung verpflichtet Unternehmen zur Einführung eines strukturierten Krisenmanagementprozesses (4.3.1). Dieser Prozess muss mindestens folgende Elemente abdecken (4.3.2):

- Klare Zuweisung von Rollen und Verantwortlichkeiten für Personal sowie gegebenenfalls externe Dienstleistende, einschließlich definierter Handlungsschritte im Krisenfall (a),
- Geeignete Kommunikationswege mit zuständigen Behörden, insbesondere zur Erfüllung von Meldepflichten und für darüber hinausgehende Informationsflüsse (b),
- Spezifische technische und organisatorische Maßnahmen, die sicherstellen, dass Netz- und Informationssysteme auch im Krisenfall angemessen geschützt bleiben (c).

Darüber hinaus müssen Unternehmen einen Prozess implementieren, um Informationen von zuständigen Behörden oder CSIRTs über Bedrohungen, Schwachstellen und Abwehrmaßnahmen gezielt zu nutzen (4.3.3). Der Krisenmanagementplan ist regelmäßig sowie nach wesentlichen Vorfällen oder Änderungen zu testen, zu überprüfen und gegebenenfalls anzupassen.

Interpretation der Anforderungen: Die Anforderungen unterstreichen, dass Unternehmen in der Lage sein müssen, bei eskalierenden Lagen (z.B. massiven Cyberangriffen, Systemausfällen oder öffentlichen Sicherheitsvorfällen) nicht nur handlungsfähig zu bleiben, sondern koordinierte Entscheidungen zu treffen und Kommunikation unter Hochdruck zu bewältigen. Für KMUs bedeutet das, dass es keine komplexen Krisenstäbe, sondern klare Verantwortlichkeiten, praktikable Kommunikationswege zu Behörden und Dienstleister:innen sowie einfache, nachvollziehbare Handlungsschritte braucht. Entscheidend ist, dass auch unter Stress rechtliche Meldepflichten, interne Koordination und Basisschutz der Systeme sichergestellt sind. Damit wird verhindert, dass Unsicherheit in der Organisation zu Reputations- oder Haftungsrisiken führt. Ein getesteter Krisenmanagementprozess schützt nicht nur die Infrastruktur, sondern die Handlungsfähigkeit des gesamten Unternehmens.

Umsetzung im NIS2-ISMS-Framework: Für KMUs ist es organisatorisch und ressourcentechnisch oftmals nicht praktikabel, zwischen Notfall- und Krisenmanagement vollständig getrennte Prozesse zu etablieren. Daher wird empfohlen, Krisen als eskalierte Notfälle zu behandeln und diese auf der bestehenden Notfallmanagement aufzubauen. Die zentrale Unterscheidung liegt dabei insbesondere in der Verantwortlichkeit: Während im Notfall der:die Notfallbeauftragte (z.B. ISB oder IT-Leitung) die Koordination übernimmt, liegt die Federführung im Krisenfall bei der obersten Leitungsebene, insbesondere wenn strategische Entscheidungen oder externe Kommunikation (z.B. zu Medien oder Behörden) erforderlich sind. Die strukturellen und kommunikativen Grundlagen (z.B. Rollen, Eskalationswege, Kontaktlisten und Kommunikationswege) wurden bereits im Notfallplan (siehe Kapitel 5.12.1) definiert und decken somit auch die Anforderungen der Verordnung weitgehend ab. Darüber hinaus ist ein strukturierter Prozess zu etablieren, wie Informationen von Behörden, CSIRTs oder CERTs verarbeitet und in die eigene Lagebeurteilung des Unternehmens integriert werden. Die Meldungen werden ebenso im Notfallplan berücksichtigt.

Regelmäßige Übungen und Tests dienen dazu, die definierten Dokumente und Abläufe auf Praxistauglichkeit zu prüfen. Wie in Kapitel 5.12.1 dargestellt, können hierfür kombinierte Planbesprechungen genutzt werden, in denen sowohl Notfall- als auch Krisenszenarien gemeinsam simuliert und systematisch evaluiert

werden.

5.13 Umgebungsbezogene und physische Sicherheit

Physische und umgebungsbezogene Sicherheit bilden das Fundament jeder Cyber-Resilienz, weil Ausfälle oder Manipulationen an Gebäuden, Versorgungseinrichtungen und Zutrittssystemen digitale Schutzmaßnahmen wirkungslos machen würden. Die folgenden Abschnitte zeigen, wie KMUs durch klar definierte Sicherheitsperimeter, überwachte Umweltparameter und redundante Versorgungsketten die kontinuierliche Betriebsfähigkeit ihrer kritischen Assets gewährleisten.

5.13.1 Sicherheitsperimeter und physische Zutrittskontrollen

Mapping - NIS2 Durchführungsverordnung (Punkt 13.3.): Abschnitt 13.3 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen dazu, unbefugten physischen Zugang zu ihren Netz- und Informationssystemen sowie zugehörigen Assets zu verhindern, zu überwachen und entsprechende Schutzmaßnahmen zu implementieren (13.3.1). Auf Basis einer Risikoanalyse (siehe Punkt 2.1 der Verordnung) sind Sicherheitsperimeter festzulegen und mit geeigneten Zutrittskontrollen abzusichern (13.3.2 a-b). Zusätzlich sind physische Sicherheitsmaßnahmen für Büros, Räume und technische Einrichtungen zu implementieren (13.3.2 c) und die Räumlichkeiten laufend auf unbefugte Zugriffe zu überwachen (13.3.2 d). Die Maßnahmen zur physischen Zugangskontrolle sind regelmäßig zu testen, zu überprüfen und bei Bedarf zu aktualisieren, insbesondere nach Vorfällen oder wesentlichen Änderungen (13.3.3).

Interpretation der Anforderungen: Die Anforderungen stellen sicher, dass Assets physisch gegen unbefugte Personen abgeschirmt, überwacht und regelmäßig geprüft werden müssen. Auf Basis der Risikoanalyse und der BIA in Kapitel 5.3.1 ist zunächst ein Zonenkonzept zu erstellen, welches vom öffentlich zugänglichen Eingangsbereich bis zum hochsensiblen Serverraum abgestufte Perimeter definiert. Jeder Übergang erhält abgestimmte Kontrollen (z.B. Schließsysteme, Ausweise für Besucher:innen, Videomonitoring oder biometrische Schleusen) deren Ereignisse zentral protokolliert und ausgewertet werden.

Umsetzung im NIS2-ISMS-Framework: Zu Beginn müssen im KMU die Sicherheitsperimeter definiert werden. Bei Sicherheitsperimetern handelt es sich im Wesentlichen um die jeweiligen physischen Zonen in einem Unternehmen, welche je nach Kritikalität differenziert zu behandeln sind. Im „IT-Sicherheitshandbuch für KMU“ der WKO werden beispielhafte Fragen genannt, welche als Basis bei der Identifikation besonders

schützenswerter Räume beachtet werden sollten. [94, p. 87]

- Welche Bereiche oder Räume sind besonders schützenwert (z.B. Serverraum)?
- Wo und wie haben interne sowie externe Personen Zutritt?

Anhand dieser Fragen können im nächsten Schritt die jeweiligen Zonen inklusive der physischen Maßnahmen und Zutrittsregelungen abgeleitet werden. Diese Zonen können unter anderem in einem mehrstufigen Zonierungskonzept (z.B. anhand einer grafischen Darstellung eines vorhandenen Grundrisses) umgesetzt werden. Das BSI beschreibt im „Umsetzungshinweis zum Baustein INF.1 Allgemeines Gebäude“ eine klare Orientierung zur Zonierung, welche von KMUs als Basis verwendet werden kann. Mithilfe des darin beschriebenen Zwiebelschalenkonzepts können sich folgende vier Zonen ableiten, wobei Räume mit ähnlicher Kritikalität zusammengefasst werden sollten: [95]

- **Zone 0:** Außenbereich (z.B. Grundstück, öffentlich zugänglich)
- **Zone 1:** Kontrollierter Innenbereich (z.B. Eingangsbereich, mit Portier:in)
- **Zone 2:** Interner Bereich (z.B. Büroflächen, nur für Mitarbeitende)
- **Zone 3:** Hochsicherheitsbereich (z.B. Serverräume, mit Multi-Faktor-Authentifizierung)

Hierbei ist auch zu berücksichtigen, welche Assets und welche Asset-Kritikalität in den jeweiligen Räumlichkeiten vorhanden sind. In der nachfolgenden Grafik (Abbildung 5.4) ist ein beispielhaftes Zonenkonzept dargestellt. Das Zonenkonzept folgt dem Prinzip der tiefengestaffelten Sicherheit und unterteilt das Gebäude in vier abgestufte Sicherheitszonen (Zone 0-3), wobei Bereiche wie Empfang und Zugang für Lieferant:innen kontrolliert zugänglich (Zone 1), Büroräume intern geschützt (Zone 2) und kritische IT-Infrastruktur besonders abgesichert (Zone 3) sind.

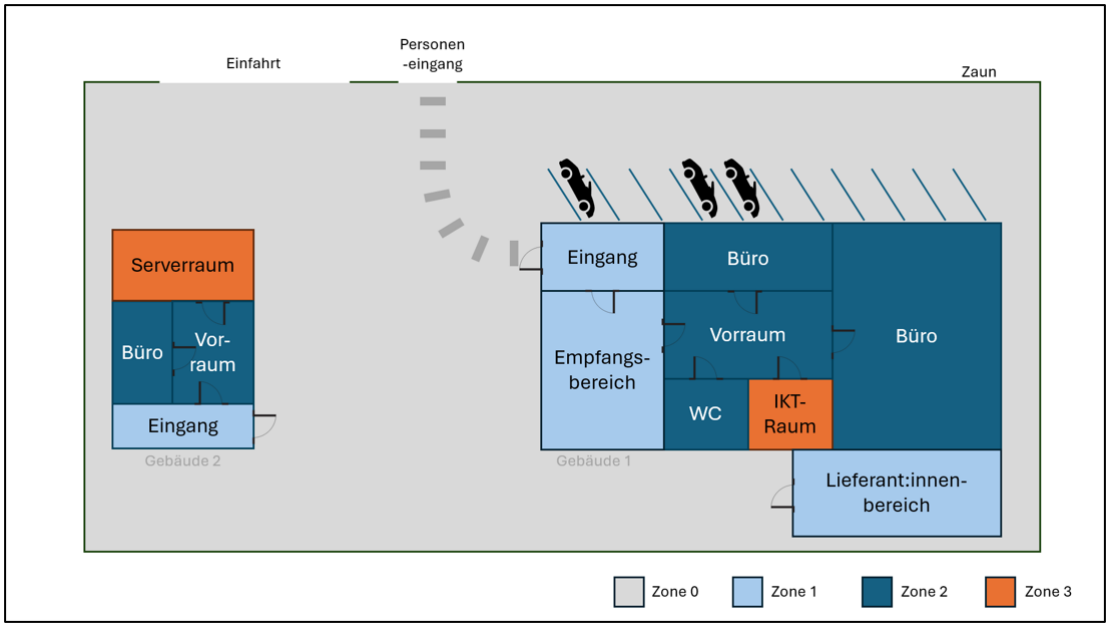

Abbildung 5.4: Beispielhaftes Zonenkonzept für ein fiktives Firmengelände

Die Ableitung der Zonen und Maßnahmen erfolgt auf Basis der im Risikomanagement (siehe Kapitel 5.3.1) festgelegten Asset-Klassifikationen. Sobald die Zonierung festgelegt und dokumentiert ist, sind für die Zonen physische Sicherheitsmaßnahmen (z.B. Videoüberwachung, Alarmanlagen, Schlösser, etc.) sowie Zutrittsregelungen abzuleiten. Für KMUs empfiehlt sich hierbei ein pragmatisches Vorgehen beispielsweise auf Basis Maßnahmen des BSI-IT-Grundschutzes oder der Empfehlungen des IT-Sicherheitshandbuches der WKO. Dies kann beispielsweise wie in der nachfolgenden Tabelle 5.16 je nach Zone definiert sowie in dem Zonenkonzept dokumentiert werden: [94, pp. 86-90]

Zone	**Empfohlene Maßnahmen**	**Ergänzende Hinweise**
Zone 0	• Abgrenzung des Grundstückes (z.B. Zaun, Schranke) • Beleuchtung zur „Abschreckung“	• Kameraüberwachung punktuell bei Zufahrt

Zone	Empfohlene Maßnahmen	Ergänzende Hinweise
Zone 1	• Besucher:innen nur gegen Anmeldung • Zutritt über Gegensprechanlage, Code oder Schlüssel • Zutrittsprotokoll	• Sicherstellung des Managements von Besucher:innen • Kontrollierte Entgegennahme von Lieferungen
Zone 2	• Abschließbare Büroräume • Sichtausweis für Mitarbeitende • Dokumentation der Schlüsselverwaltung	• Zutritt nur für Beschäftigte mit Berechtigung • Keine Schlüsselweitergabe • Regelmäßige Prüfung der Zutrittsregelung
Zone 3	• Starke Einschränkung des Zutritts (z.B. Code, Karte) • Separat abschließbar (z.B. Stahltür) • Protokollierung des Zutritts • Beachtung von Brandschutz	• Dokumentation der Zutrittsrechte • Zugang nur im Bedarfsfall

Tabelle 5.16: Beispielhafte Zonen mit Sicherheitsmaßnahmen

In besonders kritischen Bereichen (z.B. Zone 3) empfiehlt sich zusätzlich der Einsatz technischer Überwachungseinrichtungen wie Videoüberwachung oder Bewegungsmeldern, um unautorisierte Zugriffe in Echtzeit erkennen und dokumentieren zu können.

Zuständig für die Umsetzung dieser Maßnahmen ist im Normalfall die dafür zuständige Stelle für physische Angelegenheiten (z.B. Facility Management, Haustechnik, etc.). Hierbei ist zu beachten, dass die Umsetzung risikoorientiert und Schritt für Schritt umgesetzt werden sollte.

Wie bereits in den abgeleiteten Maßnahmen erwähnt, ist ein weiterer wesentlicher Punkt die Verwaltung der Besucher:innen. Ebenso müssen Vorgaben dokumentiert werden. Das Besucher:innenmanagement stellt sowohl im Umsetzungshinweis des BSI als auch im IT-Sicherheitshandbuch der WKO einen zentralen

Baustein physischer Sicherheitsmaßnahmen dar. Im BSI-Dokument wird empfohlen, den Zutritt externer Personen ausschließlich nach vorheriger Anmeldung und Identitätsprüfung zu gewähren. Besucher:innen sollen einen gut sichtbaren, temporären Ausweis erhalten, sich in ein Buch für Besucher:innen eintragen und während ihres Aufenthalts stets durch berechtigte Mitarbeitende begleitet werden. Zudem sollen sensible Bereiche nur nach gesonderter Freigabe betreten werden dürfen, um unkontrollierte Zugänge in höhere Sicherheitszonen zu verhindern. [95, pp. 6-7] Das WKO-IT-Sicherheitshandbuch konkretisiert diese Anforderungen für die betrieblichen Realitäten von KMUs. Es empfiehlt, definierte Prozesse für Besucher:innen einzuführen, den Empfang als Kontrollinstanz zu etablieren und auch einfache, analoge Mittel wie Besuchslisten oder Papierausweise einzusetzen. Ziel ist ein dokumentierter und nachvollziehbarer Umgang mit externen Personen, um Risiken wie unautorisierten Zugriff, Datenabfluss oder Sabotage vorzubeugen. [94, p. 87] Hierbei sind auch Lieferant:innen zu beachten. Laut BSI sollten diese ausschließlich Zutritt zur Anlieferzone erhalten (Zone 1). Außerdem sollte die Übergabe von Waren so gestaltet sein, dass für Lieferant:innen kein Zugang zu internen Bereichen notwendig ist. [95, p. 25] Das IT-Sicherheitshandbuch empfiehlt, Lieferant:innen analog zum Besucher:innenmanagement zu behandeln. Ihr Zutritt ist klar zu regeln und zu dokumentieren und der Zugang sollte ausschließlich über definierte Empfangsregelungen erfolgen. Eine freie Bewegung im Gebäude ist grundsätzlich nicht zulässig und darf nur nach formaler Freigabe und entsprechender Protokollierung erfolgen. [94, pp. 87-88]

Sind die definierten physischen Maßnahmen und Zutrittsregelungen umgesetzt, müssen diese mindestens jährlich oder anlassbezogen durch die physisch-verantwortliche Stelle in Bezug auf Wirksamkeit und Aktualität überprüft werden. Hierbei sollten insbesondere Zutrittskontrollen und Alarmanlagen gewartet, getestet und stichprobenartig kontrolliert werden, um Schwachstellen frühzeitig zu erkennen und abzustellen. Dies wird idealerweise durch den:die ISB initiiert und kontrolliert. Die Ergebnisse fließen in die Anpassung und kontinuierliche Verbesserung ein.

5.13.2 Schutz vor umgebungsbezogenen Gefährdungen

Mapping - NIS2 Durchführungsverordnung (Punkt 13.2.): Abschnitt 13.2 der NIS2-Durchführungsverordnung verpflichtet Einrichtungen dazu, geeignete Maßnahmen zum Schutz vor physischen und umgebungsbezogenen Gefährdungen zu implementieren, um deren Auswirkungen zu verhindern oder zu minimieren (13.2.1). Die Maßnahmen müssen risikobasiert gemäß der vorangegangenen Risikoanalyse (siehe 2.1 der Verordnung) festgelegt werden. Insbesondere sind folgende Anforderungen zu erfüllen (13.2.2.):

- Schutzmaßnahmen gegen physische und umweltbedingte Bedrohungen müssen entworfen und umge-

setzt werden (a),

- Mindest- und Maximalgrenzwerte für Umgebungsparameter (z.B. Temperatur, Feuchtigkeit, Rauchentwicklung) müssen definiert werden (b),
- Abweichungen von diesen Grenzwerten sind zu überwachen und an zuständiges internes oder externes Personal zu melden (c).

Zusätzlich sind die Schutzmaßnahmen regelmäßig sowie anlassbezogen zu testen, zu überprüfen und gegebenenfalls anzupassen (13.2.3).

Interpretation der Anforderungen: Die Anforderungen betonen, dass Organisationen in der Lage sein müssen, auch bei Ereignissen wie Feuer, Wasser, Stromausfall oder Erdbeben die Sicherheit und Verfügbarkeit ihrer Systeme aufrechtzuerhalten oder schnellstmöglich wiederherzustellen. Für KMUs bedeutet das keine aufwändigen Lösungen, sondern einfache Schutzmaßnahmen wie beispielsweise Rauchmelder und Feuchtigkeitsmesser sowie eine geeignete Standortwahl für Server. Die Festlegung von Grenzwerten (z.B. Temperatur, Feuchtigkeit) sowie deren Überwachung und Auswertung (z.B. durch Sensorik) ist dabei zentral. Regelmäßige Überprüfungen (z.B. durch Haustechnik oder externe Dienstleistende) sorgen für Nachhaltigkeit und Anpassbarkeit der Maßnahmen. So wird verhindert, dass physische Einwirkungen zu ungeplanten Ausfällen oder Datenverlust führen.

Umsetzung im NIS2-ISMS-Framework: Auf Basis der in Kapitel 5.13.1. definierten Sicherheitszonen müssen Schutzmaßnahmen gegen physische und umgebungsbezogene Gefährdungen definiert und dokumentiert werden. Besonders exponierte Gefährdungen für KMUs umfassen unter anderem Feuer, Wasser, Einbruch, Vandalismus sowie klimatische infrastrukturelle Ausfälle. Im IT-Sicherheitshandbuch für KMUs der WKO werden einige bauliche Risiken aufgeführt, welche bei der Planung und Absicherung kritischer Bereiche berücksichtigt werden sollten. Darunter zählen beispielsweise: [94, p. 85]

- Vermeidung von Serverräumen in gefährdeten Bereichen wie Kellern (Wasser), Erdgeschoss (Einbruch/Vandalismus) sowie unter Flachdächern (Regenwasser)
- Umsetzung technischer Schutzmaßnahmen wie Alarmanlagen, Fenstergitter, Wassermelder oder Klimaanlagen

Ergänzend dazu beschreibt der BSI-Umsetzungshinweis zum Baustein INF.1 konkrete Schutzmaßnahmen gegen Umgebungseinflüsse wie: [95]

- Rauch- und Feuermelder sowie automatische Löschsysteme
- Unterbrechungsfreie Stromversorgung und Notstromaggregate
- Klimatisierung und Temperaturüberwachung von Serverräumen

Im Rahmen der Risikoanalyse (siehe Kapitel 5.3.1) sollten relevante Bedrohungen in Bezug auf natürliche (z.B. Hochwasser), technische (z.B. Stromausfälle) sowie menschliche Ursachen (z.B. Brandstiftung oder Sabotage) betrachtet und potenzielle Risiken abgeleitet werden. Auf Basis dieser sollten für relevante Gefährdungen im nächsten Schritt Mindest- und Höchstwerte (z.B. Temperatur, Luftfeuchtigkeit) sowie Alarmierungs- und Eskalationsschwellen festgelegt und dokumentiert werden. Die Überwachung kann hierbei durch einfache Sensorik (z.B. Thermometer, Wasser- oder Rauchmelder, etc.) erfolgen. Ereignisse, welche außerhalb der definierten Schwellwerte sind, müssen an relevante verantwortliche Stellen (z.B. Haustechnik) gemeldet werden.

Die definierten Schutzmaßnahmen sind im Rahmen einer jährlichen oder anlassbezogenen Überprüfung der physisch-relevanten Stelle in Bezug auf die Wirksamkeit und Funktionalität zu testen. Dies wird idealerweise durch den:die ISB initiiert und kontrolliert. Ergebnisse fließen in die Anpassung sowie kontinuierliche Verbesserung ein.

5.13.3 Versorgungseinrichtungen

Mapping - NIS2 Durchführungsverordnung (Punkt 13.1.): Abschnitt 13.1 verpflichtet Unternehmen dazu, den Ausfall oder die Beeinträchtigung von unterstützenden Versorgungseinrichtungen zu verhindern, um Unterbrechungen, Schäden oder Kompromittierungen von Netzwerk- und Informationssystemen zu vermeiden (13.1.1). Dafür sind (auf Basis der Risikoanalyse gemäß Punkt 2.1 der Verordnung) folgende Maßnahmen erforderlich (13.1.2):

- Schutz der Infrastruktur gegen Ausfälle kritischer Versorgungsleistungen wie Strom, Telekommunikation, Wasser, Gas, Abwasser, Belüftung und Klimatisierung (a),
- Berücksichtigung von Redundanz bei den Versorgungsleistungen (b),
- Schutz strom- und datenführender Leitungen gegen Abhören oder Beschädigung (c),
- Überwachung und Meldung von Störungen der Versorgungsleistungen (d),
- Abschluss von Notfallverträgen für kritische Versorgungen, z.B. Treibstoff für Notstromaggregate (e),
- Sicherstellung der kontinuierlichen Versorgung der Systeme mit Strom, Kühlung, Internet und Telekommunikation sowie regelmäßige Tests und Wartung der Versorgungsketten (f).

Alle Maßnahmen sind regelmäßig zu testen, zu überprüfen und bei Bedarf zu aktualisieren (13.1.3).

Interpretation der Anforderungen: Die Anforderung macht deutlich, dass Betriebssicherheit nicht allein von digitalen Schutzmaßnahmen abhängt, sondern wesentlich durch die physische Infrastruktur und deren stabile Versorgung beeinflusst wird. Für KMUs bedeutet es, dass bereits einfache Maßnahmen zur Absicherung der Stromversorgung (z.B. USV), zur Klimakontrolle (z.B. Klimageräte mit Temperaturalarm) oder zur Absicherung von Internetverbindungen (z.B. Zweitanbindung oder Mobilfunk-Fallback) können die Resilienz im Ernstfall erheblich erhöhen. Kritisch ist auch die Überwachung dieser Systeme, beispielsweise durch einfache Sensorik oder Ausfallmeldungen. Redundanz muss dabei nicht zwangsläufig aufwändig sein und oft reicht bereits eine durchdachte Kombination aus alternativer Stromversorgung und Kommunikationswegen. Entscheidend ist, dass die Versorgungseinrichtungen dokumentiert, regelmäßig getestet und bei Bedarf angepasst wird. Ein besonders zentraler Punkt für KMUs ist darüber hinaus, im Vorfeld entsprechende Notfallverträge mit Energie- oder Kommunikationsdienstleistern abzuschließen, um im Ernstfall schnell und koordiniert reagieren zu können.

Umsetzung im NIS2-ISMS-Framework: Als Grundvoraussetzung müssen hierfür kritische Abhängigkeiten identifiziert sein, um die Betriebsfähigkeit trotz Ausfällen in Versorgungseinrichtungen sicherzustellen. Hierfür muss analysiert werden, welche Versorgungseinrichtungen im Einsatz sind und inwiefern kritischen Assets (gemäß BIA in Kapitel 5.3.1) davon abhängig sind. In dem IT-Sicherheitshandbuch für KMU der WKO sind insbesondere Stromversorgung, Klimatisierung und die Telekommunikation besonders kritisch eingestuft und bedürfen spezifischer Vorkehrungen. [94, pp. 90-91] Im Rahmen der Risikoanalyse (siehe Kapitel 5.3.1) sollten potenzielle Risiken in Bezug auf Stromausfall, Netzausfall, Telekommunikationsausfall sowie Klimaausfall (z.B. Serverüberhitzung) und Wasser und Brände erfasst werden. Auf Basis davon müssen im nächsten Schritt geeignete organisatorische und technische Maßnahmen abgeleitet und dokumentiert werden. Das IT-Sicherheitshandbuch beschreibt beispielsweise folgende Maßnahmen, welche als Basis betrachtet werden können. [94, pp. 90-91]

- **Stromversorgung:**
  - USV insbesondere für kritische Systeme (siehe BIA-Ergebnisse)
  - Notstromaggregate / Ersatzversorgung in Verträgen mit Dienstleister:innen sicherstellen, um längere Ausfälle zu überbrücken
- **Telekommunikation und Internetzugang:**
  - Redundante Internetverbindung (z.B. über Mobilfunk/LTE-Router), um bei Netzausfall hand-

lungsfähig zu bleiben

- Alternative Kanäle (z.B. Mobilfunk) für Kommunikation in Notfällen

Außerdem empfiehlt die WKO im IT-Sicherheitshandbuch, dass KMUs Verträge mit externen Dienstleistenden über beispielsweise Notstromaggregate oder alternative Internetanbindungen abschließen sollten. [94, pp. 90-91] Dabei sollten insbesondere der Leistungsumfang, die Reaktionszeiten (SLA), sowie die Ansprechpartner:innen und die Testmöglichkeiten klar definiert sein (siehe Kapitel 5.7.1) Dies ist besonders im Hinblick auf die Haftungsreduzierung, Ressourcensicherung sowie der Zeitkritik im Ernstfall wichtig vertraglich abzusichern. Wie im Kapitel zuvor thematisiert, müssen hier ebenso Schwellwerte und kontinuierliche Überwachungs- und Alarmierungsmechanismen implementiert werden, um Ausfälle von Versorgungseinrichtungen frühzeitig bemerken und schnellstmöglich handeln zu können. Die Schwellwerte leiten sich hierbei von der durchgeführten BIA inklusive der RTO-Werten ab. USVs dienen in der Regel zur sofortigen Überbrückung beispielsweise eines Totalausfalls der Stromversorgung und treten direkt in Kraft. Das WKO beschreibt hierbei eine Überbrückungszeit von zehn bis fünfzehn Minuten bis dies bestenfalls von einem Notstromaggregat übernommen wird. [94, p. 90] Für die technische Umsetzung eignet sich für KMUs beispielsweise die Open-Source-Lösung „Grafana“, womit können sowohl On-Premise als auch in der Cloud die Schwellwerte in einem Dashboard dargestellt werden. Hierfür können Daten aus verschiedenen Quellen (z.B. SNMP oder MQTT) aggregiert, visualisiert und bewertet werden. Hierbei können bei Abweichungen der Schwellwerte Benachrichtigungsdienste wie E-Mail oder SMS-Gateways angebunden werden. [96] Zusätzlich sollte definiert und dokumentiert werden, wer bei kritischen Abweichungen informiert wird und welche Eskalationsschritte folgen.

Um die Versorgung vor Manipulationen zu schützen, sollten die Strom- und Kommunikationsleitungen sowohl technisch als auch organisatorisch gesichert werden. Im BSI-Umsetzungshinweis wird darauf hingewiesen, dass Verteiler (z.B. Energieversorgung, Telefonie) geordnet, zugänglich und nur durch autorisierte Personen geöffnet werden dürfen. Die Zugriffsmöglichkeiten müssen über differenzierte Schließsysteme und Schlüsselverwaltung gesteuert sein. [95]

Darüber hinaus ist sicherzustellen, dass alle Schutzmaßnahmen zumindest jährlich und anlassbezogen durch die physisch-verantwortliche Stelle regelmäßig getestet, gewartet und bei Bedarf angepasst werden. Dies wird durch den:die ISB initiiert und die Durchführung stichprobenartig auf Einhaltung kontrolliert. Die Ergebnisse fließen in die Anpassung sowie kontinuierliche Verbesserung ein.

5.14 Umsetzungs-Fahrplan zur Einführung des Frameworks

Zur praxisgerechten Einführung des entwickelten ISMS-Frameworks wurde ein strukturierter Umsetzungs-Fahrplan auf hoher Detailebene erarbeitet. Dieser orientiert sich methodisch am bewährten PDCA-Zyklus und soll insbesondere KMUs einen schrittweisen, ressourcenschonenden Einstieg in die Umsetzung der NIS2-Anforderungen ermöglichen. Der Fahrplan adressiert die Themenbereiche der Anlage 3 des NISG 2024, welche im Rahmen dieser Arbeit analysiert, strukturiert und in Maßnahmen überführt wurden.

5.14.1 Planung und Strukturierung

In der ersten Phase (Plan) liegt der Fokus auf der Schaffung strategischer und organisatorischer Grundlagen. Zentrale Voraussetzung ist das formale Commitment der obersten Leitungsebene zur Einführung und kontinuierlichen Weiterentwicklung der Informationssicherheit. Dies erfolgt unter anderem durch die Genehmigung der Informationssicherheitsleitlinie, die Festlegung von Rollen und Verantwortlichkeiten (z.B. Informationssicherheitsbeauftragte:r) sowie die Etablierung eines regelmäßigen Berichtskanals an die oberste Leitungsebene. Diese Maßnahmen adressieren die Anforderungen aus den Themenbereichen Leitungsorgane (siehe Kapitel 5.1), Sicherheitsrichtlinien und Verantwortlichkeiten (siehe Kapitel 5.2) sowie Sicherheit im Personalwesen (siehe Kapitel 5.5.1).

Parallel dazu wird eine Gap-Analyse durchgeführt, um bestehende Sicherheitsmaßnahmen mit den Anforderungen der Anlage 3 des NISG abzugleichen und eine Grundlage zur risikobasierten Priorisierung der Handlungsfelder zu schaffen (Überwachung der Einhaltung von Vorgaben; siehe Kapitel 5.3.3). Ergänzend erfolgt eine erste BIA und Risikoanalyse zur Identifikation kritischer Geschäftsprozesse und möglicher Bedrohungen (Risikomanagementrichtlinie und -prozess; siehe Kapitel 5.3.1). Im Rahmen dieser Tätigkeiten werden auch alle relevanten physischen und digitalen Assets dokumentiert und klassifiziert (Inventarisierung und Klassifikation von Vermögenswerten; siehe Kapitel 5.4.1 und 5.4.2).

Darauf aufbauend werden zentrale themenspezifische Sicherheitsrichtlinien entwickelt, etwa zur Zugriffssteuerung, Schwachstellenmanagement oder Lieferkettensicherheit (siehe beispielsweise Kapitel 5.8, 5.9.3 und 5.7.1). Parallel dazu erfolgt die Definition erster KPIs, um die spätere Wirksamkeit von Maßnahmen systematisch erfassen zu können (siehe Kapitel 5.3.2).

5.14.2 Umsetzung der Kernmaßnahmen

In der zweiten Phase (Do) wird die Umsetzung der zuvor definierten Maßnahmen konkret vorangetrieben. Hier erfolgt unter anderem die operative Umsetzung technischer und organisatorischer Maßnahmen gemäß den priorisierten Handlungsfeldern. Zum Beispiel Zugriffskontrollmechanismen (siehe Kapitel 5.8), Überwachungs- und Protokollierungslösungen (siehe Kapitel 5.11.2), Schwachstellenmanagement (siehe Kapitel 5.9.3) sowie Backup- und Wiederherstellungsstrategien (siehe Kapitel 5.12.2). Weitere Maßnahmen betreffen den sicheren Umgang mit Assets (siehe Kapitel 5.4.3 und 5.4.4), den Schutz vor bösartiger Software (siehe Kapitel 5.9.10.) sowie die Umsetzung von Netzwerksicherheitsmaßnahmen (siehe Kapitel 5.9.8, 5.9.9 und 5.10).

Ergänzend werden Awareness-Schulungen und Sensibilisierungsmaßnahmen eingeführt, insbesondere für sicherheitskritische Rollen wie Administrator:innen oder Dienstleister:innen mit Systemzugriff, womit die Themenbereiche Personalwesen (siehe Kapitel 5.5.1) und Cyberhygiene und Schulungen (siehe Kapitel 5.5.2) abgedeckt werden. Auch das Sicherheitsvorfallsmanagement inklusive Meldewegen, Eskalationsprozessen und Reaktionsmechanismen wird in dieser Phase etabliert (siehe Kapitel 5.11).

5.14.3 Überwachung und Bewertung

In der dritten Phase (Check) liegt der Fokus auf der Überprüfung der Effektivität und Konformität der umgesetzten Maßnahmen. Hierbei werden die zuvor definierten KPIs zur Erfolgskontrolle genutzt (siehe Kapitel 5.3.2). Die Bewertung erfolgt im Rahmen regelmäßiger interner Überprüfungen, z.B. durch die sicherheitsverantwortliche Stelle oder stichprobenartige Selbstprüfungen (siehe Kapitel 5.3.3). Ergänzend finden unabhängige Überprüfungen (siehe Kapitel 5.3.4) und Lessons Learned nach Vorfällen (siehe Kapitel 5.11.6) statt. Die dabei gewonnenen Erkenntnisse werden strukturiert dokumentiert und im Rahmen von Management-Reviews aufbereitet. Damit fließen die Bewertungen nicht nur in die Berichtspflicht gegenüber der Leitungsebene ein (siehe Kapitel 5.1.1), sondern bilden auch die Grundlage für fundierte Weiterentwicklungsmaßnahmen im nächsten Zyklusabschnitt.

5.14.4 Anpassung und kontinuierliche Verbesserung

Die vierte Phase (Act) thematisiert die kontinuierliche Verbesserung des ISMS. Aufbauend auf den Ergebnissen aus internen und externen Überprüfungen, Lessons Learned aus Vorfällen sowie der Bewertung der KPIs, werden bestehende Prozesse und Sicherheitsrichtlinien sowie Maßnahmen gezielt weiterentwickelt.

Dies umfasst unter anderem die Aktualisierung von Sicherheitsdokumenten, das Nachschärfen von Maßnahmenplänen sowie die systematische Nachverfolgung und Umsetzung identifizierter Korrekturmaßnahmen, beispielsweise durch Sicherheitstests oder das Patchmanagement (siehe Kapitel 5.9.4 und 5.9.5). Zudem ist es ratsam, die Gap-Analyse in regelmäßigen Intervallen zu wiederholen, um den aktuellen Reifegrad zu bewerten und weitere Optimierungspotenziale zu identifizieren. Damit wird der PDCA-Zyklus geschlossen und als Regelprozess im KMU etabliert.

6 Validierung des entwickelten Frameworks

Um unter anderem die Praxistauglichkeit, Struktur sowie den Inhalt testen zu können, wurde das Framework mit zwei Fachpersonen in Form von Kurzinterviews und einem standardisierten Fragebogen evaluiert und validiert. Bei den zwei befragten Personen handelt es sich um einerseits um eine:n Informationssicherheitsbeauftragte:n in einem produzierenden KMU sowie einem:einer Unternehmensberater:in mit langjähriger Beratungspraxis im Bereich ISMS sowie regulatorischen Anforderungen (insbesondere NIS2)

Der standardisierte Fragebogen umfasste folgende Fragen:

1. Verständlichkeit
    - Wie beurteilen Sie die grundsätzliche Verständlichkeit und Struktur des vorgestellten ISMS-Frameworks für KMUs?
    - Welche Elemente waren für Sie besonders eingängig, und gab es Stellen, die aus Ihrer Sicht erklärungsbedürftig oder unklar waren?
2. Umsetzbarkeit
    - aInwieweit erscheint Ihnen das Framework für KMUs mit begrenzten Ressourcen realistisch umsetzbar, insbesondere hinsichtlich personeller und finanzieller Aufwände?
    - Gibt es Maßnahmen, die aus Ihrer Sicht zu komplex oder zu voraussetzungsvoll sind?
3. Praxisnutzen
    - Welche Inhalte im Framework empfinden Sie als besonders hilfreich oder relevant?
    - Was hat aus Ihrer Sicht echten Mehrwert für die Praxis?
4. Vollständigkeit
    - Fehlen im Framework Inhalte oder Maßnahmen zur Umsetzung der NIS2-Anforderungen?
    - Falls ja: Welche Ergänzungen schlagen Sie vor?
5. Priorisierung und Einstiegshilfen
    - Erhalten Anwender:innen Ihres Erachtens ausreichend Orientierung, welche Maßnahmen zuerst umzusetzen sind?

6. Unterstützungsbedarf
    - Welche weiteren Unterstützungsangebote (z.B. Toolsets, Schulungen, Vorlagen) würden die Umsetzung des Frameworks in der Praxis erleichtern?
7. Gesamtbeurteilung
    - Würden Sie das Framework weiterempfehlen oder selbst einsetzen? Warum (nicht)?

6.1 Kurzinterview mit Person A - Informationssicherheitsbeauftragte:r in einem KMU

Verständlichkeit: Die interviewte Person A beurteilt das Framework als grundsätzlich verständlich und klar strukturiert. Die Inhalte seien nachvollziehbar aufgebaut und auch ohne tiefgehende regulatorische Kenntnisse zugänglich. Dies ist insbesondere für KMUs ohne juristisches oder normatives Vorwissen von Bedeutung. Besonders eingängig wurden die Vorlagen und Musterdokumente bewertet, da sie praxisnah erläutern, wie Maßnahmen konkret umzusetzen sind. Kritisch angemerkt wurden jedoch bestimmte unkonkrete und abstrakte Begriffe in Anforderungen wie „angemessen“ oder „geeignet“, da diese in der Praxis Interpretationsspielräume lassen. Ohne ergänzende Beispiele oder Erläuterungen sei es schwierig, den erforderlichen Umsetzungsgrad richtig einzuschätzen.

Umsetzbarkeit: Das Framework wird als grundsätzlich realisierbar eingeschätzt, insbesondere durch den strukturierten Fahrplan, der eine klare Reihenfolge vorgibt und damit Orientierung für KMUs mit eingeschränkten Ressourcen bietet. Kritikpunkte betrafen die Definition des Umfangs einzelner Anforderungen, etwa bei der Asset-Inventarisierung. Die interviewte Person A regte an, hier klarere Abgrenzungen vorzunehmen, um eine realistische Einschätzung des Umsetzungsaufwands zu ermöglichen.

Praxisnutzen: Als besonders hilfreich wurden die bereitgestellten Vorlagen und der Umsetzungsfahrplan genannt. Diese ermöglichen eine praxisnahe Orientierung und strukturierte Umsetzung auch ohne externe Beratung. Die Materialien und der methodische Aufbau des Frameworks schaffen eine solide Grundlage für KMUs und bieten echten operativen Mehrwert. Besonders hervorgehoben wurde die Möglichkeit, auch ohne vertiefte regulatorische Expertise Maßnahmen implementieren zu können.

Vollständigkeit: Explizite Inhalte, die fehlen, wurden nicht benannt. Allerdings wurde angedeutet, dass es bei der praktischen Anwendung zu Unklarheiten kommen kann, insbesondere bei der Auslegung generischer

Anforderungen und Formulierungen. Empfohlen wurden präzisere Hinweise und Beispiele, insbesondere bei unkonkreten und abstrakten Begriffen, um die einfachere Umsetzung sicherzustellen.

Priorisierung und Einstiegshilfen: Der Fahrplan zur Umsetzung wurde als sehr nützlich bewertet. Er bietet eine klare Struktur und Reihenfolge, an der sich KMUs effektiv orientieren können.

Unterstützungsbedarf: Gewünscht wurden zusätzliche Erläuterungen und Beispiele zu unkonkreten Begriffen und Maßnahmen. Dies würde die praktische Umsetzbarkeit erhöhen. Der Bedarf an Toolsets oder Schulungen wurde implizit durch den Hinweis auf den Mehrwert von Vorlagen und Orientierungshilfen angedeutet.

Gesamtbeurteilung: In der Gesamtbewertung wird das Framework als geeignete Grundlage für KMUs eingeschätzt. Die interviewte Person A würde das Framework in der Praxis empfehlen. Für komplexere Umsetzungen wird der ergänzende Einbezug externer Beratung als sinnvoll erachtet.

6.2 Kurzinterview mit Person B - Unternehmensberater:in im Bereich Informationssicherheit

Verständlichkeit: Die interviewte Person B lobt die Struktur des Frameworks entlang der Themenbereiche der Anlage 3 des NISG 2024 und die Ableitung der Anforderungen auf Basis der NIS2-Durchführungsverordnung. Diese inhaltliche Orientierung wurde als nachvollziehbar und logisch empfunden, auch vor dem Hintergrund einer noch ausstehenden nationalen Gesetzgebung. Die Kombination aus struktureller Klarheit, inhaltlicher Konkretisierung und methodischer Unterstützung wurde als wesentliches Merkmal hervorgehoben. Keine explizit unklaren Stellen wurden genannt, jedoch wurde die Notwendigkeit betont, Dokumentations- und Nachweispflichten stärker in den Vordergrund zu rücken.

Umsetzbarkeit: Die Vorlagen wurden als praxisnah und gut einsetzbar bewertet. Sie erleichtern insbesondere KMUs die Umsetzung regulatorischer Anforderungen. Die Notwendigkeit zur durchgängigen sowie prüfungstauglichen Dokumentation wird als herausfordernd, aber essenziell für die spätere Nachweiserbringung dargestellt. Unternehmen sollen frühzeitig dokumentieren, wo Abweichungen bestehen, um Auditor:innen ein nachvollziehbares Bild zu liefern.

Praxisnutzen: Die Gap-Analyse wurde sowohl zur Bestandsaufnahme als auch als Ausgangspunkt (für die weitere Arbeit) für eine Reifegradbewertung als besonders wertvoll hervorgehoben. Die systematische Erfassung und Bewertung von Lücken durch die Gap-Analyse-Fragen bieten laut der interviewten Person echten Mehrwert für die Auditvorbereitung und strategische Weiterentwicklung des ISMS.

Vollständigkeit: Die formale Deckung mit regulatorischen Anforderungen wird grundsätzlich als gegeben angesehen. Jedoch fehlt eine explizite Verankerung der Vorgehensweise im Umgang mit begründeten Abweichungen. Empfohlen wurde die Integration von Beispielen zur Dokumentation von bewussten Abweichungen, zeitlichen Verschiebungen und risikobasierten Kompensationsmaßnahmen.

Priorisierung und Einstiegshilfen: Die vorhandene Struktur wird als hilfreich für die Orientierung beschrieben, insbesondere durch die thematische Gliederung entlang des NISG. Der Ausbau der Gap-Analyse wird als zukünftige Möglichkeit zur gezielten Priorisierung empfohlen.

Unterstützungsbedarf: Neben bestehenden Vorlagen wird angeregt, zusätzliche Hilfsmittel bereitzustellen, insbesondere zur Dokumentation von Abweichungen und temporären Maßnahmen. Die strukturierte Erfassung von Nachweisen entlang der regulatorischen Themenfelder (z.B. die Themenbereiche der NISG 2024) wurde als wesentlich betont.

Gesamtbeurteilung: Das Framework wird als professionelles und anschlussfähiges Instrument für KMUs bewertet, das insbesondere bei prüfungstauglicher Umsetzung einen hohen Nutzen entfaltet. Die interviewte Person B empfiehlt den Einsatz des Frameworks und sieht es als geeignete Grundlage für eine systematische Auseinandersetzung mit der NIS2-Richtlinie. Die Weiterentwicklung der Gap-Analyse hin zu einem Reifegradmodell wird als zukunftsweisender Schritt empfohlen.

7 Diskussion

Im folgenden Kapitel werden sowohl die Erkenntnisse aus der Validierung sowie aus der Selbstreflexion bei der Entwicklung des Framework zusammengefasst und Optimierungspotenziale identifiziert.

7.1 Methodische und konzeptionelle Erfahrungen

Die Entwicklung des Frameworks stellte vor allem zu Beginn eine methodische Herausforderung dar. Die inhaltlichen Überschneidungen zwischen der NIS2-Richtlinie, der NIS2-Durchführungsverordnung und der Anlage 3 des österreichischen NISG 2024 erschwerten eine klare Strukturierung. Nach sorgfältiger Abwägung wurde die Gliederung entlang der 13 Themenbereiche der Anlage 3 gewählt, da diese den erwarteten rechtlichen Rahmen auf nationaler Ebene abbildet und somit für betroffene KMUs in Österreich eine tragfähige Orientierung bietet.

Eine weitere Herausforderung lag in der Übersetzung abstrakter Begriffe wie „angemessen“ oder „geeignet“ in konkrete, verständliche Handlungsempfehlungen. Um diese Unschärfen zu vermeiden, wurden möglichst präzise Formulierungen und praxisnahe Beispiele eingesetzt. Dennoch zeigte sich insbesondere in der Validierung mit Person A, dass einzelne Anforderungen aus Sicht der Praxis (z.B. bei Rollen in der IT-Abteilung oder Asset-Inventarisierung) weiterhin schwer greifbar bleiben.

Ein methodisch wirksames Element war die Integration eines priorisierten Fahrplans, welcher sich am PDCA-Zyklus orientiert. Dieser stellt sicher, dass die grundlegenden ISMS-Prinzipien berücksichtigt werden und gleichzeitig ein nachvollziehbarer Einstieg für KMUs geschaffen wird. Themen wie Einholung des Management Commitments, Festlegung der Rollen und Verantwortlichkeiten sowie Etablierung eines Risikomanagements inklusive Asset-Management wurden bewusst als Startpunkte gewählt, da sie als Fundament für jede weitere Maßnahme dienen.

7.2 Weiterführende Erkenntnisse und Beitrag für KMUs

Ein zentrales Ziel war es, das Framework praxisnah und ressourcenschonend zu gestalten. Besonders die bereitgestellten Vorlagen und Musterdokumente haben sich in den Interviews mit beiden Personen als wirkungsvoll erwiesen. Sie ermöglichen es KMUs, ohne tiefgehende Expertise grundlegende Anforderungen systematisch umzusetzen.

Gleichzeitig wurde deutlich, dass einige Inhalte, insbesondere im technisch-organisatorischen Bereich, klarer formuliert und stärker kontextualisiert werden sollten. Auch das Thema Nachweisdokumentation wurde laut dem Interview mit Person B nicht ausreichend adressiert. In zukünftigen Versionen könnten strukturierte Hilfsmittel wie Checklisten oder Vorlagen zur Begründung risikobasierter Abweichungen einen wichtigen Mehrwert bieten. Darüber hinaus zeigte sich im Verlauf der Arbeit, dass die laufende Verwaltung eines ISMS, beispielsweise im Hinblick auf Aufgabenverfolgung, Fristenkontrolle und die revisionssichere Dokumentation von Umsetzungsständen, für viele KMUs eine nicht zu unterschätzende Herausforderung darstellt. Der organisatorische Aufwand steigt insbesondere dann, wenn keine zentrale Koordination über geeignete Tools möglich ist. Da spezialisierte ISMS-Softwarelösungen für KMUs oft zu kostspielig oder funktional überdimensioniert sind, wäre eine vertiefte Auseinandersetzung mit niederschwelligen Alternativen, beispielsweise auf Basis gängiger Office-Anwendungen oder frei verfügbarer Open-Source-Lösungen, sinnvoll gewesen.

Rückblickend wäre zudem ein stärker iterativer Entwicklungsansatz des Frameworks sinnvoll gewesen. Weitere Rückmeldeschleifen mit Expert:innen (z.B. Vertreter:innen aus KMUs sowie Berater:innen) hätten es ermöglicht, sprachliche Unschärfen früher zu erkennen und unternehmensspezifische Anforderungen gezielter zu berücksichtigen.

Ein frühzeitiger Test des Frameworks in einem realen KMU-Kontext hätte wertvolle Einblicke in die tatsächliche Anwendbarkeit und mögliche Hindernisse bei der operativen Umsetzung geliefert. Gerade vor dem Hintergrund, dass das Thema Informationssicherheit in vielen KMUs weder strategisch noch personell umfassend verankert ist, stellt sich die Frage, wie das Framework in Organisationen aufgenommen wird, welche bislang wenig Berührungspunkte mit Sicherheitsanforderungen hatten. Auch wenn die Fachpersonen der Validierung das Framework als verständlich und strukturiert bewerten, bleibt offen, ob diese Einschätzung auch für weniger erfahrene Anwender:innen des Frameworks ohne spezifisches Vorwissen

gilt. Die subjektive Wahrnehmung von Komplexität ist hierbei als subjektiv zu, da nicht alle sicherheitsverantwortlichen Personen insbesondere in einem KMU das gleiche Fachwissen aufweisen können.

7.3 Umsetzungstauglichkeit und Rückmeldungen aus der Praxis

Im Verlauf der Arbeit wurde deutlich, dass viele KMUs über keine strukturierten Ansätze für Informationssicherheit verfügen und sicherheitsrelevante Aufgaben häufig informell oder zusätzlich durch IT-Personal übernommen werden. Gleichzeitig fehlt es in vielen Fällen an klarer Unterstützung durch die oberste Leitungsebene, wodurch die Wirksamkeit von Sicherheitsmaßnahmen erheblich eingeschränkt werden kann. Die persönliche Haftung der obersten Leitungsebene im Rahmen der NIS2 könnte künftig als Verstärker wirken, um Informationssicherheit als strategisches Thema zu verankern.

Im Vergleich zu bestehenden Standards wie ISO 27001 bietet das Framework einen niedrigschwelligen Zugang zur Umsetzung von NIS2-Anforderungen in KMUs. Es verzichtet bewusst auf komplexe Tiefe typischer Managementsysteme und orientiert sich stattdessen an der tatsächlichen Umsetzbarkeit unter begrenzten Ressourcen. Der kombinierte Einsatz von thematischer Struktur, Fahrplan, Gap-Analyse und Dokumentvorlagen stellt eine praxisgerechte Alternative zu klassischen ISMS-Modellen dar und kann einen Beitrag zur Erhöhung der Cyberresilienz in KMUs leisten.

8 Conclusio

Ziel dieser Arbeit war die Entwicklung eines praxistauglichen ISMS-Frameworks für österreichische KMUs mit Fokus auf NIS2. Ausgangspunkt bildete die zentrale Forschungsfrage:
„Wie kann ein auf den 13 Themenbereichen der Anlage 3 NISG 2024 basierendes ISMS-Framework für österreichische KMUs gestaltet werden, sodass es sämtliche in Artikel 21 Absatz 2 der NIS2-Richtlinie genannten Mindestanforderungen abdeckt?“

Zur Beantwortung dieser Forschungsfrage wurde ein strukturierter methodischer Ansatz gewählt. Zu Beginn wurde ein vollständiges Mapping der Anforderungen der NIS2-Durchführungsverordnung auf die Themenbereiche der Anlage 3 des NISG 2024 durchgeführt und in der Datei der NIS2 Framework Analyse dokumentiert. Dieses Mapping diente als systematische Referenz für die inhaltliche Abdeckung der NIS2-Anforderungen. Ergänzend wurde eine gezielte Recherche zur aktuellen Sicherheitslage und zum Reifegrad europäischer und insbesondere österreichischer KMUs durchgeführt, um deren spezifische Herausforderungen in die Framework-Gestaltung einfließen zu lassen.

Das daraus entwickelte Framework umfasst neben strukturierten Maßnahmenvorschlägen auch eine Gap-Analyse, praxisnahe Umsetzungshilfen sowie Dokumentenvorlage. Ein priorisierter Fahrplan auf Basis des PDCA-Zyklus soll KMUs dabei unterstützen, zentrale Einstiegspunkte und Abhängigkeiten zwischen Themenbereichen zu erkennen und schrittweise zu bearbeiten.

Die qualitative Validierung mit zwei Fachpersonen aus der Praxis bestätigte die Vollständigkeit und grundsätzliche Anwendbarkeit des Frameworks. Die Rückmeldungen zeigten, dass die Struktur logisch aufgebaut ist, die Inhalte überwiegend nachvollziehbar formuliert sind und das Framework eine hilfreiche Orientierung für Unternehmen ohne tiefgehende Vorkenntnisse im Informationssicherheitsmanagement bietet. Gleichzeitig wurde darauf hingewiesen, dass manche Maßnahmen und Umsetzungshilfen konkreter formuliert werden sollten und das Thema Nachweisdokumentation künftig noch stärker thematisiert werden muss.

Insgesamt kann festgehalten werden, dass die Forschungsfrage beantwortet wurde. Das entwickelte Framework erfüllt die in Artikel 21 Absatz 2 der NIS2-Richtlinie geforderten Mindestanforderungen, ist an der voraussichtlichen nationalen Rechtslage gemäß NISG 2024 ausgerichtet und berücksichtigt die spezifischen Rahmenbedingungen österreichischer KMUs. Es stellt damit eine fundierte Grundlage dar, welcher als Ausgangspunkt für die praktische Umsetzung und für weiterführende Entwicklungen genutzt werden kann.

8.1 Weiterführende Arbeiten

Trotz der positiven Bewertung durch die Interviews bestehen gewisse Einschränkungen hinsichtlich der Tiefe, der Übertragbarkeit und der praktischen Testung des entwickelten Frameworks. Die Validierung stützte sich auf zwei Interviews und deckt damit nur einen kleinen Teil der potenziellen Anwender:innen ab. Eine breitere empirische Validierung unter Einbezug weiterer KMUs unterschiedlicher Branchen und Größenordnungen erscheint daher als sinnvoller nächster Schritt.

Darüber hinaus wurde das Framework bewusst in Teilen allgemein gehalten, um eine flexible Anwendung zu ermöglichen. Gerade im technisch-organisatorischen Bereich wurden in der Rückmeldung jedoch punktuell konkretere Handlungshilfen eingefordert. Auch der Aspekt der ISMS-Verwaltung wurde bislang nicht im Detail adressiert. Viele KMUs stehen vor der Herausforderung, Aufgabenverteilung, Einhaltung von Fristen und Dokumentation sowie Nachweise ohne professionelle ISMS-Tools zu organisieren, da diese oftmals zu teuer oder zu komplex sind. Eine Auseinandersetzung mit praxistauglichen Alternativen, etwa auf Basis vorhandener Office-Anwendungen oder leichtgewichtiger Open-Source-Tools, sollte daher in einer Weiterentwicklung des Frameworks detaillierter berücksichtigt werden.

Empfohlen wird zudem eine praktische Pilotierung und Validierung in ausgewählten KMUs, um die Umsetzbarkeit im operativen Alltag zu evaluieren und Verbesserungspotenziale systematisch zu erfassen. Außerdem könnte die bestehende Gap-Analyse zu einem einfachen Reifegradmodell weiterentwickelt werden. Auf diese Weise ließen sich Fortschritte besser erfassen und gezielte Handlungsprioritäten ableiten.

Abbildungsverzeichnis

Tabellenverzeichnis

Akronyme

BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
ENISA	European Union Agency for Cybersecurity
ISMS	Informationssicherheitsmanagementsystem
IT-Grundschutz	IT-Grundschutz-Kompendium des BSI
KMU	Kleine und mittlere Unternehmen
MFA	Multi-Faktor-Authentifizierung
NIS2	Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU
NISG 2024	Netz- und Informationssystemsicherheitsgesetz 2024
NIST	National Institute of Standards and Technology
PDCA	Plan-Do-Check-Act

Literatur

[1] European Union Agency for Cybersecurity (ENISA), „Cybersecurity for SMEs: Challenges and Recommendations“, European Union Agency for Cybersecurity (ENISA), Techn. Ber., Juni 2021, (besucht am 14. 12. 2024). DOI: 10.2824/770352. Adresse: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf.

[2] Europäisches Parlament und Rat, *Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union*, Dez. 2022. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555.

[3] Wirtschaftskammer Österreich (WKO), *NISG 2024 im Nationalrat nicht beschlossen*, (besucht am 14. 12. 2024), Apr. 2024. Adresse: https://www.wko.at/it-sicherheit/nisg-2024-im-nationalrat-nicht-beschlossen.

[4] Republik Österreich Bundesministerium für Inneres (BMI), „Ministerialentwurf – Bundesgesetz über die Gewährleistung eines hohen Cybersicherheitsniveaus (NISG 2024)“, Parlament der Republik Österreich, Techn. Ber., Apr. 2024. Adresse: https://www.parlament.gv.at/dokument/XXVII/ME/326/fname_1621122.pdf.

[5] Europäische Kommission, *Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Bekannt gegeben unter Aktenzeichen K(2003) 1422)*, Mai 2003. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361.

[6] Europäisches Parlament und Rat, *Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*, Juli 2016. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148.

[7] heyData, *5 wichtige Änderungen von NIS1 zu NIS2*, (besucht am 10. 2. 2025), Feb. 2025. Adresse: https://heydata.eu/magazin/5-wichtige-aenderungen-von-nis1-zu-nis2.

[8] Wirtschaftskammer Österreich (WKO), *Cybersicherheits-Richtlinie NIS 2 – Neue Regelungen für mehr Cybersicherheit in der EU*, (besucht am 10. 2. 2025), Feb. 2025. Adresse: https://www.wko.at/it-sicherheit/nis2-uebersicht.

[9] Republik Österreich Bundesministerium für Inneres (BMI), „Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird“, Parlament der Republik Österreich, Techn. Ber., Apr. 2024. Adresse: https://www.parlament.gv.at/dokument/XXVII/ME/326/fname_1621118.pdf.

[10] Europäische Kommission, *Durchführungsverordnung (EU) 2024/2690 der Kommission vom 25. Juli 2024 zur Festlegung technischer und organisatorischer Anforderungen gemäß Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555*, Juli 2024. Adresse: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402690.

[11] European Union Agency for Cybersecurity (ENISA), „Implementation guidance - On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures“, European Union Agency for Cybersecurity (ENISA), Techn. Ber., Nov. 2024. Adresse: https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation%20guidance%20on%20security%20measures_FOR%20PUBLIC%20CONSULTATION.pdf.

[12] Zaidatulnajla Hamdi, Azah Anir Norman, Nurul Nuha Abdul Molok und Farkhondeh Hassandoust, „A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors“, *Journal of Physics: Conference Series*, Jg. 1339, S. 012 103, 2019. DOI: 10.1088/1742-6596/1339/1/012103. Adresse: https://iopscience.iop.org/article/10.1088/1742-6596/1339/1/012103/pdf.

[13] International Organization for Standardization und International Electrotechnical Commission, „ISO /IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements“, International Organization for Standardization (ISO), Techn. Ber., 2022.

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber., Feb. 2021. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf.

[15] Hamed Taherdoost, „Understanding Cybersecurity Frameworks and Information Security Standards — A Review and Comprehensive Overview“, *Electronics*, Jg. 11, Nr. 14, S. 2181, 2022. DOI: 10.3390/electronics11142181. Adresse: https://www.mdpi.com/2079-9292/11/14/2181.

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI-Standards: IT-Grundschutz und weitere Standards zur Informationssicherheit*, (besucht am 20. 2. 2025), 2024. Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html.

[17] Celia Paulsen und Patricia Toth, „Small Business Information Security: The Fundamentals“, National Institute of Standards und Technology (NIST), U.S. Department of Commerce, Techn. Ber. NISTIR 7621 Revision 1, Nov. 2016. Adresse: https://doi.org/10.6028/NIST.IR.7621r1.

[18] Neeshe Khan, Steven Furnell, Maria Bada, Matthew Rand und Jason R.C. Nurse, „Investigating the experiences of providing cyber security support to small- and medium-sized enterprises“, *Computers & Security*, Jg. 154, S. 104 448, 2025. DOI: 10.1016/j.cose.2025.104448. Adresse: https://doi.org/10.1016/j.cose.2025.104448.

[19] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, „SMEs and High Inflation – Summary Report“, Publications Office of the European Union, Techn. Ber., Dez. 2023. DOI: 10.2873/290624. Adresse: https://single-market-economy.ec.europa.eu/document/download/3c847b9c-2020-4e99-a676-38bf3ff9ffba_en?filename=Summary+report_v3.1.pdf.

[20] Alina Salzberger, „Cyber Risk Awareness of German SMEs: An Empirical Study on the Influence of Biases and Heuristics“, *Zeitschrift für die gesamte Versicherungswissenschaft*, Jg. 113, S. 55–104, 2024. DOI: 10.3790/zverswiss.2024.1430701. Adresse: https://www.researchgate.net/publication/379721298_Cyber_Risk_Awareness_of_German_SMEs_An_Empirical_Study_on_the_Influence_of_Biases_and_Heuristics.

[21] Martina Neri, Federico Niccolini und Rosario Pugliese, „Assessing SMEs' Cybersecurity Organizational Readiness: Findings from an Italian Survey“, *Online Journal of Applied Knowledge Management*, Jg. 10, Nr. 2, S. 1–22, 2022. DOI: 10.36965/OJAKM.2022.10(2)1-22. Adresse: https://www.researchgate.net/publication/363741932_Assessing_SMEs'_cybersecurity_organizational_readiness_Findings_from_an_Italian_survey.

[22] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2024“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber., Okt. 2024. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5.

[23] Marc K. Peter, Katja Dörlemann, Kristof Hertig, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian und Nicole Wettstein, „Cyberstudie 2024: IT-Sicherheit in Schweizer KMU, bei IT-Dienstleistungsunternehmen und in der Schweizer Bevölkerung“, digitalswitzerland; FHNW; Die Mobiliar; Swiss Internet Security Alliance (SISA); Allianz Digitale Sicherheit Schweiz (ADSS); SATW; YouGov Schweiz, Techn. Ber., Nov. 2024. DOI: 10.13140/RG.2.2.25032.12803. Adresse: https://www.researchgate.net/publication/385776189.

[24] Bjarne Lill, Clemens Sauerwein, Alexander Zeisler, Carina Hochstrasser und Nico Mexis, „Assessing Cybersecurity Readiness Among SME“, in *Proceedings of the 27th International Conference on Enterprise Information Systems (ICEIS 2025) - Volume 2*, SCITEPRESS – Science und Technology Publications, 2025, S. 253–263, ISBN: 978-989-758-749-8. DOI: 10.5220/0013353400003929. Adresse: https://www.scitepress.org/Papers/2025/133534/133534.pdf.

[25] Theresa Hirsch, Johanna Berndorfer, Willibald Krenn und Florian Lorber, „CyberGuide 2024 – Anforderungen von KMU zur Cybersicherheit“, Bundesministerium für Finanzen (BMF), Österreich, Techn. Ber., Okt. 2024. Adresse: https://www.bmf.gv.at/dam/jcr:d2551aec-9368-4bc7-9d6c-40f972e34cca/CyberGuide_Dez2024_barrierefrei.pdf.

[26] Allianz Commercial, „Allianz Risk Barometer 2025 – Identifying the major business risks for 2025“, Allianz Global Corporate Specialty SE, Techn. Ber., Jan. 2025. Adresse: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf.

[27] VdS Schadenverhütung GmbH, *VdS 10000:2025-01 – Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU) – Anforderungen*, (besucht am 14. 3. 2025). Adresse:

https://vds.de/kompetenzen/cyber-security/vds-10000-die-neue-version-2025.

[28] SWI-Informationssicherheit für den Mittelstand GmbH, *Was ist CISIS12?*, (besucht am 14. 3. 2025). Adresse: https://cisis12.de/was-ist-cisis12/.

[29] International Electrotechnical Commission (IEC), *ISO/IEC 27001-HBK - Information Security Management Systems - A practical guide for SMEs*, (besucht am 14. 3. 2025). Adresse: https://webstore.iec.ch/en/publication/94641.

[30] National Institute of Standards and Technology (NIST), „NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide“, U.S. Department of Commerce, National Institute of Standards und Technology, Techn. Ber. NIST SP 1300, Feb. 2024. DOI: 10.6028/NIST.SP.1300. Adresse: https://doi.org/10.6028/NIST.SP.1300.

[31] Frederik Mijnhardt, Thijs Baars und Marco Spruit, „Organizational Characteristics Influencing SME Information Security Maturity“, *Journal of Computer Information Systems*, Jg. 56, Nr. 2, S. 106–115, 2016. DOI: 10.1080/08874417.2016.1117369. Adresse: https://doi.org/10.1080/08874417.2016.1117369.

[32] Shekhar Pawar und Hemant Palivela, „LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)“, *International Journal of Information Management Data Insights*, Jg. 2, S. 100 080, 2022. DOI: 10.1016/j.jjimei.2022.100080. Adresse: https://www.researchgate.net/publication/360754201_LCCI_A_framework_for_least_cybersecurity_controls_to_be_implemented_for_small_and_medium_enterprises_SMEs.

[33] European DIGITAL SME Alliance, „SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management“, Small Business Standards (SBS), Techn. Ber., Feb. 2024. Adresse: https://sbs-sme.eu/wp-content/uploads/2024/02/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-2.pdf.

[34] Thomas Joswig und Walter Kurz, „Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany“, *Journal of Next-Generation Research 5.0*, Jg. 1, Nr. 3, S. 1–21, März 2025, ISSN: 3075-2868. DOI: 10.70792/jngr5.0.v1i3.99. Adresse: https://www.researchgate.net/publication/389785119_Empirical_Analysis_of_

NIS2_Adoption_in_EU_SMEs_Challenges_for_Critical_Infrastructure_in_Germany.

[35] Eloisa Gonçalves da Silva Torlig, Pedro Carlos Resende Junior, Ricardo Ken Fujihara, Lana Montezano und Gisela Demo, „Validation Proposal for Qualitative Research Scripts (Vali-Quali)“, *Administração: Ensino e Pesquisa*, Jg. 23, Nr. 1, S. 4–29, 2022, ISSN: 2358-0917. DOI: 10.13058/raep.2022.v23n1.2022. Adresse: https://www.researchgate.net/publication/361211698_Validation_Proposal_for_Qualitative_Research_Scripts_Vali-Quali.

[36] IKARUS Security Software GmbH, *Cyber Security Schecks 2023: Förderung für NIS2-betroffene KMU*, (besucht am 12. 1. 2025), Okt. 2023. Adresse: https://www.ikarussecurity.com/security-news/cyber-security-schecks-2023-foerderung-fuer-nis2-betroffene-kmu/.

[37] Österreichische Forschungsförderungsgesellschaft (FFG), *Cyber Security Schecks 2024*, (besucht am 12. 1. 2025). Adresse: https://www.ffg.at/ausschreibung/cybersecurityschecks2024.

[38] Austria Wirtschaftsservice GmbH (aws), *aws Digitalisierung - spezielle Konditionen/Bedingungen: KMU.Cybersecurity*, (besucht am 12. 1. 2025). Adresse: https://www.aws.at/kmucybersecurity/.

[39] Energie und Tourismus und Wirtschaftskammer Österreich (WKO) Bundesministerium für Wirtschaft, *Förderungsprogramm KMU.DIGITAL*, (besucht am 12. 1. 2025). Adresse: https://www.kmudigital.at/kmudigital/start.html.

[40] Kärntner Wirtschaftsförderungs Fonds (KWF), *Digitalisierungs.IMPULS Förderung für Kleinst-, Klein- und Mittelunternehmen Projektkosten von EUR 5.000,- bis 25.000,-*, (besucht am 12. 1. 2025). Adresse: https://kwf.at/foerderungen/digitalisierungsimpuls/.

[41] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Bundesamt für Sicherheit in der Informationstechnik, Techn. Ber. BSI-TR-02102-1, Jan. 2025. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf.

[42] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Daten auf Festplatten, Datenträgern und Smartphones sicher löschen*, (besucht am 20. 2. 2025), 2025. Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-

und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html.

[43] Plattform Digitales Österreich, *IT-Sicherheitshandbuch für Mitarbeiter*, (besucht am 25. 2. 2025). Adresse: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Handbuecher/IT-Sicherheitshandbuch-fuer-Mitarbeiter.html.

[44] Wirtschaftskammer Österreich (WKO), *Basismaßnahmen der Informationssicherheit für Unternehmen*, (besucht am 25. 2. 2025). Adresse: https://www.wko.at/it-sicherheit/basismassnahmen-informationssicherheit-unternehmen.

[45] Bundesministerium für Inneres (BMI), *Cybersecurity Awareness – Informations- und Sensibilisierungsplattform für Cybersicherheit in Österreich*, (besucht am 25. 2. 2025). Adresse: https://www.cybersecurity-awareness.at/.

[46] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Informationssicherheit für kleine und mittlere Unternehmen (KMU)*, (besucht am 25. 2. 2025). Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html.

[47] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Leichter Einstieg in die Informationssicherheit für KMU*, (besucht am 25. 2. 2025). Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/leichter_Einstieg/leichter_Einstieg_node.html.

[48] Europol, *Cyber Scams: Erkennen und Verhindern von Online-Betrug*, 2024. Adresse: https://www.europol.europa.eu/sites/default/files/documents/at.pdf.

[49] Inc. Red Hat, *Was ist Role-Based Access Control (RBAC)?*, (besucht am 12. 3. 2025). Adresse: https://www.redhat.com/de/topics/security/what-is-role-based-access-control.

[50] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Sichere Passwörter erstellen*, (besucht am 2. 4. 2025). Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html.

[51] IBM Corporation, *Was sind CIS Benchmarks?*, (besucht am 4. 4. 2025). Adresse: https://www.ibm.com/de-de/topics/cis-benchmarks.

[52] Wondershare Recoverit, *Clonezilla: So klonen Sie eine Festplatte mit dem kostenlosen Tool*, (besucht am 4. 4. 2025). Adresse: https://recoverit.wondershare.de/data-backup/clonezilla-clone-disk.html.

[53] Inc. Red Hat, *Kickstart Howto – Red Hat Enterprise Linux 7 Installation Guide*, (besucht am 4. 4. 2025). Adresse: https://docs.redhat.com/de/documentation/red_hat_enterprise_linux/7/html/installation_guide/sect-kickstart-howto.

[54] National Institute of Standards und Technology (NIST), *Common Vulnerability Scoring System (CVSS)*, (besucht am 28. 3. 2025). Adresse: https://nvd.nist.gov/vuln-metrics/cvss.

[55] National Institute of Standards und Technology (NIST), *Statement of Work (SOW)*, (besucht am 10. 4. 2025). Adresse: https://csrc.nist.gov/glossary/term/statement_of_work.

[56] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI TR-03185 – Sicherheitsanforderungen an Anbieter von Telemediendiensten*, (besucht am 15. 4. 2025). Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03185/TR-03185_node.html.

[57] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Technische Richtlinie BSI TR-03185 – Sicherer Software-Lebenszyklus“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber. TR-03185, Aug. 2024. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03185/BSI-TR-03185.pdf.

[58] OWASP Foundation, *OWASP Secure Coding Practices Quick Reference Guide – Version 2.0.1*, Dez. 2022. Adresse: https://github.com/OWASP/secure-coding-practices-quick-reference-guide/releases/tag/v2.0.1.

[59] OWASP Foundation, *Static Code Analysis (SCA)*, (besucht am 15. 4. 2025). Adresse: https://owasp.org/www-community/controls/Static_Code_Analysis.

[60] OWASP Foundation, *Dynamic Application Security Testing (DAST) – OWASP DevSecOps Guideline*, (besucht am 15. 4. 2025). Adresse: https://owasp.org/www-project-devsecops-guideline/latest/02b-Dynamic-Application-Security-Testing.

[61] Michael Powell, John Hoyt, Aslam Sherule und Lynette Wilcox, „Security Segmentation in a Small Manufacturing Environment“, National Institute of Standards und Technology (NIST), Techn. Ber. NIST CSWP 28, Apr. 2023. DOI: 10.6028/NIST.CSWP.28. Adresse: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.28.pdf.

[62] Bundesamt für Sicherheit in der Informationstechnik (BSI), *IT-Grundschutz Schulung: Lektion 3.05 – Strukturanalyse durchführen*, (besucht am 17. 4. 2025). Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_3_Strukturanalyse/Lektion_3_05/Lektion_3_05_node.html.

[63] Cybersecurity und Infrastructure Security Agency (CISA), *Enhanced Visibility and Hardening Guidance for Communications Infrastructure*, (besucht am 17. 4. 2025). Adresse: https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure.

[64] Karen Scarfone, Murugiah Souppaya, Amanda Cody und Angela Orebaugh, „Technical Guide to Information Security Testing and Assessment“, National Institute of Standards und Technology (NIST), Techn. Ber. SP 800-115, Sep. 2008. DOI: 10.6028/NIST.SP.800-115. Adresse: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

[65] ProSec Networks GmbH, *802.1X Network Access Control – Was ist das und wie funktioniert es?*, (besucht am 18. 4. 2025). Adresse: https://www.prosec-networks.com/blog/802-1x-network-access-control/.

[66] Inc. Juniper Networks, *Persistent Sticky MAC Learning*, (besucht am 18. 4. 2025). Adresse: https://www.mist.com/documentation/persistent-sticky-mac-learning/.

[67] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Leitfaden für eine sichere IPv6-Netzwerkarchitektur (ISi-L-IPv6)“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber. ISi-L-IPv6, 2012. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf.pdf.

[68] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI TR-03108 – Secure Email Transport: Requirements for Email Service Providers Regarding Secure Email Transport“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber. TR-03108, Juni 2023. Adresse: https://

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinie
TR03108/TR03108.pdf.

[69] Microsoft Corporation, *Microsoft Defender for Business overview*, (besucht am 20. 4. 2025). Adresse: https://learn.microsoft.com/en-us/defender-business/mdb-overview.

[70] ClamAV Team, *ClamAV Blog – Beiträge und Ankündigungen 2024*, (besucht am 20. 4. 2025). Adresse: https://blog.clamav.net/2024/.

[71] Microsoft Corporation, *AppLocker overview*, (besucht am 20. 4. 2025). Adresse: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview.

[72] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Mindeststandard zur Protokollierung und Detektion von Cyberangriffen“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber. Version 2.1, Nov. 2024. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/MST_BSI_PD_Version_2_1.pdf.

[73] Abteilung IV/S/2 – Netz- und Informationssystemsicherheit Bundesministerium für Inneres (BMI), „Log-Daten als Grundlage für Incident Response – Sammlung, Analyse & Weiterverarbeitung“, Bundesministerium für Inneres (BMI), Techn. Ber., Feb. 2022. Adresse: https://www.nis.gv.at/dam/jcr:39193b9e-e178-48d9-9f30-2c091ce64c62/Schriftenreihe_Cybersicherheit_Log-Daten_als_Grundlage_fuer_Incident_Response_Februar_2022.pdf.

[74] Microsoft Corporation, *Windows-Zeitdienst – Tools und Einstellungen*, (besucht am 25. 4. 2025). Adresse: https://learn.microsoft.com/de-de/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings?tabs=config.

[75] NXLog Ltd., *How to Forward Windows Event Log to Syslog Server*, (besucht am 25. 4. 2025). Adresse: https://nxlog.co/page/eventlog-to-syslog.html.

[76] Rsyslog Project, *ommail – Send Mail Output Module*, (besucht am 25. 4. 2025). Adresse: https://rsyslog.readthedocs.io/en/latest/configuration/modules/ommail.html.

[77] Inc. Wazuh, *Wazuh Platform Overview*, (besucht am 25. 4. 2025). Adresse: https://wazuh.com/platform/overview/.

[78] Inc. Wazuh, *ClamAV logs collection*, (besucht am 25. 4. 2025). Adresse: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/clam-av-logs-collection.html.

[79] Inc. Wazuh, *Windows Defender logs collection*, (besucht am 25. 4. 2025). Adresse: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/win-defender-logs-collection.html.

[80] Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), „Incident Response Guideline for SMEs“, Hong Kong Productivity Council, Techn. Ber., Feb. 2022. Adresse: https://www.hkcert.org/f/blog/910073/911398/Incident%20Response%20Guideline%20for%20SMEs.pdf.

[81] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI-Standard 200-4 Business Continuity Management (BCM)“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber., 2023. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8.

[82] Cybersecurity und Infrastructure Security Agency (CISA), *Ransomware Response Checklist*, (besucht am 26. 4. 2025). Adresse: https://www.cisa.gov/ransomware-response-checklist.

[83] Cybersecurity, Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing und Analysis Center (MS-ISAC), „Phishing Guidance: Stopping the Attack Cycle at Phase One“, Cybersecurity und Infrastructure Security Agency (CISA), Techn. Ber., Okt. 2023. Adresse: https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf.

[84] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya und Karen Scarfone, „Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile“, National Institute of Standards und Technology (NIST), Techn. Ber. NIST SP 800-61r3, Apr. 2025. DOI: 10.6028/NIST.SP.800-61r3. Adresse: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

[85] Microsoft Corporation, *Remediate and unblock users in Microsoft Entra ID Protection*, (besucht am 26. 4. 2025). Adresse: https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-remediate-unblock.

[86] Wirtschaftskammer Österreich (WKO), *Ich habe einen Vorfall – Was tun? Checkliste für Unternehmen*, (besucht am 26. 4. 2025). Adresse: https://www.wko.at/it-sicherheit/ich-habe-einen-vorfall-checkliste.

[87] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Ich habe einen IT-Sicherheitsvorfall – Checkliste für die Technik*, (besucht am 26. 4. 2025). Adresse: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik_node.html.

[88] CERT.at GmbH, *NIS-Portal Österreich – Informationen und Unterstützung zur NIS-Richtlinie*, (besucht am 26. 4. 2025). Adresse: https://nis.cert.at.

[89] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Vorlage Notfallhandbuch gemäß BSI-Standard 200-4 – Business Continuity Management*, (besucht am 27. 4. 2025). Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Notfallhandbuch.html.

[90] Wirtschaftskammer Österreich (WKO), *Vorlage Notfallplan für IT-Sicherheitsvorfälle*. Adresse: https://www.wko.at/oe/it-sicherheit/vorlage-notfallplan.docx.

[91] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Datensicherung – wie geht das?*, (besucht am 27. 4. 2025). Adresse: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datensicherung-und-Datenverlust/Datensicherung-wie-geht-das/datensicherung-wie-geht-das_node.html.

[92] Wirtschaftskammer Österreich (WKO), *Aufbewahrungspflichten: Welche Unterlagen wie lange aufbewahrt werden müssen*, (besucht am 27. 4. 2025). Adresse: https://www.wko.at/steuern/aufbewahrungspflichten.

[93] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Redundanz – Modularität – Skalierbarkeit“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber., 2018. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/redundanz-modularitaet-skalierbarkeit.pdf.

[94] Wirtschaftskammer Österreich (WKO), „IT-Sicherheitshandbuch für kleine und mittlere Unternehmen“, Bundessparte Information und Consulting, Wirtschaftskammer Österreich, Techn. Ber., dez 2018. Adresse: https://www.wko.at/oe/it-sicherheit/it-sicherheitshandbuch-kmu.pdf.

[95] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Umsetzungshinweis zum Baustein INF.1 Allgemeines Gebäude“, Bundesamt für Sicherheit in der Informationstechnik (BSI), Techn. Ber., 2022. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2022/Umsetzungshinweis_zum_Baustein_INF_1_Allgemeines_Gebaeude.pdf.

[96] Grafana Labs, *Grafana Alerting Documentation*, (besucht am 27. 4. 2025). Adresse: https://grafana.com/docs/grafana/latest/alerting/.