UMSETZUNG DER NIS-2-RICHTLINIE IM ABWASSERSEKTOR

HERAUSFORDERUNGEN UND GOOD PRACTICES ZUR CYBERSICHERHEIT IN KRITISCHEN INFRASTRUKTUREN

ausgeführt am 27.Juni 2025

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Von: Dominik Döttl
Personenkennzeichen: 00608505

Graz, am 27. Juni 2025 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

An dieser Stelle gilt meiner Familie herzlicher Dank für die stetige Unterstützung, den Rückhalt und das Verständnis während der gesamten Studienzeit. Besonderer Dank gilt zudem Herrn DI(FH) Christian Schmid, MSc, dessen Fachwissen und motivierende Art diese Arbeit kontinuierlich begleitet und gefördert haben. Für diese wertvolle Hilfe und die stets offenen Worte sei herzlich gedankt.

KURZFASSUNG

Die vorliegende Arbeit untersucht die Umsetzung der EU-NIS-2-Richtlinie im Abwassersektor als Teil der kritischen Infrastruktur. Der Fokus liegt auf der Bewertung des aktuellen Umsetzungsstands, der Identifikation von Herausforderungen und der Erfassung von Good Practices. Die Thematik ist hochrelevant und aktuell, da die NIS-2-Richtlinie spätestens bis Oktober 2024 in nationales Recht überführt werden muss und erstmals auch mittelgroße Unternehmen in die Pflicht nimmt. Die Studie reagiert auf die Forschungslücke hinsichtlich sektorspezifischer Umsetzungserfahrungen und liefert einen praktischen Beitrag zur Stärkung der Cybersicherheit in der öffentlichen Daseinsvorsorge.

Die Arbeit folgt einem Mixed-Methods-Ansatz im Paradigma der verhaltensorientierten Wirtschaftsinformatik. Datenerhebungsmethode ist eine standardisierte Online-Befragung unter Akteuren der Abwasserwirtschaft im deutschsprachigen Raum. Der Fragebogen kombiniert geschlossene (quantitative) mit offenen (qualitativen) Items, die sieben Themenkategorien der NIS-2-Richtlinie abbilden. Die Auswertung erfolgte quantitativ-deskriptiv sowie qualitativ mittels strukturierter Inhaltsanalyse nach Mayring. Ein Pretest sicherte die Validität der Instrumente; die Datenerhebung erfolgte in Kooperation mit der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V.

Die Ergebnisse zeigen ein heterogenes, aber überwiegend hohes Umsetzungsniveau bei organisatorischen, technischen und physischen Maßnahmen. Die Mehrheit der Unternehmen hat ein Risikomanagement etabliert, regelmäßige Schulungen eingeführt und strukturelle Verantwortlichkeiten verankert. Die häufigsten Herausforderungen betreffen personelle Ressourcen, fehlende branchenspezifische Leitfäden und komplexe technische Anforderungen. Good Practices umfassen unter anderem adaptive Risikoanalysen, szenariobasierte Verfahren und die Integration von ISO/IEC-Standards. Die Ergebnisse werden mit bestehenden wissenschaftlichen Arbeiten, etwa von ENISA oder BSI, verglichen und kontextualisiert.

Die Analyse verdeutlicht, dass Cybersicherheit zunehmend als strategische Aufgabe in der Abwasserwirtschaft erkannt wird, allerdings je nach Größe und Struktur der Unternehmen unterschiedlich ausgeprägt ist. Die Arbeit zeigt, dass etablierte Sicherheitsstandards wie ISO 27001, B3S Wasser/Abwasser und das ÖWAV-Handbuch praktikable Rahmenbedingungen bieten, jedoch an spezifische Sektorbedürfnisse angepasst werden müssen. Die Resultate unterstreichen die Notwendigkeit gemeinsamer Leitfäden, sektoraler Koordination und staatlicher Unterstützung. Ein Ausblick benennt weiterführende Forschungsschwerpunkte wie

die Wirksamkeit konkreter Maßnahmen, die Rolle externer Dienstleister und die Entwicklung belastbarer Metriken zur Cybersicherheitsreife.

ABSTRACT

This thesis examines the implementation of the EU NIS-2 Directive in the wastewater sector, which is classified as part of critical infrastructure. The study aims to assess the current state of implementation, identify challenges, and capture good practices. The topic is highly relevant and timely, as the directive must be transposed into national law by October 2024 and, for the first time, includes medium-sized enterprises. The study addresses a notable research gap concerning sector-specific implementation experiences and contributes practically to strengthening cybersecurity in public utility services.

The study applies a mixed-methods approach within the behavioral paradigm of Information Systems research. Data was collected through a standardized online survey among stakeholders in the German-speaking wastewater sector. The questionnaire combined closed (quantitative) and open (qualitative) items, covering seven thematic categories derived from the NIS-2 Directive. Quantitative results were analyzed using descriptive statistics, while qualitative responses were evaluated using Mayring's structured content analysis. A pretest ensured the validity of the instrument, and the survey was distributed with the support of the German Association for Water, Wastewater and Waste (DWA).

Findings show a heterogeneous but generally high level of implementation of organizational, technical, and physical measures. Most companies have established risk management systems, conduct regular cybersecurity training, and have defined responsibilities. The main challenges identified include limited human resources, lack of sector-specific guidelines, and technical complexity. Good practices include adaptive risk analyses, scenario-based procedures, and the integration of ISO/IEC standards. The findings are contextualized with existing literature, such as those by ENISA and BSI.

The results indicate a growing recognition of cybersecurity as a strategic task in the wastewater sector, although the degree of implementation varies based on company size and structure. The study shows that established security standards like ISO 27001, B3S Water/Wastewater, and the ÖWAV handbook offer practical frameworks but must be adapted to sector-specific needs. The findings highlight the need for joint guidelines, sectoral coordination, and government support. Future research should examine the effectiveness of specific measures, the role of external service providers, and the development of robust metrics for cybersecurity maturity.

INHALTSVERZEICHNIS

1 EINLEITUNG 1

1.1 Ausgangslage und Motivation 2
1.2 Relevanz der Informationssicherheit im Sektor Abwasser 2
1.3 Forschungsstand und bestehende Ansätze 3
1.4 Herleitung der Forschungsfrage 4
1.5 Forschungszielsetzung 4
1.6 Forschungsdesign und -paradigma 5
1.6.1 Forschungshypothese 6

1.7 Aufbau der Thesis 6

2 THEORETISCHER RAHMEN 8

2.1 Die NIS-2-Richtlinie 8
2.1.1 Verantwortung der wesentlichen und wichtigen Einrichtungen in der NIS-2-Richtlinie 8
2.1.2 Risikomanagement und Sicherheitsmaßnahmen 8
2.1.3 Technische und organisatorische Sicherheitsmaßnahmen 9
2.1.4 Berichtspflichten und Meldeverfahren 10
2.1.5 Einhaltung internationaler und europäischer Standards 10
2.1.6 Zusätzliche Verpflichtungen für die Einrichtungen 11

2.2 Informationssicherheits- und Cybersecurityframeworks und –leitfäden 11
2.2.1 Österreichisches Sicherheitshandbuch 12
2.2.2 IT-Grundschutzkompendium des BSI 12
2.2.3 ISO 27000er-Normenfamilie 12
2.2.4 B3S Branchenspezifischer Sicherheitsstandard Wasser/Abwasser 13
2.2.5 ÖWAV-Arbeitsbehelf zur IKT-Sicherheit im Bereich Abwasser 13
2.2.6 KRITIS 14
2.2.7 Cybersecurity Framework 14
2.2.8 Framework for Improving Critical Infrastructure Cybersecurity 15
2.2.9 Cyber Assessment Framework 15
2.2.10 Cyber Assessment Framework v3.0 15

3 BEFRAGUNG NIS2-BETROFFENER UNTERNEHMEN AUS DEM SEKTOR ABWASSER 16

3.1 Zielsetzung der Befragung 16

3.2 Design und Methodik der Befragung 16
3.2.1 Planung und Konstruktion der Befragung zur Datenerhebung und des Fragenkataloges 16
3.2.2 Durchführung eines Pre-Tests 17
3.2.3 Auswahl der Zielgruppe bzw. Stichprobe 17
3.2.4 Planung der Datenauswertung 17

4 AUSWERTUNG UND ANALYSE DER DATEN 19

4.1 Methoden zur Auswertung und Analyse der Antworten 19
4.1.1 Quantitative Datenanalyse der Befragungsantworten 19
4.1.2 Qualitative Datenanalyse der Befragungsantworten 19

4.2 Auswertung der Fragen aus Themenkategorie 1 „Governance“ 20
4.2.1 Frage 1: Wie ist die Cybersicherheit in Ihrem Unternehmen strukturell organisiert? 20
4.2.2 Frage 2: Welche Führungsebene ist in ihrem Unternehmen für Cybersicherheit bzw. die Umsetzung der NIS-2-RL verantwortlich? 21
4.2.3 Frage 3: Welche Governance-Maßnahmen setzen sie zur Erfüllung der NIS-2-Richtlinie um? 22

4.3 Auswertung der Fragen aus Themenkategorie 2 „Organisatorische Maßnahmen“ 23
4.3.1 Frage 4: Welche organisatorischen Maßnahmen haben Sie zur Sicherstellung der Cybersicherheit gemäß der NIS-2-Richtlinie implementiert? 24

4.4 Auswertung der Fragen aus Themenkategorie 3 „Risikomanagement“ 25
4.4.1 Frage 5: Haben Sie ein Risikomanagementsystem für Informations- und Cybersicherheit implementiert? 25
4.4.2 Frage 6: Welche der folgenden Risikoanalyseverfahren setzen Sie ein? 26
4.4.3 Frage 7: Wie definieren Sie die Risikobewertungskriterien für die Cybersicherheit in Ihrem Unternehmen? 27
4.4.4 Frage 8: Welche Faktoren berücksichtigen Sie bei der Festlegung der Risikobewertungskriterien? 29
4.4.5 Frage 9: Welche Methoden zur Risikobeurteilung setzen Sie in Ihrem Unternehmen ein? 30
4.4.6 Frage 10: Wie wird die Kritikalität der einzelnen Bedrohungen in Ihrem Unternehmen ermittelt?“ 31

4.5 Auswertungen der Fragen aus Themenkategorie 4 „Technische Maßnahmen“ 32
4.5.1 Frage 11: Welche technischen Cybersicherheitsmaßnahmen haben Sie implementiert um den Anforderungen der NIS-2-Richtlinie zu entsprechen? 32

4.6 Auswertungen der Fragen aus Themenkategorie 5 „Physische Maßnahmen“ 35
4.6.1 Frage 12: Welche physischen Maßnahmen setzen Sie ein, um den Schutz Ihrer IT- und Netzwerksysteme zu gewährleisten? 35
4.6.2 Frage 13: Wie häufig werden physische Sicherheitsmaßnahmen überprüft? 36

4.7 Auswertungen der Fragen aus Themenkategorie 6 „NIS-2 und Cybersicherheitsstandards“ 37
4.7.1 Frage 14: Welche zusätzlichen Informations- und Cybersicherheits-standards oder -normen setzen Sie neben der NIS-2-Richtlinie um? 37
4.7.2 Frage 15: Für welche Anforderungen der NIS-2-Richtlinie setzen die Informations- und Cybersicherheitsstandards bzw. Teile/Kapitel dieser Standards ein? 38

4.8 Auswertung der Fragen aus Themenkategorie 7 „Anregungen für zukünftige Leitfäden/Standards zur NIS-2-Richtlinie“ 40
4.8.1 Frage 16: Welche technischen Herausforderungen haben Sie bei der Implementierung der NIS-2-Richtlinie identifiziert? 40
4.8.2 Frage 17: Welche weiteren Unterstützungsmöglichkeiten oder Ressourcen benötigen Sie, um die Anforderungen der NIS-2-Richtlinie vollständig zu erfüllen? 41
4.8.3 Frage 18: Was sind aus Ihrer Sicht die wichtigsten Good Practices bei der Umsetzung der NIS-2-Richtlinie? 42

5 ERGEBNISSE 45

5.1 Ergebnisse aus Themenkategorie 1: Governance 45
5.2 Ergebnisse aus Themenkategorie 2: Organisatorische Maßnahmen 45
5.3 Ergebnisse aus Themenkategorie 3: Risikomanagement 46
5.4 Ergebnisse aus Themenkategorie 4: Technische Maßnahmen 46
5.5 Ergebnisse aus Themenkategorie 5: Physische Maßnahmen 46
5.6 Ergebnisse aus Themenkategorie 6: NIS-2 und Cyber-sicherheitsstandards 47
5.7 Ergebnisse aus Themenkategorie 7: Herausforderungen und Unterstützungsbedarfe 47
5.8 Zusammenfassung und Fazit 48
5.9 Spezifische Anforderungen und Implikationen für den Sektor Abwasser 48
5.9.1 Strukturelle Fragmentierung und Ressourcenengpässe 48
5.9.2 Technologische Besonderheiten und veraltete Systemlandschaften 49
5.9.3 Bedeutung branchenspezifischer Normen und Leitlinien 49
5.9.4 Kooperationsnetzwerke und sektorspezifischer Wissensaustausch 49
5.9.5 Zusammenfassung und sektorale Handlungsperspektiven 49

6 BEANTWORTUNG DER FORSCHUNGSFRAGE 51

6.1 Zusammenfassung der Ergebnisse 51
6.2 Beantwortung der Forschungsfrage 52
6.2.1 Strukturelle Gestaltung und Verantwortlichkeiten 53
6.2.2 Organisatorische Maßnahmen 53
6.2.3 Technische Maßnahmen 53
6.2.4 Herausforderungen bei der Umsetzung 53
6.2.5 Good Practices für eine sektorweite Standardisierung 54

6.3 Handlungsempfehlungen für die Praxis 54
6.3.1 Entwicklung eines sektorspezifischen, modularen Umsetzungsleitfadens 54
6.3.2 Etablierung zentraler Unterstützungs- und Beratungsstellen 55
6.3.3 Förderung interkommunaler und verbandlicher Kooperation 55
6.3.4 Integration von Cybersicherheit in Förderprogramme 55
6.3.5 Verstärkte Schulungs- und Qualifizierungsinitiativen 55
6.3.6 Verpflichtende Integration von Lieferkettenaspekten 56
6.3.7 Verankerung von Cybersicherheit auf Leitungsebene 56
6.3.8 Benennung dedizierter Cybersicherheitsbeauftragter 56
6.3.9 Verpflichtende Awareness-Schulungen für Mitarbeitende 56
6.3.10 Nutzung kombinierter Sicherheitsstandards als Orientierungsrahmen 56
6.3.11 Etablierung technischer Frühwarn- und Monitoring-Systeme 56
6.3.12 Integration von Lieferkettenaspekten in das Risikomanagement 57
6.3.13 Entwicklung eines sektorspezifischen, modularen Umsetzungsleitfadens 57
6.3.14 Etablierung zentraler Unterstützungs- und Beratungsstellen 57
6.3.15 Förderung interkommunaler und verbandlicher Kooperation 57
6.3.16 Integration von Cybersicherheit in Förderprogramme 57
6.3.17 Verstärkung von Schulungs- und Qualifizierungsinitiativen 58
6.3.18 Intensivierung des sektorinternen und sektorübergreifenden Informations-austauschs 58

7 CONCLUSIO UND AUSBLICK 59

7.1 Wissenschaftlicher und praktischer Beitrag 59
7.2 Limitationen und Kritikpunkte 60
7.3 Potenziale für weiterführende Forschung 60
7.4 Ausblick auf die Zukunft der Cybersicherheit im Sektor Abwasser 61

ANHANG A - 1. ANHANG: FRAGENKATALOG DER BEFRAGUNG 62

ANHANG B - 2. ANHANG: ROHDATEN DER BEFRAGUNGSANTWORTEN 66

ABKÜRZUNGSVERZEICHNIS 67

ABBILDUNGSVERZEICHNIS **69**

TABELLENVERZEICHNIS **70**

LITERATURVERZEICHNIS **71**

Bücher 71
Journale 72
Gesetze und Verordnungen 72

1 EINLEITUNG

Die fortschreitende Digitalisierung und die zunehmende Vernetzung technischer Systeme verändern nahezu alle gesellschaftlichen und wirtschaftlichen Bereiche. Betreiber Kritischer Infrastrukturen (KRITIS) bewegen sich zwischen der Effizienzsteigerung durch digitale Technologien und einer wachsenden Verwundbarkeit gegenüber Cyberbedrohungen (Bendiek & Metzger, 2021). Die Versorgungssicherheit in Sektoren wie Energie, Gesundheit, Transport und Wasser hängt immer stärker von der Verfügbarkeit und Sicherheit informationstechnologischer Systeme ab.

Die Abwasserentsorgung bildet einen besonders sensiblen Bereich innerhalb der KRITIS-Kategorien. Als essenzieller Bestandteil der öffentlichen Daseinsvorsorge besitzt dieser Sektor infrastrukturelle, ökologische und gesundheitliche Bedeutung. Zugleich kennzeichnen ihn kleinteilige Strukturen, heterogene Betreiberlandschaften sowie teilweise begrenzte IT-Ressourcen (BDEW, 2023). Diese Rahmenbedingungen erschweren die Implementierung einheitlicher und wirksamer Cybersicherheitsmaßnahmen.

Zur Eindämmung des steigenden Cyberangriffsrisikos auf kritische Infrastrukturen verabschiedete die Europäische Union im Jahr 2022 die NIS-2-Richtlinie (Directive (EU) 2022/2555). Diese überarbeitete und deutlich verschärfte Fassung der ursprünglichen NIS-Richtlinie verfolgt das Ziel, ein hohes gemeinsames Niveau der Cybersicherheit innerhalb der Union sicherzustellen. Erstmals verpflichtet das Regelwerk auch mittelgroße Unternehmen und Einrichtungen, angemessene technische und organisatorische Sicherheitsvorkehrungen zu implementieren, sofern eine Zuordnung zu einem kritischen oder wichtigen Sektor vorliegt (Europäische Union, 2022).

Die praktische Umsetzung der NIS-2-Richtlinie konfrontiert den Abwassersektor mit neuen Herausforderungen. Neben rechtlichen Fragen treten Aspekte der technischen Machbarkeit, der organisatorischen Realisierbarkeit und der personellen Ressourcen in den Vordergrund. Vor diesem Hintergrund analysiert die vorliegende wissenschaftliche Arbeit die Auswirkungen der NIS-2-Richtlinie auf Unternehmen des Abwassersektors. Im Mittelpunkt steht die Bewertung der Umsetzungsbereitschaft sowie der bestehenden Hindernisse aus Sicht der betroffenen Akteure.

Ziel dieser wissenschaftlichen Arbeit ist es, anhand einer empirischen Befragung von Unternehmen der Abwasserentsorgung zu ermitteln, wie die Anforderungen der NIS-2-Richtlinie bewertet werden, welche Sicherheitsmaßnahmen bereits implementiert sind und welche Hindernisse oder Unterstützungsbedarfe vorliegen. Die Untersuchung leistet einen praxisbezogenen Beitrag zur aktuellen Diskussion über Cybersicherheit im KRITIS-Sektor und bildet eine Grundlage für politische, technische und organisatorische Handlungsempfehlungen.

1.1 Ausgangslage und Motivation

Den Ausgangspunkt dieser wissenschaftlichen Arbeit bildet die Verlautbarung der NIS-2-Richtlinie (Network and Information Security Directive 2) der Europäischen Union. Diese Richtlinie schafft einen rechtsverbindlichen Rahmen, der die Cybersicherheit kritischer Infrastrukturen stärkt. Von betroffenen Unternehmen, darunter Betreiber wesentlicher Dienste im Abwassersektor, verlangt die Richtlinie die Einführung umfassender Risikomanagementmaßnahmen, die Verbesserung der Informationssicherheit und die Einhaltung spezifischer Meldepflichten bei Sicherheitsvorfällen. Ein wesentliches Ziel besteht darin, durch verstärkten Austausch und die Entwicklung branchenspezifischer Leitfäden die Sicherheitsstandards zwischen den Unternehmen zu harmonisieren und fortzuentwickeln. Artikel 8 hebt ausdrücklich die Notwendigkeit von Kooperation und Informationsaustausch zwischen wesentlichen Einrichtungen hervor. Dieser Fokus auf den Austausch bewährter Verfahren begründet die Motivation der vorliegenden Untersuchung. Die angestrebte Zusammenarbeit ermöglicht es, Sicherheitslücken frühzeitig zu erkennen und zu schließen und die Resilienz kritischer Infrastrukturen gegenüber Cyberangriffen zu erhöhen. Zudem verpflichtet die Richtlinie die Mitgliedstaaten, die Erstellung und Verbreitung branchenspezifischer Leitfäden zu fördern, die Unternehmen eine praxisnahe, sektorspezifische Umsetzung der Anforderungen erleichtern.

Vor diesem Hintergrund untersucht diese Arbeit die Umsetzungsstrategien der NIS-2-Richtlinie im Abwassersektor und identifiziert Good Practices sowie bestehende Lösungen, die Abwasserdienstleistern helfen, ihre Informations- und Cybersicherheitsstandards zu verbessern. Die Analyse des aktuellen Status quo und die systematische Erfassung bereits umgesetzter Maßnahmen sollen es ermöglichen, Handlungsempfehlungen abzuleiten und den Unternehmen eine tragfähige Grundlage für die Optimierung ihrer Sicherheitsstrategien zu bieten.

Darüber hinaus leistet die Untersuchung einen Beitrag zur Erstellung branchenspezifischer Leitfäden, indem diese darstellt, welche Maßnahmen und Standards sich in der Praxis als besonders wirksam erweisen. Die gewonnenen Ergebnisse stärken die Informationssicherheitskultur in der Abwasserwirtschaft und fördern die Zusammenarbeit sowie den Wissensaustausch zwischen den Unternehmen. Auf diese Weise lässt sich die Resilienz des gesamten Sektors gegenüber zukünftigen Cyberbedrohungen erhöhen und eine kontinuierliche Verbesserung der Sicherheitsmaßnahmen unterstützen.

1.2 Relevanz der Informationssicherheit im Sektor Abwasser

Die Relevanz der IKT-Sicherheit in der Siedlungswasserwirtschaft und Abwasserwirtschaft ergibt sich hauptsächlich aus der zunehmenden Integration von Informations- und Kommunikationstechnologien (IKT) in diesen Sektoren. Mit der fortschreitenden Digitalisierung der Wasserversorgungs- und Abwasserbehandlungsprozesse bringt die Vernetzung von Systemen erhebliche betriebliche und wirtschaftliche Vorteile mit sich, erhöht jedoch auch die Risiken für IKT-Vorfälle, einschließlich Cyberangriffe. Diese Vorfälle können zu Störungen oder Ausfällen bei Wasserversorgungsunternehmen und Abwasserreinigungsanlagen führen, was die öffentliche Gesundheit und die Umweltsicherheit beeinträchtigen kann. Daher ist es

entscheidend, ein hohes Maß an IKT-Sicherheit aufrechtzuerhalten, um die betriebliche Zuverlässigkeit und Sicherheit in der Siedlungswasserwirtschaft zu gewährleisten (Pointl et al., 2019)

Die Relevanz der NIS-2-Richtlinie sowie der Themen Informationssicherheit und Cybersicherheit im Bereich der Abwasserdienstleistungen ist von zentraler Bedeutung, da diese Einrichtungen als Teil der wesentlichen Dienste und der kritischen Infrastruktur fungieren. Der Abwassersektor spielt eine entscheidende Rolle für die öffentliche Gesundheit, den Umweltschutz und das reibungslose Funktionieren von städtischen Infrastrukturen. Eine Störung der Abwassersysteme kann gravierende Folgen haben, wie etwa die Verunreinigung von Wasserquellen, Gesundheitsrisiken für die Bevölkerung oder weitreichende Umweltschäden.

Durch die zunehmende Digitalisierung und den Einsatz von IT-Systemen zur Steuerung und Überwachung von Abwassernetzen und Kläranlagen wächst das Risiko von Cyberangriffen und anderen Bedrohungen der Informationssicherheit. Netz- und Informationssysteme, die für den Betrieb dieser Anlagen verantwortlich sind, werden zu attraktiven Zielen für Angreifer, die durch Ransomware-Angriffe, Sabotage oder Datendiebstahl den Betrieb lahmlegen oder empfindliche Daten kompromittieren können. Solche Vorfälle könnten zu erheblichen Störungen der öffentlichen Ordnung und massiven wirtschaftlichen Schäden führen.

Die NIS-2-Richtlinie der Europäischen Union stellt einen rechtlichen Rahmen dar, der darauf abzielt, das Cybersicherheitsniveau in kritischen Infrastrukturen, einschließlich der Abwasserwirtschaft, signifikant zu erhöhen. Diese fordert von den wesentlichen Einrichtungen nicht nur die Implementierung von technischen und organisatorischen Sicherheitsmaßnahmen, sondern auch die Ermittlung und das Management von Risiken, die Schaffung von Notfallplänen und die Meldung schwerwiegender Sicherheitsvorfälle an die zuständigen Behörden. Diese Maßnahmen sind entscheidend, um die Resilienz und den kontinuierlichen Betrieb von Abwasserdienstleistungen sicherzustellen.

In diesem Zusammenhang sind Informations- und Cybersicherheit nicht nur technische Herausforderungen, sondern auch strategische Aufgaben, die auf der Führungsebene von Abwasserdienstleistungsunternehmen adressiert werden müssen. Durch die Umsetzung der NIS-2-Richtlinie können diese Unternehmen sicherstellen, dass diese gegen eine wachsende Zahl von Bedrohungen gewappnet sind, und gleichzeitig die Anforderungen des Gesetzgebers erfüllen, um ihre Systeme und Dienstleistungen bestmöglich zu schützen.

1.3 Forschungsstand und bestehende Ansätze

Der gegenwärtige Forschungsstand zur Umsetzung der NIS-2-Richtlinie und zu deren Folgen für wesentliche sowie wichtige Einrichtungen, insbesondere im Bereich der Abwasserdienstleistungen, befindet sich noch in einem frühen Entwicklungsstadium. Obwohl die NIS-2-Richtlinie ein breites Spektrum an Cybersicherheitsmaßnahmen umfasst, weist die wissenschaftliche Literatur eine ausgeprägte Lücke hinsichtlich der konkreten Umsetzung in sektoralen Infrastrukturen wie der Abwasserwirtschaft auf. Aktuelle wissenschaftliche Arbeiten legen den Schwerpunkt auf übergeordnete rechtliche und technische Fragestellungen. Die

tatsächliche Implementierung auf Unternehmensebene, insbesondere in kleinen und mittleren Versorgungsbetrieben, bleibt bislang nur am Rande betrachtet (Bossong & Wagner, 2019; ENISA, 2023).

Die Interaktion zwischen organisatorischen, technischen und personellen Faktoren im Umsetzungsprozess ist bisher kaum systematisch untersucht. Ebenso besteht eine Forschungslücke in Bezug auf sektorspezifische Umsetzungsstrategien, die über generische Normen hinausgehen und die Besonderheiten der Wasser- und Abwasserwirtschaft berücksichtigen (Pflüger & Pohlmann, 2020). Vergleichende empirische Untersuchungen zur Wirksamkeit verschiedener Sicherheitsstandards, beispielsweise ISO/IEC 27001, BSI IT-Grundschutz oder B3S Wasser/Abwasser, in Bezug auf die Einhaltung der NIS-2-Richtlinie liegen bislang nur vereinzelt vor (Tikk & Kerttunen, 2021).

Die vorliegende wissenschaftliche Arbeit untersucht diese Forschungslücken durch eine gezielte Analyse des Abwassersektors im deutschsprachigen Raum und stellt Erkenntnisse bereit, die sowohl wissenschaftlich als auch praktisch verwertbar sind.

1.4 Herleitung der Forschungsfrage

Der aktuelle Forschungsstand, die identifizierte Forschungslücke und die praktischen Herausforderungen in der Abwasserwirtschaft führen zur folgenden Forschungsfrage:

„Wie gestalten und implementieren Abwasserdienstleister im deutschsprachigen Raum strukturelle und organisatorische Maßnahmen zur Einhaltung der NIS-2-Richtlinie, welche Herausforderungen treten dabei auf, und welche Good Practices lassen sich daraus für eine sektorweite Standardisierung der Cybersicherheit ableiten?“

Diese mehrdimensionale Frage umfasst wesentliche Elemente der Richtlinie im spezifischen Kontext der Abwasserwirtschaft. Ein Mixed-Methods-Design ermöglicht eine empirische Untersuchung, die qualitative und quantitative Daten integriert und dadurch eine differenzierte Analyse zulässt. Die Untersuchung erfasst nicht nur den Status quo der Umsetzung, sondern identifiziert darüber hinaus Good Practices und leitet daraus systematisch Handlungsempfehlungen ab, die branchenweit anwendbar sind.

1.5 Forschungszielsetzung

Die vorliegende wissenschaftliche Arbeit verfolgt das Ziel, den Umsetzungsstand der NIS-2-Richtlinie im Abwassersektor zu erheben, bestehende Herausforderungen zu benennen und vorhandene Lösungen sowie Good Practices zu identifizieren. Auf dieser Grundlage werden praxisrelevante Handlungsempfehlungen formuliert, damit Unternehmen und politische Entscheidungsträger bei der Ausgestaltung eines sektorspezifischen Cybersicherheitsstandards unterstützt werden, der den Einrichtungen des Abwassersektors eine normkonforme Umsetzung der Richtlinie ermöglicht.

Darüber hinaus sollen Potenziale und Optimierungsmöglichkeiten für künftige Implementierungen aufgezeigt werden. Die empirische Erhebung untersucht organisatorische Strukturen, technische und physische Schutzmaßnahmen sowie den Einsatz etablierter Normen und Leitfäden. Die gewonnenen Ergebnisse liefern Abwasserdienstleistern eine belastbare Grundlage, um die Anforderungen der NIS-2-Richtlinie effizient und nachhaltig umzusetzen und damit die Cybersicherheit in der gesamten Branche zu stärken.

1.6 Forschungsdesign und -paradigma

Für die Untersuchung kam die empirische Methode der standardisierten Befragung zum Einsatz, deren Wurzeln in den Sozialwissenschaften liegen und die sich besonders zur Erhebung von Meinungen, Einschätzungen und organisatorischen Strukturen eignet (Atteslander 2010). Um die komplexe Umsetzung der NIS-2-Richtlinie im Abwassersektor umfassend zu analysieren, wurde ein Mixed-Methods-Ansatz gewählt; dabei lassen sich quantitative und qualitative Elemente systematisch verbinden (Creswell & Plano Clark 2018).

Die quantitative Komponente basiert auf einem strukturierten Fragebogen mit geschlossenen Formaten. Ziel war es, den Status quo der Umsetzung der NIS-2-Anforderungen in Unternehmen der Abwasserwirtschaft abzubilden. Diese Datengrundlage ermöglicht deskriptiv-statistische Auswertungen, um Muster, Korrelationen und signifikante Unterschiede zwischen Organisationen zu identifizieren.

Ergänzend wurden qualitative Elemente in Form offener Fragen integriert. Diese Vorgehensweise erfasst kontextspezifische Perspektiven und untersucht verhaltensorientierte Dimensionen der Sicherheitskultur (Flick 2019). Die Befragten konnten dabei spezifische Herausforderungen, Good Practices sowie eigene Erfahrungen mit der NIS-2-Umsetzung ausführlich darstellen.

Die quantitativen Daten wurden mithilfe statistischer Verfahren der Häufigkeitsanalyse und der deskriptiven Statistik ausgewertet; explorative Korrelationsanalysen dienten der vertiefenden Mustererkennung. Für die qualitativen Antworten kam eine strukturierte Inhaltsanalyse nach Mayring (2015) zur Anwendung, um wiederkehrende Themen, Muster und Handlungslogiken herauszuarbeiten. Durch die methodische Triangulation beider Ansätze wurden die Ergebnisse vertieft, kontextualisiert und kritisch reflektiert.

Dieses Design stellt eine robuste und valide Grundlage bereit, die theoriegeleitete sowie praxisorientierte Erkenntnisse zur Umsetzung der NIS-2-Richtlinie im Sektor der Abwasserdienstleistungen ermöglicht.

Die Untersuchung ist im Paradigma der verhaltensorientierten Forschung der Wirtschaftsinformatik verortet. Dieses Paradigma analysiert das Verhalten von Individuen, Gruppen und Organisationen im Umgang mit Informationssystemen und zeigt, wie technologische Vorgaben und Richtlinien durch handelnde Akteure aufgenommen und umgesetzt werden.

Im Kontext der NIS-2-Richtlinie untersucht der verhaltensorientierte Ansatz, wie Abwasserdienstleister auf die neuen Anforderungen der Informations- und Cybersicherheit

reagieren. Eine deskriptive Feldforschung analysierte die individuellen Verhaltensweisen sowie die organisationalen Prozesse, die für eine erfolgreiche Implementierung organisatorischer, technischer und physischer Maßnahmen erforderlich sind. Dabei wurden die Risikobewertung durch Entscheidungsträger, wahrgenommene Handlungszwänge und bestehende Hindernisse einbezogen.

Der verhaltensorientierte Fokus erlaubt somit eine ganzheitliche Betrachtung der Wechselwirkungen zwischen den technologischen Anforderungen der NIS-2-Richtlinie und den menschenbezogenen Aspekten ihrer Umsetzung. Dies ist ein wesentliches Anliegen in der kritischen Infrastruktur des Abwassersektors.

1.6.1 Forschungshypothese

Auf Grundlage des aktuellen Stands der Technik und der Verfügbarkeit verschiedener Cybersicherheits-frameworks für unterschiedliche Industriebereiche wird angenommen, dass diese Rahmenwerke, Technologien und Werkzeuge auch im Abwasserdienstleistungsbereich zielgerichtet eingesetzt werden können. Daraus ergibt sich die Hypothese:

„Durch kombinierten Einsatz verschiedener Informations- und Cybersicherheits-frameworks lässt sind im Abwasserdienstleistungsbereich Bearbeitung der NIS-2-Anforderungen unterstützen.“

1.7 Aufbau der Thesis

Das erste Kapitel erläutert Ausgangslage, Forschungshintergrund und Motivation. Auf Basis des gegenwärtigen Forschungsstands wird eine Forschungslücke ausgewiesen und daraus die leitende Forschungsfrage abgeleitet. Eine darauf abgestimmte Hypothese sowie das übergeordnete Forschungsziel werden formuliert. Anschließend folgen Forschungsmethodik und -design; die methodischen Überlegungen begründen nachvollziehbar die gewählten Erhebungs- und Auswertungsverfahren.

Das zweite Kapitel entwickelt den theoretischen Bezugsrahmen. Es definiert zunächst alle relevanten Fachtermini und beschreibt dann die rechtlichen Rahmenbedingungen der Informations- und Cybersicherheit im Abwassersektor. Damit wird die empirische Untersuchung im wissenschaftlichen und regulatorischen Kontext verankert.

Das dritte Kapitel dokumentiert die empirische Untersuchung. Neben Untersuchungsdesign, Zielgruppenauswahl, Fragebogengestaltung und Datenerhebung werden Überlegungen zu Validität und Reliabilität dargestellt, um die wissenschaftliche Qualität zu sichern.

Im vierten Kapitel werden die erhobenen Daten deskriptiv-statistisch ausgewertet. Statistische Kennzahlen und grafische Darstellungen veranschaulichen Tendenzen, Verteilungen und Zusammenhänge und bilden die Grundlage für die Beantwortung der Forschungsfrage sowie die Prüfung der Hypothese.

Das fünfte Kapitel interpretiert die Ergebnisse. Die wesentlichen Erkenntnisse werden in den theoretischen Rahmen und den aktuellen Forschungsstand eingeordnet. Dabei wird die Hypothese überprüft und diskutiert, welche Perspektiven sich für Praxis und Forschung eröffnen.

Das sechste Kapitel fasst die vorliegende Arbeit zusammen. Die wichtigsten Ergebnisse werden reflektiert, der wissenschaftliche und praktische Beitrag herausgestellt, Limitationen benannt und ein Ausblick auf zukünftige Entwicklungen der Informations- und Cybersicherheit im Abwassersektor gegeben. Möglichkeiten weiterführender Forschung und praxisorientierter Maßnahmen schließen das Kapitel ab.

Diese Struktur gewährleistet eine systematische und nachvollziehbare Auseinandersetzung mit der Thematik und verbindet theoretische Basis mit empirischer Evidenz, um einen umfassenden Beitrag zur Informations- und Cybersicherheit in kritischen Infrastrukturen zu leisten.

2 THEORETISCHER RAHMEN

2.1 Die NIS-2-Richtlinie

Die erste Richtlinie über Netz- und Informationssicherheit (NIS-Richtlinie 2016/1148) trat 2016 in Kraft und schuf erstmals einen unionsweiten Rechtsrahmen für die Cybersicherheit von Betreibern wesentlicher Dienste und ausgewählten digitalen Dienstleistern. In Österreich erfolgte die Umsetzung über das Netz- und Informationssystem-sicherheitsgesetz (NISG), die NIS-Verordnung und die EU-NIS-Durchführungsverordnung.

Die Nachfolgeregelung, die Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 (kurz: NIS-2-Richtlinie) wurde am 27. Dezember 2022 im Amtsblatt der Europäischen Union (L 333/80) veröffentlicht und trat am 16. Januar 2023 in Kraft. Die Vorgaben sind bis spätestens 17. Oktober 2024 in österreichisches Recht zu überführen. Bis zu diesem Zeitpunkt gelten weiterhin die Bestimmungen des NIS-Gesetzes, der NIS-Verordnung und der EU-NIS-Durchführungsverordnung.

Die NIS-2-Richtlinie verfolgt das Ziel, ein einheitliches, hohes Schutzniveau für Netz- und Informationssysteme kritischer und sensibler Infrastrukturen in den Mitgliedstaaten zu gewährleisten. Diese definiert daher sowohl Verantwortlichkeiten der betroffenen Einrichtungen als auch Pflichten der Mitgliedstaaten. Wesentliche und wichtige Einrichtungen müssen angemessene Risikomanagementmaßnahmen implementieren und ihre Netz- und Informationssysteme schützen. Die Mitgliedstaaten sind für die strategische Ausgestaltung, Überwachung und Durchsetzung der Vorgaben verantwortlich und stellen sicher, dass die Richtlinie unionsweit wirksam umgesetzt wird.

2.1.1 Verantwortung der wesentlichen und wichtigen Einrichtungen in der NIS-2-Richtlinie

Die NIS-2-Richtlinie der Europäischen Union verfolgt das Ziel, das Cybersicherheitsniveau wesentlicher Infrastrukturen und wichtiger Sektoren zu erhöhen. Für als „wesentlich“ oder „wichtig“ eingestufte Einrichtungen legt diese konkrete Pflichten fest. Diese Verpflichtungen erstrecken sich auf ein wirksames Risikomanagement, die Implementierung angemessener technischer und organisatorischer Schutzmaßnahmen, die fristgerechte Meldung von Sicherheitsvorfällen sowie die Orientierung an etablierten internationalen Normen.

2.1.2 Risikomanagement und Sicherheitsmaßnahmen

Das Risikomanagement spielt eine zentrale Rolle in der NIS-2-Richtlinie. Wesentliche und wichtige Einrichtungen müssen sicherstellen, dass diese Cybersicherheitsrisiken angemessen bewerten und bewältigen. Dies erfordert die Einführung eines robusten

Risikomanagementsystems, das verschiedene Sicherheitsmaßnahmen umfasst. Zu den Anforderungen gehören:

Risikobewertung

Wesentliche und wichtige Einrichtungen führen systematische Analysen durch, um potenzielle Gefährdungen ihrer Netz- und Informationssysteme zu identifizieren. Dabei werden sowohl physische Bedrohungen, beispielsweise Naturereignisse oder Diebstahl, als auch digitale Angriffe wie Hackerangriffe, Malware- oder Ransomware-Vorfälle berücksichtigt (Europäische Union, 2022).

Implementierung von Maßnahmen

Auf Basis der identifizierten Risiken setzen die Einrichtungen angemessene technische und organisatorische Schutzvorkehrungen um, die das Risiko erheblich reduzieren. Typische Instrumente sind Firewalls, Intrusion-Detection-Systeme und Verschlüsselungslösungen. Diese Vorkehrungen sollen Vorfälle verhindern und im Ereignisfall eine rasche sowie wirksame Reaktion ermöglichen (Europäische Union, 2022).

Schutz von Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit

Die Richtlinie verlangt Maßnahmen, die die kontinuierliche Verfügbarkeit der Systeme, die Echtheit der Daten, deren Unverfälschtheit und die Vertraulichkeit gewährleisten. Sowohl bei Speicherung als auch bei Übertragung ist sicherzustellen, dass ausschließlich autorisierte Personen Zugriff erhalten und Daten unverändert bleiben (Europäische Union, 2022).

Kontinuierliche Sicherheitsüberwachung

Einrichtungen etablieren Prozesse zur fortlaufenden Überwachung ihrer Netz- und Informationssysteme. Regelmäßige Audits, Tests und Schwachstellenanalysen dienen dazu, Sicherheitslücken frühzeitig zu erkennen und umgehend geeignete Gegenmaßnahmen einzuleiten (Europäische Union, 2022).

2.1.3 Technische und organisatorische Sicherheitsmaßnahmen

Neben dem allgemeinen Risikomanagement schreibt die NIS-2-Richtlinie explizit technische und organisatorische Maßnahmen vor, die von den wesentlichen und wichtigen Einrichtungen umgesetzt werden müssen. Diese betreffen unter anderem die folgenden Punkte:

Netzwerksicherheit

Die Richtlinie verlangt eine Absicherung der Netz- und Informationssysteme durch zeitgemäße Schutzlösungen wie Firewalls, Intrusion-Prevention-Systeme und eine konsequente Netzwerksegmentierung. Insbesondere sind kritische Segmente separat zu schützen, um unbefugte Zugriffe zu verhindern und den stabilen Betrieb der Infrastruktur sicherzustellen (Europäische Union, 2022).

Physische Sicherheit

Einrichtungen implementieren Maßnahmen, die Gebäude, Serverräume und sonstige sensible Bereiche vor physischen Bedrohungen bewahren. Zugang erhalten ausschließlich autorisierte Personen; Videoüberwachung, Zutrittskontrollen und Alarmanlagen bilden hierfür wesentliche Komponenten (Europäische Union, 2022).

Datensicherheit

Die Vertraulichkeit und Integrität von Daten ist zu gewährleisten. Verschlüsselungsverfahren und differenzierte Zugriffssteuerungen sorgen dafür, dass nur berechtigte Personen sensible Informationen nutzen können. Gleiches gilt für die Sicherstellung der Datenintegrität während Übertragung und Speicherung (Europäische Union, 2022).

Lieferkettensicherheit

Da Abwasserdienstleister vielfach Drittanbieter, beispielsweise für Cloud- oder Sicherheitsdienste, einbinden, ist die Cyberresilienz entlang der gesamten Lieferkette zu prüfen. Hierzu zählt die Evaluation der Sicherheitsvorkehrungen der Partner sowie die vertragliche Verpflichtung auf vergleichbare Schutzstandards (Europäische Union, 2022).

2.1.4 Berichtspflichten und Meldeverfahren

Eine wesentliche Neuerung der NIS-2-Richtlinie ist die Einführung strengerer Meldepflichten. Alle wesentlichen und wichtigen Einrichtungen müssen relevante Cybersicherheitsvorfälle melden. Diese Berichtspflichten umfassen:

Meldung erheblicher Sicherheitsvorfälle

Erhebliche Vorfälle, die die Kontinuität der angebotenen Dienste oder den Betrieb der Netz- und Informationssysteme beeinträchtigen, sind unverzüglich an die zuständige nationale Behörde zu melden, um rasche Gegenmaßnahmen zu ermöglichen (Europäische Union, 2022).

Inhalt der Meldung

Die Mitteilung umfasst eine Beschreibung des Vorfalls, die ergriffenen Sofortmaßnahmen, die geschätzten Auswirkungen auf den Dienstbetrieb, die Dauer des Vorfalls, betroffene Systeme und Daten sowie identifizierte Schwachstellen (Europäische Union, 2022).

Zusammenarbeit mit Behörden und CSIRTs

Über die Meldung hinaus stellen Einrichtungen alle relevanten Informationen bereit, die für die Analyse des Vorfalls und die Umsetzung angemessener Abhilfemaßnahmen erforderlich sind. Hierzu zählt die aktive Kooperation mit der jeweiligen Behörde und den zuständigen Computer-Sicherheitsvorfall-Teams (Europäische Union, 2022).

2.1.5 Einhaltung internationaler und europäischer Standards

Die NIS-2-Richtlinie verpflichtet wesentliche und wichtige Einrichtungen, ihre Cybersicherheits-strategien an international anerkannten Normen auszurichten und bewährte Verfahren umzusetzen (Europäische Union, 2022).

Orientierung an bestehenden Normen

Die konsequente Anwendung von Normen wie ISO/IEC 27001 für das Informationssicherheits-management gewährleistet, dass Risikoanalysen, Sicherheitsmaßnahmen, Audits und die kontinuierliche Verbesserung systematisch verankert sind. Auf diese Weise lässt sich sicherstellen, dass alle relevanten Sicherheitsdimensionen abgedeckt werden (Europäische Union, 2022).

Förderung bewährter Verfahren

Die Europäische Union und die Mitgliedstaaten unterstützen den Austausch bewährter Vorgehensweisen, um eine kohärente Umsetzung der Richtlinie zu ermöglichen. Leitlinien für spezifische Sektoren, beispielsweise Wasser- und Abwasserwirtschaft, adressieren sektorspezifische Herausforderungen und erleichtern eine einheitliche Anwendung der Sicherheitsanforderungen (Europäische Union, 2022).

2.1.6 Zusätzliche Verpflichtungen für die Einrichtungen

Die Richtlinie verlangt neben den technischen und organisatorischen Schutzvorkehrungen weitere flankierende Maßnahmen (Europäische Union, 2022).

Mitarbeiterschulung und Sensibilisierung

Einrichtungen stellen sicher, dass Beschäftigte regelmäßig geschult werden, um ein ausgeprägtes Bewusstsein für Cyberbedrohungen zu entwickeln. Schulungsinhalte umfassen den Umgang mit sensiblen Informationen sowie die Erkennung von Phishing-Angriffen und vergleichbaren Gefährdungen.

Verpflichtung zur kontinuierlichen Verbesserung

Die getroffenen Sicherheitsmaßnahmen unterliegen einer laufenden Überprüfung und Anpassung. Sicherheitsvorfälle und identifizierte Schwachstellen werden systematisch analysiert, um das Schutzniveau fortlaufend zu steigern und künftige Risiken zu minimieren.

Durch die Kombination aus international anerkannten Normen, bewährten Verfahren, regelmäßigen Schulungen und einer fortwährenden Optimierung der Sicherheitsmaßnahmen leisten wesentliche und wichtige Einrichtungen einen substantiellen Beitrag zur Resilienz kritischer Infrastrukturen und tragen zur Stabilität des europäischen Binnenmarktes bei.

2.2 Informationssicherheits- und Cybersecurityframeworks und –leitfäden

Im Zuge der Recherche konnten die nachfolgend angeführten Informationssicherheits- und Cybersecurityframeworks identifiziert werden.

2.2.1 Österreichisches Sicherheitshandbuch

Das Österreichische Informationssicherheitshandbuch erläutert eine systematische Vorgehensweise zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) in Unternehmen und Einrichtungen der öffentlichen Verwaltung. Neben methodischen Anleitungen bietet es übergreifende Inhalte zur Informationssicherheit sowie thematische Schwerpunkte, beispielsweise zur Nutzung von Smartphones, Cloud-Diensten und sozialen Medien, die ebenfalls für Privatpersonen Relevanz besitzen.

2.2.2 IT-Grundschutzkompendium des BSI

Das IT-Grundschutzkompendium bildet gemeinsam mit den BSI-Standards die maßgebliche Grundlage für eine umfassende Informationssicherheitspraxis. Den Kern bilden die IT-Grundschutz-Bausteine, die jeweils ein Themenfeld aus mehreren sicherheitsrelevanten Blickwinkeln beleuchten. Jeder Baustein beginnt mit einer Bedrohungsdarstellung und leitet daraus verbindliche Sicherheitsanforderungen ab. Die Bausteine sind zehn Kategorien wie Anwendungen (APP), Industrielle IT (IND) oder Sicherheitsmanagement (ISMS) zugeordnet und decken dadurch ein breites Themenspektrum ab. Eine aktualisierte Edition erscheint jährlich im Februar; Entwürfe neuer Bausteine werden fortlaufend veröffentlicht und können von Anwenderinnen und Anwendern kommentiert werden. Praxisorientierte Umsetzungshinweise zeigen, wie die Anforderungen erfüllt werden können und bleiben seit der Edition 2020 versionsunabhängig nutzbar. Bereits während der Erstellung der Bausteine erfolgte eine Risikobewertung für Bereiche mit normalem Schutzbedarf, sodass die Anforderungen dem Stand der Technik entsprechen.

2.2.3 ISO 27000er-Normenfamilie

Die ISO/IEC-27000-Normenfamilie (ISO27K) umfasst zahlreiche Informationssicherheits-standards, die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) veröffentlicht werden. Die Reihe definiert bewährte Verfahren für den Umgang mit Informationsrisiken und liefert ein umfassendes Rahmenwerk für ein ISMS. Dieses Managementsystem orientiert sich an etablierten Systemen, etwa zur Qualitätssicherung oder zum Umweltschutz, und integriert gezielt Sicherheits-, Datenschutz- und IT-Belange. Die Normen lassen sich branchenunabhängig anwenden, da die Sicherheitsmaßnahmen flexibel an die spezifischen Anforderungen und Risiken jeder Organisation anpassbar sind. Das ISMS-Konzept beruht auf kontinuierlichem Feedback und laufender Verbesserung, um neue Bedrohungen oder Schwachstellen angemessen zu adressieren. Die Einhaltung der ISO-27000-Standards gilt daher als wichtiger Schritt auf dem Weg zu einem umfassenden Schutzprogramm. Die Pflege und Weiterentwicklung der Normenreihe erfolgen im internationalen Gremium ISO/IEC JTC 1 SC 27, das sich halbjährlich trifft.

2.2.4 B3S Branchenspezifischer Sicherheitsstandard Wasser/Abwasser

Der Branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA) stellt einen IT-Sicherheitsleitfaden dar, der speziell für die kritischen Infrastrukturen der Trinkwasserversorgung und Abwasserentsorgung in Deutschland ausgearbeitet wurde. Er basiert auf dem IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) und definiert die Mindestanforderungen an die Informations- und Cybersicherheit für Betreiber dieses Sektors. Das Ziel ist die Unterstützung der Betreiber bei der Einführung und Aufrechterhaltung von Sicherheitsmaßnahmen, die den gesetzlichen Anforderungen, beispielsweise dem BSI-Gesetz und dem IT-Sicherheitsgesetz, genügen.

Der Standard wird im zweijährigen Rhythmus überarbeitet, um sowohl dem Stand der Technik als auch den gesetzlichen Vorgaben zu entsprechen. Die Aktualisierung erfolgt in enger Kooperation mit dem BSI und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Die Edition 2023 berücksichtigt erstmals ausdrücklich die Anforderungen der NIS-2-Richtlinie sowie die Vorgaben des neuen NIS2UmsuCG-Gesetzes. Diese wendet sich an Betreiber kritischer Infrastrukturen der Trinkwasserversorgung und Abwasserentsorgung und bietet konkrete Hilfestellungen für den Nachweis gemäß § 8a BSIG.

Für die Zukunft ist vorgesehen, den B3S WA kontinuierlich an aktuelle Sicherheitsstandards anzupassen. Durch die fortlaufende Weiterentwicklung in Abstimmung mit dem BSI fungiert der Standard als verlässliche Grundlage für den nachhaltigen Schutz dieser kritischen Infrastrukturen.

2.2.5 ÖWAV-Arbeitsbehelf zur IKT-Sicherheit im Bereich Abwasser

Der ÖWAV-Arbeitsbehelf 67 dient als praxisnaher Leitfaden für Betreiber abwassertechnischer Anlagen, um die Informations- und Kommunikationssicherheit in diesem kritischen Sektor zu erhöhen. Die Publikation wurde vom Österreichischen Wasser- und Abfallwirtschaftsverband (ÖWAV) erstellt und berücksichtigt die herausgehobene Bedeutung jener Anlagen für die öffentliche Gesundheit und die Grundversorgung.

Ziel und Zielgruppe

Adressiert werden Betreiber aller Größenkategorien, Planungsbüros sowie IKT-Verantwortliche. Der Leitfaden unterstützt beim Entwurf sicherer Anlagen und bei der Verbesserung bestehender Strukturen, um den Regelbetrieb zuverlässig zu gewährleisten.

Risikoanalyse und Maßnahmenplanung

Ein risikobasierter Ansatz ermöglicht die systematische Identifikation, Analyse und Priorisierung relevanter Gefährdungen. Darauf aufbauend werden Sicherheitsmaßnahmen konzipiert, die die spezifischen Risiken der jeweiligen Anlage adressieren.

Maßnahmenkatalog

Der Katalog enthält konkrete Empfehlungen zur Steigerung der Resilienz abwassertechnischer IKT-Systeme. Beispiele umfassen Netzwerksegmentierung, Schutz vor Schadsoftware sowie Vorkehrungen gegen unbefugten Zugriff.

Praxisorientierte Werkzeuge

Zur Umsetzung stellt der Arbeitsbehelf Excel-Vorlagen bereit, die die Risikoanalyse und die Dokumentation unterstützen.

Mindestanforderungen und kontinuierliche Verbesserung

Für kleinere Anlagen oder Betreiber, die zunächst keinen vollständigen risikobasierten Ansatz einführen können, definiert der Leitfaden ein eigenständiges Mindestniveau. Diese Anforderungen bilden eine Einstiegsebene für ein systematisches Sicherheitsmanagement.

Gesetze und Standards

Der Arbeitsbehelf berücksichtigt einschlägige Normen, beispielsweise ISO/IEC 27001 und IEC 62443, sowie das österreichische NIS-Gesetz. Dadurch wird eine Anschlussfähigkeit an internationale Standards gewährleistet.

2.2.6 KRITIS

Die KRITIS-Regulierung verpflichtet Betreiber Kritischer Infrastrukturen in Deutschland, die Vorgaben des BSI-Gesetzes umzusetzen. Damit soll die Versorgungssicherheit in den KRITIS-Sektoren durch verbindliche Betreiberpflichten im Bereich der Informations- und Cybersicherheit gewährleistet werden.

2.2.7 Cybersecurity Framework

Das Cybersecurity Framework (CSF) des amerikanischen National Institute of Standards and Technology (NIST) unterstützt Organisationen aller Größenordnungen und Branchen beim Management und der Reduktion von Cybersicherheitsrisiken. Das Rahmenwerk liefert sektor- und technologieneutrale Ergebnisse, die Führungskräfte, Managementebenen und Fachkräfte gleichermaßen nachvollziehen können. Es umfasst Kernkomponenten mit sechs Funktionen (Führen, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen) sowie zugehörige Kategorien und Unterkategorien, die die angestrebten Cybersicherheits-ergebnisse systematisieren. Mit Version 2.0 rücken die Themen Governance und Lieferketten in den Vordergrund. Sogenannte Quick-Start Guides erleichtern insbesondere kleineren Organisationen den Einstieg. Als gemeinsame Sprache verbessert das Framework die Kommunikation von Erwartungen, Planungen und Ressourcen im Kontext der Informations- und Cybersicherheit. Ferner lässt es sich flexibel in bestehende Risikomanagementprogramme integrieren, berücksichtigt individuelle Risikotoleranzen und unterstützt die kontinuierliche Anpassung der Sicherheitspraktiken an neue Bedrohungslagen sowie an technologische Entwicklungen.

2.2.8 Framework for Improving Critical Infrastructure Cybersecurity

Dieses Dokument des NIST adressiert Cybersicherheitsrisiken Kritischer Infrastrukturen und stellt Eigentümerinnen und Eigentümern ein flexibles, wiederholbares und freiwillig anwendbares Rahmenwerk bereit. Es gliedert sich in drei Hauptbestandteile: Framework-Profile, Implementierungsebenen und den Framework-Kern. Letzterer verweist auf Branchenstandards und Leitlinien, sodass Organisationen ihren aktuellen Reifegrad bestimmen und priorisierte Maßnahmen ableiten können, um definierte Sicherheitsziele effizient zu erreichen.

2.2.9 Cyber Assessment Framework

Das britische National Cyber Security Centre (NCSC) entwickelte das Cyber Assessment Framework (CAF), um eine einheitliche Bewertung der Cybersicherheitslage in den unter die NIS-Verordnungen fallenden Sektoren zu gewährleisten. Der ergebnisorientierte Ansatz dient ebenso der Selbstbewertung wie der aufsichtsrechtlichen Prüfung durch zuständige Behörden. Bewertet wird, ob das Schutzniveau einer Einrichtung im angemessenen Verhältnis zu den relevanten Risiken steht, die sowohl den eigenen Betrieb als auch von der Einrichtung unterstützte Funktionen betreffen.

2.2.10 Cyber Assessment Framework v3.0

Die Version 3.0 des CAF, veröffentlicht 2019 durch das NCSC, ermöglicht eine strukturierte Cybersicherheitsbewertung durch interne Teams oder externe Dienstleister. Die Bewertungsarchitektur umfasst vier Hauptziele: Schutz vor Cyberangriffen, Management von Sicherheitsrisiken, Erkennung von Cybersicherheitsvorfällen und Minimierung der Auswirkungen solcher Vorfälle. Diese Ziele werden in vierzehn Prinzipien und insgesamt neununddreißig spezifische Ergebnisse untergliedert. Für jedes Ergebnis ist festzustellen, ob es vollständig, teilweise oder nicht erreicht wurde; dadurch entsteht ein differenziertes Bild der Wirksamkeit der bestehenden Sicherheitsmaßnahmen im Verhältnis zum jeweiligen Risikoprofil.

3 BEFRAGUNG NIS2-BETROFFENER UNTERNEHMEN AUS DEM SEKTOR ABWASSER

Zur Beantwortung der Forschungsfrage kommt datenbasierte empirische Sozialforschung zum Einsatz. Diese umfasst Datenerhebung, -analyse und -auswertung auf der Grundlage qualitativer und quantitativer Methoden. Das Ziel ist die Beschreibung sozialer Wirklichkeiten, die Überprüfung der aufgestellten Theorie bzw. Hypothese sowie die Erarbeitung praxisorientierter Lösungsansätze und – sofern erforderlich – die Entwicklung neuer theoretischer Perspektiven.

3.1 Zielsetzung der Befragung

Die Befragung erfasst Umsetzungsstrategien, Standards und Herausforderungen von Abwasserdienstleistern sowie Good Practices und vorhandene Umsetzungshilfen, die zur unionsweiten Verbesserung des Cybersicherheitsniveaus beitragen können. Die erhobenen Daten bilden die Grundlage, um Good Practices zu identifizieren und Empfehlungen zur Optimierung der Cybersicherheitsmaßnahmen im Abwassersektor abzuleiten.

3.2 Design und Methodik der Befragung

Ausgehend vom aktuellen Forschungsstand, der identifizierten Forschungslücke und der praktischen Problemstellung in der Abwasserwirtschaft wurde eine mehrdimensionale Forschungsfrage entwickelt, die die Umsetzung der NIS-2-Richtlinie fokussiert. Zur empirischen Untersuchung dient eine standardisierte Online-Befragung auf Basis eines strukturierten Fragebogens. Dieses Verfahren ermöglicht eine systematische, vergleichbare und statistisch auswertbare Erhebung organisationaler Praktiken, Einschätzungen und Erfahrungen (Atteslander 2010; Schnell, Hill & Esser 2013).

Der Einsatz eines Mixed-Methods-Ansatzes (Creswell & Plano Clark 2018) verbindet quantitative Analysen, die generalisierbare Aussagen erlauben, mit qualitativen Elementen, die tiefergehende Einblicke in spezifische Herausforderungen und Good Practices liefern. Die Kombination beider Perspektiven gewährleistet eine differenzierte Betrachtung der organisatorischen Umsetzung der NIS-2-Richtlinie im Abwassersektor.

3.2.1 Planung und Konstruktion der Befragung zur Datenerhebung und des Fragenkataloges

Die Konzeption des Fragebogens stützte sich auf theoretische Vorüberlegungen und einschlägige Fachliteratur. Ziel war die Operationalisierung valider und reliabel messbarer Indikatoren für das untersuchte Verhalten. Klare, verständliche und neutrale Formulierungen der Items minimieren Verzerrungen durch Suggestion oder Mehrdeutigkeit (Porst 2014).

Auf Grundlage der Anforderungen der NIS-2-Richtlinie im Kontext kritischer Infrastrukturen wurden die strukturellen, organisatorischen und technischen Vorgaben in sieben Themenkategorien (TK) überführt:

Themenkategorie 1 – Governance

Themenkategorie 2 – Organisatorische Maßnahmen – Strukturelle Organisation der Cybersicherheit

Themenkategorie 3 – Risiko- und Incidentmanagement

Themenkategorie 4 – Technische Maßnahmen

Themenkategorie 5 – physische Maßnahmen

Themenkategorie 6 – Cybersicherheitsframeworks, -standards, -leitfäden

Themenkategorie 7 – Anregungen für zukünftige Leitfäden/Standards zur NIS-2

Innerhalb dieser Kategorien kamen geschlossene Fragen mit Multiple-Choice-Formaten und optionalen Freitexteinträgen ebenso zum Einsatz wie offene Fragen. Die geschlossenen Items erfassen Umsetzungsmaßnahmen, Herausforderungen und Zuständigkeiten systematisch; die offenen Items ermöglichen individuelle Einschätzungen und kontextspezifische Darstellungen. Präzise und neutrale Formulierungen gewährleisten die inhaltliche Validität. Der Fragebogen ist in Anhang A1 enthalten.

3.2.2 Durchführung eines Pre-Tests

Zur Prüfung von Verständlichkeit und Funktionalität wurde ein Pre-Test mit einer kleinen Stichprobe von Branchenvertretern durchgeführt. Die Rückmeldungen flossen in die finale Fassung ein und verbesserten Verständlichkeit sowie Praktikabilität.

3.2.3 Auswahl der Zielgruppe bzw. Stichprobe

Als Zielgruppe wurden insgesamt Unternehmen und Abwasserverbände aus dem deutschsprachigen Raum definiert. Die Datenerhebung erfolgte über die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA), die den Fragebogen an sämtliche Mitglieder des Erfahrungsaustauschkomitees der Großstädte versandte.

3.2.4 Planung der Datenauswertung

Für die deskriptiv-statistische Analyse wurden zunächst die absoluten Häufigkeiten der gewählten Antwortoptionen erfasst und anschließend in Prozentwerte umgerechnet. Die Prozentangaben beziehen sich auf die Gesamtzahl der Teilnehmer, die die jeweilige Frage beantworteten. Dieses Vorgehen gewährleistet eine übersichtliche Darstellung der Verteilungen und ermöglicht erste Rückschlüsse auf das Verhalten der befragten Unternehmen (Diekmann 2017). Die geschlossenen Fragen sahen Mehrfachnennungen und ergänzende Freitexteinträge vor; dadurch lässt sich die Mehrdimensionalität der Problemlage angemessen abbilden, und sowohl

parallele Maßnahmen als auch Herausforderungen innerhalb eines Unternehmens können quantitativ erfasst werden (Bortz & Döring 2006). Aufgrund des explorativen Charakters der wissenschaftlichen Arbeit war eine inferenzstatistische Auswertung nicht vorgesehen.

4 AUSWERTUNG UND ANALYSE DER DATEN

Im vorliegenden Kapitel werden die im Rahmen der empirischen Erhebung gewonnenen Daten systematisch ausgewertet und analysiert. Das Ziel ist es, die zentralen Forschungsfragen zu beantworten und die aufgestellte Hypothese anhand der erhobenen Daten zu überprüfen. Die Auswertung erfolgt sowohl deskriptiv-statistisch, unter Angabe der absoluten Häufigkeiten sowie deren prozentualem Anteil an der Gesamtzahl der antwortgebenden Organisationen (N), als auch qualitativ-inhaltlich, um ein umfassendes Bild des Datenbestands zu erhalten.

Zunächst werden die allgemeinen Merkmale der Stichprobe beschrieben, um einen Überblick über die Zusammensetzung der Befragungsteilnehmern zu bieten. Anschließend folgt die detaillierte Auswertung der einzelnen Themenbereiche der Befragung; dabei werden quantitative Zusammenhänge, relevante Tendenzen und auffällige Verteilungen herausgearbeitet.

Die Ergebnisse werden strukturiert und nachvollziehbar unter Verwendung von Diagrammen präsentiert; dies gewährleistet eine transparente und anschauliche Darstellung der Befunde, die im nachfolgenden Kapitel inhaltlich interpretiert und in den Kontext der Forschungsfragen sowie des theoretischen Rahmens eingeordnet werden.

4.1 Methoden zur Auswertung und Analyse der Antworten

Die Antworten auf die Fragen wurden mittels standardisierter Online-Befragung erhoben. Mehrfachnennungen (Multiple Choice) waren möglich.

4.1.1 Quantitative Datenanalyse der Befragungsantworten

Die absoluten Häufigkeiten der gewählten Antwortoptionen wurden erfasst und in Prozentwerte in Bezug zur Gesamtzahl der antwortenden Teilnehmer umgerechnet. Die Darstellung erfolgt deskriptiv-statistisch, um Rückschlüsse auf das Verhalten der befragten Unternehmen zu ermöglichen.

4.1.2 Qualitative Datenanalyse der Befragungsantworten

Zur Vertiefung der quantitativen Ergebnisse wurden im Fragebogen zusätzlich Optionen für Freitextantworten und offene Fragen integriert, um individuelle Einschätzungen zu bedeutsamen Good Practices bei der Umsetzung der NIS-2-Richtlinie zu erfassen. Für die Auswertung und inhaltliche Strukturierung dieser Freitextantworten kam die qualitative Inhaltsanalyse nach Mayring (2015) zum Einsatz. Ziel war die Identifikation wiederkehrender Argumentationsmuster, die thematischen Kategorien (Cluster) zugeordnet wurden. Hierzu diente ein induktives Kategorienbildungssystem, das eine strukturierende Analyse ermöglichte. Die Antworten wurden paraphrasiert, thematisch reduziert und zu Oberkategorien zusammengeführt, um wesentliche thematische Cluster systematisch abzubilden. Die Kategorien basierten auf inhaltlichen

Ähnlichkeiten; methodische und branchenspezifische Aspekte dienten als zusätzliche Differenzierungskriterien. Als Analyseeinheit fungierte jede einzelne inhaltliche Aussage zum Thema und wurde für die Häufigkeitszählung herangezogen. Die so erhobenen Häufigkeiten verdeutlichten Relevanz und Verbreitung der Aussagen. Anschließend erfolgte die Interpretation der Ergebnisse. Diese Methodik gestattete auch bei begrenzter Zahl an Freitextantworten eine strukturierte und vergleichbare Auswertung.

4.2 Auswertung der Fragen aus Themenkategorie 1 „Governance“

Dieses Kapitel präsentiert die Auswertungen der Fragen zur Governance im Rahmen der NIS-2-Umsetzung.

4.2.1 Frage 1: Wie ist die Cybersicherheit in Ihrem Unternehmen strukturell organisiert?

Insgesamt übermittelten 13 Unternehmen Angaben zur strukturellen Organisation der Cybersicherheit. Da Mehrfachnennungen zulässig waren, übersteigt die Summe der Nennungen 100 %.

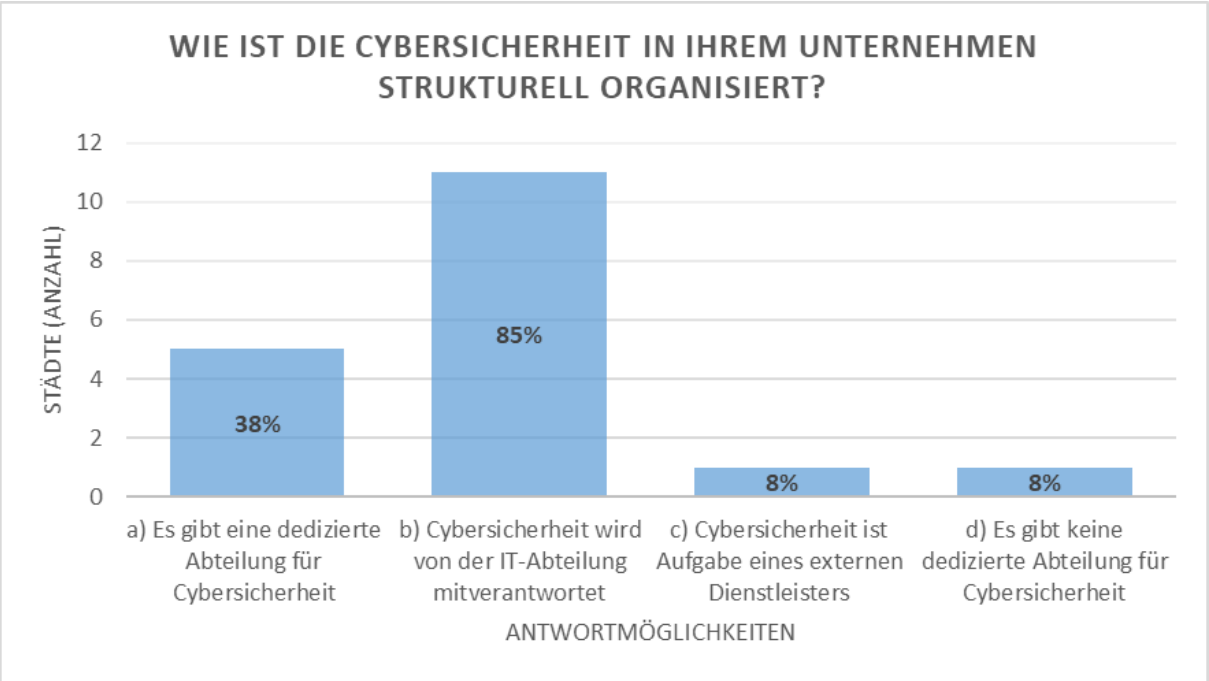

Abbildung 1: Strukturelle Organisation der Cybersicherheit

Die Analyse zur organisatorischen Verankerung der Cybersicherheit zeigt, dass in der Mehrheit der befragten Unternehmen (85 %, n = 11) die Verantwortung für Cybersicherheit in die bestehende IT-Abteilung integriert ist. Dieses Modell stellt somit die häufigste Strukturform dar und verweist auf eine enge Verzahnung von IT- und Sicherheitsfunktionen.

In 38 % der Unternehmen (n = 5) existiert zusätzlich eine eigenständige Abteilung für Cybersicherheit. Diese Ausprägung lässt auf ein höheres Maß an Spezialisierung sowie eine stärkere Priorisierung des Themas innerhalb der Unternehmensorganisation schließen.

Lediglich ein Unternehmen (8 %) gab an, Cybersicherheitsaufgaben vollständig an einen externen Dienstleister ausgelagert zu haben. Ein weiteres Unternehmen (ebenfalls 8 %) verfügt über keine dedizierte organisatorische Einheit für Cybersicherheit.

Insgesamt lässt sich festhalten, dass Cybersicherheit in den meisten Fällen integraler Bestandteil der internen IT-Strukturen ist. Die Einrichtung spezialisierter Einheiten oder die vollständige Auslagerung an externe Stellen stellt hingegen eine weniger verbreitete Ausnahme dar.

4.2.2 Frage 2: Welche Führungsebene ist in ihrem Unternehmen für Cybersicherheit bzw. die Umsetzung der NIS-2-RL verantwortlich?

Diese geschlossene Frage wurde von 13 Unternehmen beantwortet. Mehrfachnennungen waren möglich; die Prozentwerte beziehen sich folglich auf den jeweiligen Anteil an der Gesamtstichprobe (N = 13) und können sich auf über 100 % summieren.

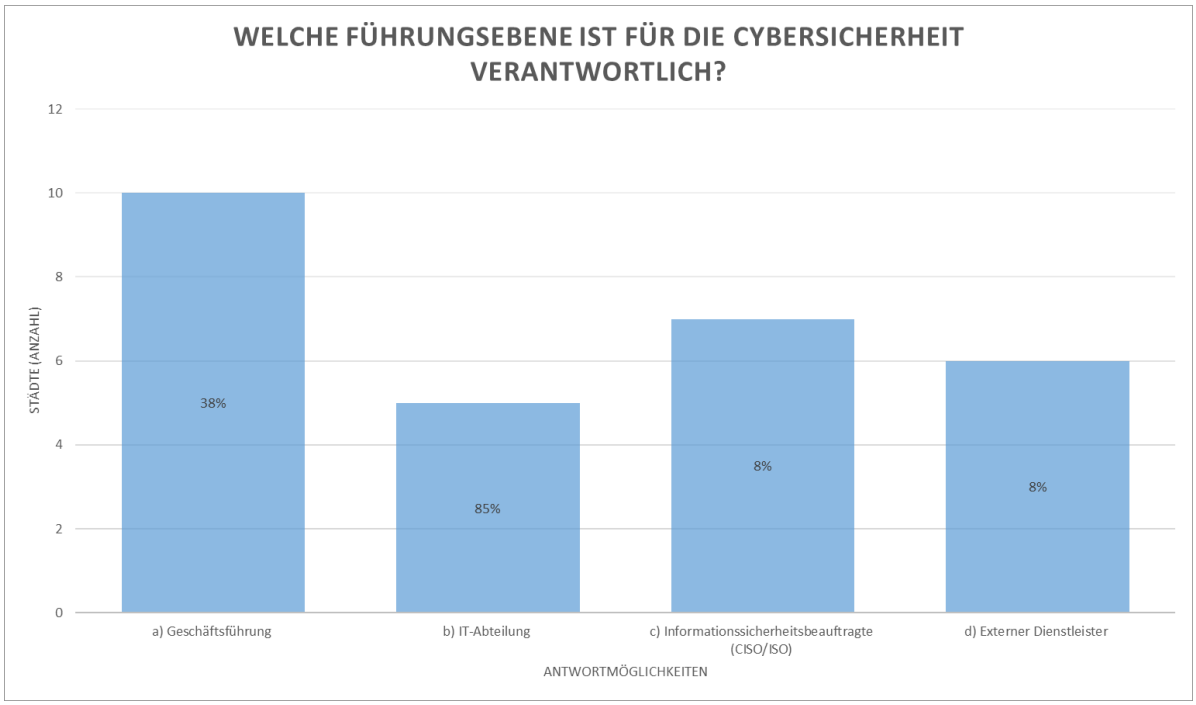

Abbildung 2: Für Cybersicherheit verantwortliche Führungsebenen

Die Analyse der Verantwortungsstrukturen für Cybersicherheit in den befragten Unternehmen ergibt ein differenziertes Bild. Bei zehn Einrichtungen (77 %) liegt die primäre Verantwortung auf Geschäftsführungsebene, was die strategische Bedeutung des Themas und dessen Verankerung bei der obersten Entscheidungsebene unterstreicht. Sieben Organisationen (54 %) benennen spezialisierte Fachfunktionen, etwa Informationssicherheitsbeauftragte (CISO/ISO), als zuständig. Damit deutet sich ein gestiegenes Professionalisierungsniveau an, das über rein

technische Zuständigkeiten hinausgeht und stärker normative sowie prozessuale Anforderungen berücksichtigt. Externe Dienstleister übernehmen in sechs Fällen (46 %) zentrale Aufgaben, womit Outsourcing-Strategien an Bedeutung gewinnen, beispielsweise in Bezug auf spezifisches Fachwissen, Effizienzgewinne oder eine geringe interne Ressourcenausstattung. Bei fünf Unternehmen (38 %) ist die Verantwortung innerhalb der IT-Abteilung verortet, was vor allem bei kleineren oder weniger spezialisierten Organisationen zu beobachten ist. Zwei Einrichtungen (15 %) wählten die Option „Sonstiges“; deren offene Angaben verweisen auf interdisziplinäre Zuständigkeitsmodelle bzw. projektbasierte Rollenzuweisungen und lassen flexible oder hybride Organisationsformen erkennen. Insgesamt wird Cybersicherheit als unternehmensweite Querschnittsaufgabe verstanden, die sowohl auf Leitungsebene als auch in spezialisierten Rollen und externen Partnerschaften verankert ist. Die Vielfalt der Zuständigkeitsmodelle spiegelt unterschiedliche Reifegrade, strategische Prioritätensetzungen und Ressourcenausstattungen wider.

4.2.3 Frage 3: Welche Governance-Maßnahmen setzen sie zur Erfüllung der NIS-2-Richtlinie um?

Diese geschlossene Frage mit ergänzender Freitextoption beantworteten 13 Unternehmen. Die nachfolgende Abbildung 3 fasst die von den befragten Organisationen implementierten Governance-Maßnahmen zur Erfüllung der Anforderungen der NIS-2-Richtlinie zusammen und zeigt die Häufigkeit der Nennungen in Prozent.

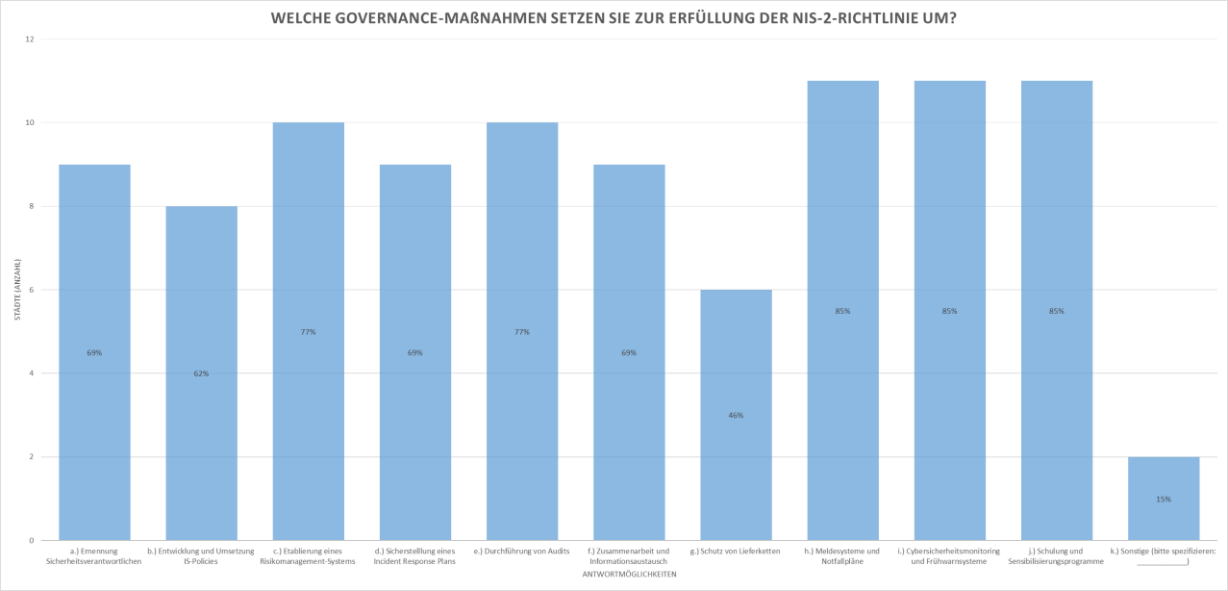

Abbildung 3: Governance-Maßnahmen zur Umsetzung der NIS-2-Anforderungen

Die Auswertung der erhobenen Daten verdeutlicht, dass die befragten Unternehmen eine breite Palette an Governance-Maßnahmen implementiert haben, um die Anforderungen der NIS-2-Richtlinie zu erfüllen.

Besonders häufig kommen Meldesysteme und Notfallpläne, Cybersicherheits-monitoring und Frühwarnsysteme sowie Schulungs- und Sensibilisierungsprogramme zum Einsatz. Diese drei Instrumente wurden jeweils von 85 % der Unternehmen (n = 11) genannt und repräsentieren damit die am weitesten verbreiteten Elemente der Cybersicherheitsgovernance. Dadurch entsteht ein ganzheitliches Verständnis von Prävention, Reaktion und kontinuierlicher Bewusstseinsbildung innerhalb der Organisationen.

Strukturverankernde und evaluierende Maßnahmen, etwa die Etablierung eines Risikomanagementsystems und die Durchführung regelmäßiger Audits, sind mit jeweils 77 % (n = 10) ebenfalls stark vertreten. Diese Instrumente gestatten es, Risiken systematisch zu identifizieren, zu bewerten und fortlaufend zu überwachen, wodurch die Resilienz gegenüber Sicherheitsvorfällen gestärkt wird.

Weitere häufig genannte Maßnahmen (jeweils 69 %, n = 9) umfassen die Benennung von Sicherheitsverantwortlichen, die Einrichtung eines Incident-Response-Plans sowie die Förderung von Kooperation und Informationsaustausch – sowohl organisationsintern als auch mit externen Stellen. Diese Aspekte erhöhen die operative Handlungsfähigkeit im Ernstfall und unterstützen eine übergreifende Sicherheitskultur.

Mit 62 % (n = 8) wurde auch die Entwicklung und Implementierung unternehmensinterner Informationssicherheitspolicies (IS-Policies) häufig realisiert. Solche formalen Regelwerke fördern die Standardisierung und institutionelle Verankerung sicherheitsrelevanter Prozesse.

Der Schutz von Lieferketten wurde hingegen lediglich von 46 % der Befragten (n = 6) angegeben, obwohl dieser Aspekt in der NIS-2-Richtlinie besondere Bedeutung besitzt. Diese Diskrepanz weist auf Herausforderungen oder Nachholbedarf in diesem Bereich hin.

In 15 % der Fälle (n = 2) nannten die Teilnehmer unter der Kategorie „Sonstige“ individuelle Maßnahmen, welche organisationsspezifische Ansätze oder ergänzende Strategien widerspiegeln.

Insgesamt belegt das Ergebnis ein hohes Maß an struktureller, strategischer und operativer Umsetzung von Cybersicherheitsmaßnahmen. Die Bandbreite und Häufigkeit der realisierten Instrumente verdeutlichen, dass zahlreiche Unternehmen bereits ganzheitliche Governance-Modelle verfolgen, um regulatorischen Vorgaben zu genügen und zugleich ein dauerhaft belastbares Sicherheitsniveau zu etablieren.

4.3 Auswertung der Fragen aus Themenkategorie 2 „Organisatorische Maßnahmen“

Dieses Kapitel enthält die Auswertung der Frage zu den organisatorischen Maßnahmen im Rahmen der NIS-2-Umsetzung.

4.3.1 Frage 4: Welche organisatorischen Maßnahmen haben Sie zur Sicherstellung der Cybersicherheit gemäß der NIS-2-Richtlinie implementiert?

Insgesamt wurden 13 gültige Rückmeldungen verarbeitet. Da Mehrfachnennungen zulässig waren, übersteigt die Summe der Prozentwerte 100 %. Die Ergebnisse sind anhand der Abbildung 4 dargestellt:

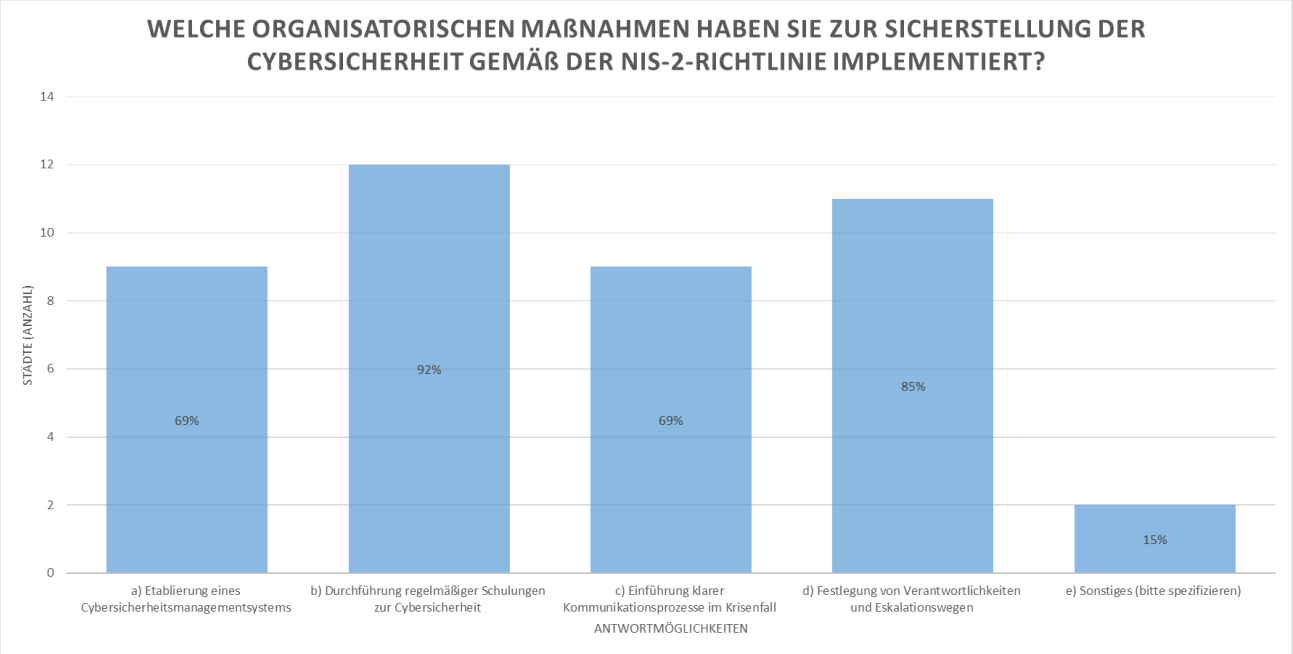

Abbildung 4: Organisatorische Maßnahmen zur Sicherstellung der Cybersicherheit

Die Verteilung belegt, dass sich die Mehrheit der Unternehmen systematisch und ganzheitlich mit organisatorischen Anforderungen auseinandersetzt, beispielsweise durch strukturierte Schulungen, Zuständigkeiten und geregelte Prozesse für Notfälle.

Ergebnisse:

Die befragten Unternehmen wenden für die Umsetzung der NIS-2-Richtlinie vielfältige organisatorische Maßnahmen an. Auffällig ist, dass 92 % der Befragten (n = 12) regelmäßige Schulungen zur Cybersicherheit durchführen; damit wird die Qualifikation der Mitarbeiter als Fundament wirksamer Sicherheitsmaßnahmen hervorgehoben.

Ebenfalls häufig genannt wurde die Festlegung von Verantwortlichkeiten und Eskalationswegen: 85 % der Unternehmen (n = 11) haben entsprechende Strukturen etabliert, was auf eine bewusste Risikoverteilung und eindeutige Rollenzuordnung schließen lässt.

Die Einführung klarer Kommunikationsprozesse im Krisenfall sowie die Einrichtung eines Cybersicherheitsmanagementsystems (CSMS) wurden jeweils von 69 % der Teilnehmer (n = 9) berichtet. Diese Maßnahmen stärken sowohl die präventive als auch die reaktive Handlungsfähigkeit bei sicherheitsrelevanten Vorfällen.

Die Antwortoption „Sonstiges“ wählten 15 % der Organisationen (n = 2). Die zugehörigen Angaben verweisen auf individuelle oder branchenspezifische organisatorische Praktiken, die über die genannten Standardmaßnahmen hinausgehen.

Interpretation

Die Ergebnisse zeigen, dass neben technischen Vorkehrungen verstärkt organisatorische Sicherheitsmechanismen etabliert werden, um die Anforderungen der NIS-2-Richtlinie umfassend zu erfüllen.

4.4 Auswertung der Fragen aus Themenkategorie 3 „Risikomanagement“

Im Folgenden werden die Antworten zu den Aspekten des Risikomanagements im Rahmen der NIS-2-Umsetzung ausgewertet und interpretiert.

4.4.1 Frage 5: Haben Sie ein Risikomanagementsystem für Informations- und Cybersicherheit implementiert?

Diese geschlossene Frage wurde von 13 Organisationen beantwortet. Die Teilnehmer wählten zwischen den Optionen Ja, Teilweise und Nein, um den Umsetzungsstand eines Risikomanagementsystems zu kennzeichnen.

Abbildung 5: Implementierung eines Risikomanagementsystems

Die Befragung verdeutlicht ein hohes Implementierungsniveau. Von 13 Unternehmen verfügen 54 % (n = 7) über ein vollständig implementiertes Risikomanagementsystem. Weitere 46 % (n = 6) berichten von einer teilweisen Umsetzung, beispielsweise in Form bereichsspezifischer Anwendungen oder noch nicht vollständig integrierter Komponenten. Kein Unternehmen verzichtet gänzlich auf ein Risikomanagementsystem. Dieses Ergebnis weist auf ein ausgeprägtes Problembewusstsein und auf die gestiegene Bedeutung strukturierter Risikoidentifikation sowie -steuerung hin.

Gleichzeitig zeigt sich ein Bedarf, vorhandene Teillösungen in ein ganzheitliches Managementsystem zu überführen. Vor dem Hintergrund der NIS-2-Richtlinie, die ein systematisches Risikomanagement explizit verlangt, markiert dieser Integrationsschritt einen wesentlichen Entwicklungspfad für die weitere Governance-Reife.

Interpretation

Risikomanagement stellt für die Mehrheit der Organisationen bereits eine etablierte Praxis dar. Die noch vorhandenen teilweisen Umsetzungen deuten jedoch auf Optimierungs-potenzial hinsichtlich eines durchgängig verankerten, organisationsweiten Ansatzes hin, wie ihn die NIS-2-Richtlinie fordert.

4.4.2 Frage 6: Welche der folgenden Risikoanalyseverfahren setzen Sie ein?

Diese geschlossene Frage mit optionaler Freitextkomponente beantworteten 13 Organisationen. Mehrfachnennungen waren möglich, um den Einsatz verschiedener Verfahren parallel abzubilden. Die Ergebnisse werden im folgenden Abschnitt quantitativ ausgewertet und qualitativ eingeordnet.

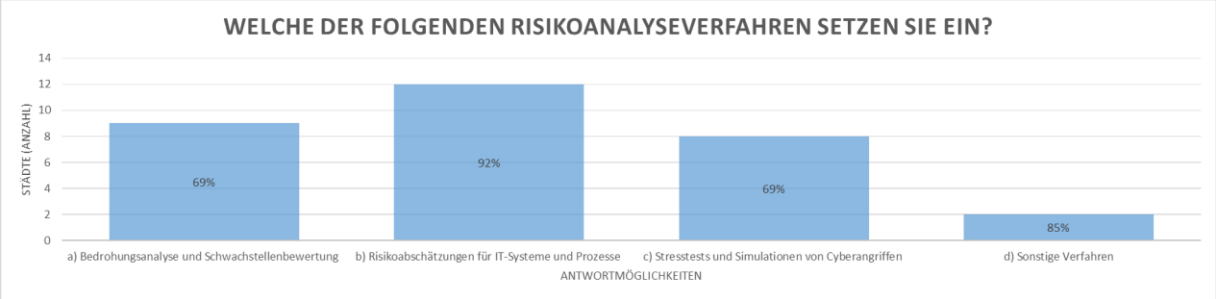

Abbildung 6: Eingesetzte Risikoanalyseverfahren

Die Befragung zur Anwendung spezifischer Verfahren der Risikoanalyse im Kontext der Informations- und Cybersicherheit zeigt, dass insbesondere klassische und etablierte Methoden weit verbreitet sind. Am häufigsten nannten 92 % der teilnehmenden Organisationen (n = 12) die Durchführung von Risikoabschätzungen für IT-Systeme und Geschäftsprozesse; diese Maßnahme bildet damit einen wesentlichen Baustein der unternehmensweiten Risikobewertung.

Bedrohungsanalysen und Schwachstellenbewertungen setzen 69 % der befragten Unternehmen (n = 9) ein. Diese Verfahren ermöglichen eine vertiefte Auseinandersetzung mit potenziellen Angriffsvektoren sowie technischen Schwachstellen innerhalb der IT-Infrastruktur.

Proaktive Ansätze, etwa Stresstests und Simulationen von Cyberangriffen, nutzen 62 % der Organisationen (n = 8). Mit diesen Instrumenten lässt sich die Reaktionsfähigkeit im Ernstfall überprüfen, und Sicherheitslücken werden unter realitätsnahen Bedingungen identifiziert.

Weitere Verfahren erfassten 15 % der Befragten (n = 2) unter der Kategorie „Sonstiges“, was auf individuelle oder spezialisierte Methoden einzelner Organisationen hinweist.

Qualitative Analyse der Freitextangaben in der Kategorie „Sonstiges“

Obwohl lediglich zwei Organisationen (15 % von N = 13) explizit weitere Verfahren beschrieben, verweisen die genannten Praktiken auf differenzierte, anlassbezogene Risikoanalysen, die über die etablierten Standardmethoden hinausgehen. Ein weiteres Unternehmen verzichtete auf Angaben zu dieser Frage.

Kategorie	Beschreibung	Häufigkeit
Zyklische und anlassbezogene Verfahren	Risikoanalysen erfolgen regelmäßig (zyklisch) und bei Bedarf (anlassbezogen), z. B. bei sicherheitsrelevanten Änderungen.	2
Standardspezifisches Vorgehen	Anwendung etablierter Normen wie ISO/IEC 27005 und BSI-Standards (z. B. BSI CSW, elementare Gefährdungen).	2
Technische Verfahren zur Bewertung	Nutzung konkreter Methoden wie Matching mit CVSS v3.1 zur Schwachstellenbewertung.	1
Prozessintegrierte Risikoanalysen	Eingebettete Risikoabschätzung z. B. im Change-Management-Prozess mittels reduzierter Risikobewertung.	1
Szenario-basierte Analyse	Einsatz von Szenarien zur Bewertung von Asset-bezogenen Risiken.	1

Tabelle 1: Sonstige eingesetzte Risikoanalysepraktiken

Die ergänzenden Freitextangaben belegen, dass neben den standardisierten Antwortoptionen auch detaillierte, praxisorientierte Verfahren eingesetzt werden. Besonders die zyklische und anlassbezogene Durchführung von Risikoanalysen in Kombination mit Normen wie ISO/IEC 27005 und dem Common Vulnerability Scoring System (CVSS) verweist auf eine systematische und zugleich adaptive Risikosteuerung. Die Einbindung in das Change-Management sowie die szenariobasierte Bewertung lassen auf eine fortschreitende Prozessintegration der Cybersicherheit schließen.

Interpretation

Die Ergebnisse verdeutlichen, dass in den untersuchten Unternehmen ein breites Spektrum strukturierter Risikoanalysemethoden Anwendung findet. Neben klassischen Risikoabschätzungen kommen vermehrt simulationsbasierte Verfahren zum Einsatz. Diese Entwicklung signalisiert ein wachsendes Sicherheitsbewusstsein und eine verstärkte Orientierung an den Anforderungen der NIS-2-Richtlinie, die ausdrücklich ein umfassendes Risikomanagementsystem und präventive Maßnahmen vorsieht.

4.4.3 Frage 7: Wie definieren Sie die Risikobewertungskriterien für die Cybersicherheit in Ihrem Unternehmen?

Insgesamt beantworteten 13 Unternehmen die geschlossene Frage mit Freitextoption. Mehrfachauswahl war möglich, sodass mehrere Quellen oder Verfahren gleichzeitig angegeben werden konnten.

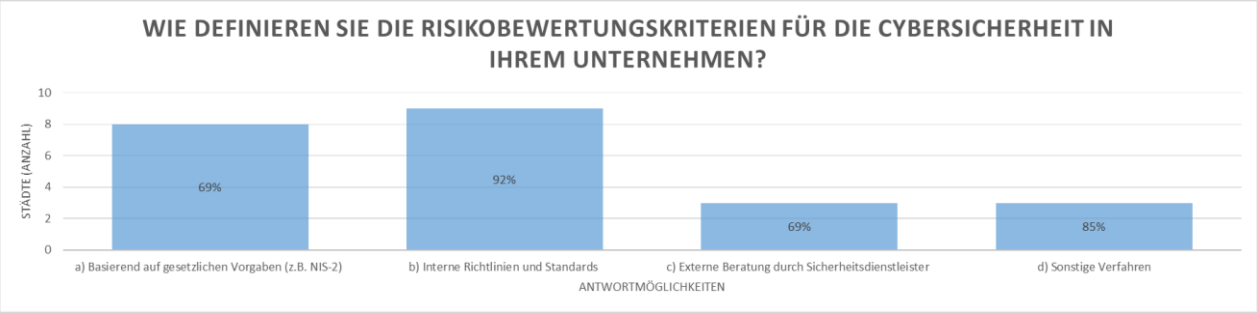

Abbildung 7: Risikobewertungskriterien für Cybersicherheitsrisiken

Die Auswertung der abgegebenen Antworten zeigt, dass 69 % der Organisationen (n = 9) vorrangig interne Richtlinien und Standards als Grundlage für ihre Risikobewertungskriterien verwenden. Diese Orientierung verdeutlicht gewachsene Governance-Strukturen sowie konsolidierte Erfahrungswerte innerhalb der Unternehmen, etwa in Form konzernweiter Vorgaben oder branchenspezifischer Regelwerke. Gesetzliche Anforderungen, insbesondere jene im Rahmen der NIS-2-Richtlinie, bilden in 62 % der Fälle (n = 8) einen wesentlichen Referenzrahmen. Das Ergebnis weist auf eine hybride Vorgehensweise hin, bei der externe Compliance-Vorgaben in bestehende interne Prozesse integriert werden.

Die Inanspruchnahme externer Beratung durch spezialisierte Sicherheitsdienstleister spielt mit 23 % (n = 3) eine vergleichsweise geringere Rolle, was auf bereits vorhandene interne Expertise oder bewusst aufgebautes Know-how schließen lässt. Ebenfalls 23 % der Organisationen (n = 3) nutzten die Kategorie „Sonstige“ und verweisen auf individuelle oder hochspezialisierte Bewertungsmethoden jenseits gängiger Standards.

Qualitative Auswertung der Kategorie „Sonstige Verfahren“

Kategorie	Beschreibung	Häufigkeit
Standardbasierte Risikomodelle	Anwendung internationaler Normen wie ISO/IEC 31000 und ISO/IEC 27005 zur systematischen Risikobewertung.	2
Berücksichtigung interessierter Parteien	Einbezug der Anforderungen interner und externer Stakeholder in die Risikobewertung.	1
Branchenspezifische Vorgaben	Nutzung von branchenspezifischen Standards wie B3S (Branchenspezifischer Sicherheitsstandard) und DWA M-1060.	1

Tabelle 2: Sonstige eingesetzte Risikobewertungsverfahren

Die Freitextangaben in der Kategorie „Sonstige“ liefern nähere Einblicke in fortgeschrittene Bewertungspraktiken. Zwei Unternehmen beschrieben ein adaptives Szenario-Modell, das quartalsweise aktualisiert wird, um veränderte Bedrohungslagen frühzeitig zu berücksichtigen. Dabei kombinierten sie Elemente aus ISO/IEC 27005 mit dem Common Vulnerability Scoring System (CVSS), um sowohl organisatorische als auch technische Einflussfaktoren konsistent abzubilden. Ein weiteres Unternehmen verwies auf eine Einbindung des Risikobewertungs-prozesses in das Change-Management. Jede wesentliche Veränderung an der IT-Infrastruktur

löst dort eine anlassbezogene Neubewertung aus, damit aktuelle Schwachstellen unmittelbar identifiziert und in das bestehende Risikoraster integriert werden können.

Interpretation

Die Ergebnisse verdeutlichen eine breite Verankerung interner Richtlinien und gesetzlicher Vorgaben als primäre Bewertungsrahmen. Gleichzeitig illustrieren die Freitextangaben, dass einige Organisationen bereits flexible, szenario-basierte Methoden einsetzen, um neue Bedrohungen agil zu adressieren. Der vergleichsweise geringe Rückgriff auf externe Beratung legt nahe, dass ein großer Teil der befragten Unternehmen fachliche Kompetenzen zur Risikobewertung institutionell etabliert hat. Insgesamt spiegelt das Vorgehen einen Reifegrad wider, in dem interne und externe Anforderungen miteinander verzahnt werden, um den Vorgaben der NIS-2-Richtlinie gerecht zu werden und gleichzeitig spezifische Organisationsbedarfe präzise abzubilden.

4.4.4 Frage 8: Welche Faktoren berücksichtigen Sie bei der Festlegung der Risikobewertungskriterien?

Diese Frage wurde von 13 Unternehmen (N = 13) beantwortet. Diese enthielt eine Mehrfachauswahl sowie ein Freitextfeld für die Option „Sonstige“. Das Ziel war die Erfassung jener Einflussgrößen, die bei der Festlegung von Risikobewertungskriterien im Bereich der Cybersicherheit herangezogen werden.

Die Verteilung der Antworten zeigt Abbildung 8:

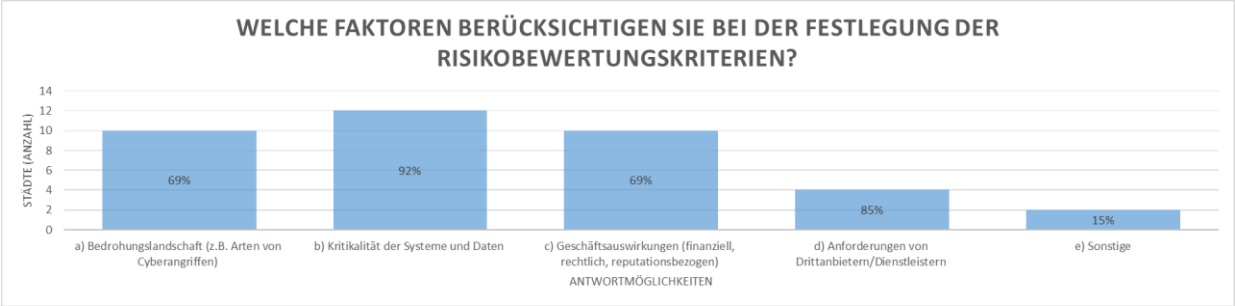

Abbildung 8: Faktoren bei der Festlegung der Risikobewertungskriterien

Die Analyse der Einflussgrößen, die bei der Definition von Risikobewertungskriterien Anwendung finden, weist eine deutliche Schwerpunktsetzung auf unternehmensinterne und operationale Faktoren auf. Mit 92 % der Nennungen (n = 12) bildet die Kritikalität der betroffenen Systeme und Daten die am häufigsten berücksichtigte Größe. Dieser Wert spiegelt den hohen Schutzbedarf in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität informationsverarbeitender Systeme wider.

Mit jeweils 77 % (n = 10) werden die allgemeine Bedrohungslage sowie potenzielle geschäftliche Auswirkungen, beispielsweise rechtliche, finanzielle oder reputative Risiken, als weitere maßgebliche Kriterien angegeben. Diese Angaben verweisen auf ein differenziertes Risikoverständnis, das externe Bedrohungsszenarien und unternehmensinterne Folgen systematisch kombiniert.

Demgegenüber fließen Anforderungen von Drittanbietern oder Dienstleistern nur bei 31 % der Organisationen (n = 4) in die Bewertung ein. Diese vergleichsweise geringe Quote deutet auf einen bislang begrenzten Einfluss externer Stakeholder, etwa in Lieferkettenbeziehungen, hin.

Lediglich 15 % der Unternehmen (n = 2) machten ergänzende Angaben unter „Sonstige“. Die Einträge wurden gemäß Mayring (2015) paraphrasiert, codiert und kategorisiert.

Kategorie	Beschreibung	Häufigkeit
Branchenspezifische Vorgaben	Anwendung von Standards wie B3S oder DWA M-1060 zur risikobasierten Bewertung	2
Regelbasierte Bewertung	Orientierung an gesetzlich regulierten Anforderungen kritischer Infrastrukturen	1 (inhaltlich überlappend)

Tabelle 3: Sonstige Faktoren für die Festlegung der Risikobewertungskriterien

Genannt wurden hier unter anderem branchenspezifische Standards wie der Branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA) oder das DWA-Merkblatt M 1060.

Interpretation

Die qualitative Analyse zeigt, dass einige Organisationen sektorspezifische Normen und Leitlinien, beispielsweise für Kritische Infrastrukturen, in ihre Risikobewertungen integrieren. Diese Vorgehensweise erweitert klassische Bedrohungsanalysen um regulatorische, sicherheitstechnische und infrastrukturelle Anforderungen und ermöglicht dadurch eine engere Verzahnung der Cybersicherheitsprozesse mit branchenspezifischen Rahmenbedingungen.

4.4.5 Frage 9: Welche Methoden zur Risikobeurteilung setzen Sie in Ihrem Unternehmen ein?

Die Frage zur Methodik der Risikobeurteilung beantworteten 13 Unternehmen. Mehrfachnennungen waren möglich.

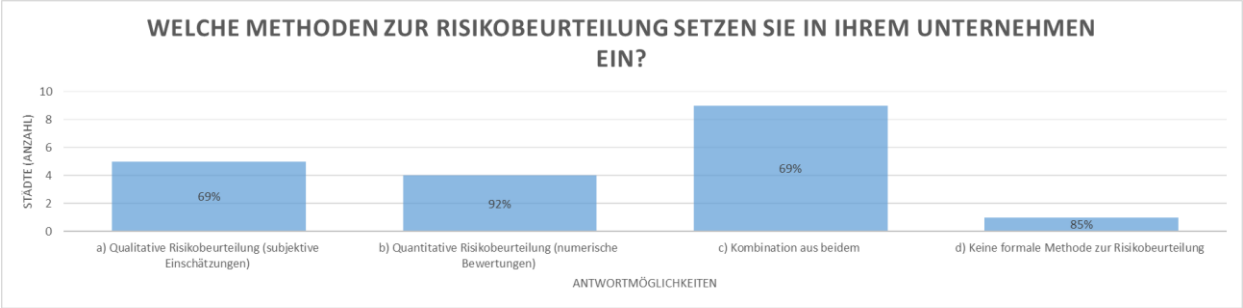

Abbildung 9: Methoden zur Risikobeurteilung

Die Mehrheit der Unternehmen (69 %) nutzt eine Kombination aus qualitativer und quantitativer Risikobeurteilung. Ausschließlich qualitative Verfahren verwenden 38 %, rein quantitative

Ansätze 31 %. Nur eine Organisation gab an, keine formale Methode zur Risikobeurteilung einzusetzen.

Interpretation

Die Ergebnisse verdeutlichen, dass zahlreiche Unternehmen eine hybride Vorgehensweise bevorzugen, um subjektive Einschätzungen und numerische Bewertungen zu verbinden. Die vergleichsweise geringe Verbreitung rein quantitativer Methoden lässt auf begrenzte Datenverfügbarkeit oder hohe Komplexität schließen. Das Fehlen formalisierter Verfahren in einem Unternehmen stellt einen möglichen Risikofaktor für Compliance und Wirksamkeit des Sicherheitsmanagements dar. Die qualitativen Angaben bestätigen, dass quantitative Verfahren häufig mit qualitativen Einschätzungen kombiniert werden, um ein ganzheitliches Risikobild zu erzeugen.

Qualitative Auswertung der Freitextangaben (Sonstiges & Kommentare)

Kategorie	Beschreibung	Häufigkeit
Hybridansatz mit Szenariobezug	Kombination qualitativer und quantitativer Methoden je nach Risikoszenario; häufig abhängig von verfügbaren Daten	3
Einschränkungen bei Quantifizierung	Quantitative Methoden gelten als schwierig, v. a. außerhalb von Finanz-/Versicherungssektoren, wegen fehlender Daten	2
Einschluss nicht-monetärer Risiken	Berücksichtigung von Reputationsverlusten, Aufwänden zur Wiederherstellung, etc.	2

Tabelle 4: Sonstige eingesetzte Methoden zur Risikobeurteilung

4.4.6 Frage 10: Wie wird die Kritikalität der einzelnen Bedrohungen in Ihrem Unternehmen ermittelt?“

Insgesamt beantworteten 13 Unternehmen (N = 13) die Frage zur Ermittlung der Kritikalität einzelner Bedrohungen. Mehrfachantworten waren zulässig. Der Schwerpunkt lag darauf, die Vorgehensweise bei der Bewertung der Kritikalität spezifischer Cyberbedrohungen angewandt wird.

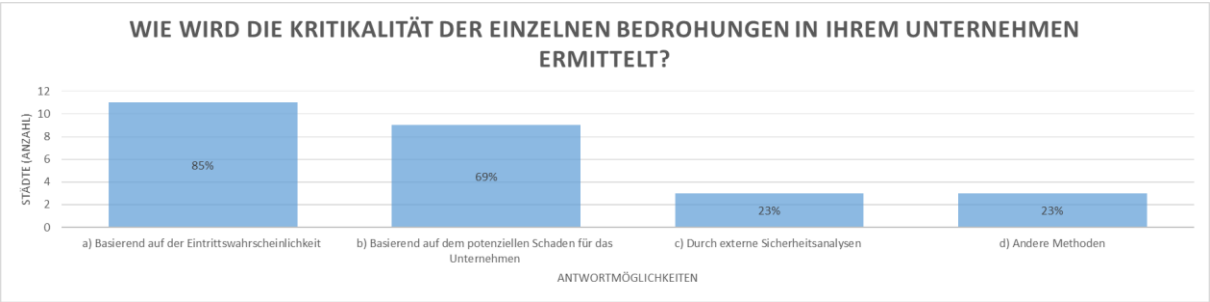

Abbildung 10: Kritikalitätsermittlungsverfahren

Die überwiegende Mehrheit der Unternehmen (85 %, n = 11) bestimmt die Kritikalität anhand der Eintrittswahrscheinlichkeit der jeweiligen Bedrohung. Beinahe ebenso häufig (69 %, n = 9) fließt das potenzielle Schadensausmaß in die Bewertung ein. Externe Sicherheitsanalysen oder alternative Verfahren werden lediglich von 23 % der Organisationen (n = 3) herangezogen.

Interpretation

Die Ergebnisse zeigen eine deutliche Fokussierung auf klassische Risikoparameter wie Eintrittswahrscheinlichkeit und Schadensausmaß. Faktoren wie Detektierbarkeit oder mehrdimensionale Risikolevel-Berechnungen nach dem Schema „Eintrittswahrscheinlichkeit × Auswirkung“ werden seltener eingesetzt, deuten jedoch auf eine zunehmende Differenzierung und Verfeinerung der Risikobewertungen hin. Externe Sicherheitsanalysen fungieren eher als ergänzendes denn als primäres Instrument.

Kategorie	Beschreibung	Häufigkeit
Kombination von Faktoren	Kritikalität = Eintrittswahrscheinlichkeit × Auswirkung bzw. Schadenshöhe	2
Einbezug von Detektierbarkeit	Bewertung ergänzt durch die Detektierbarkeit einer Bedrohung als dritter Faktor neben Eintritt und Schaden	2
Risikolevelbildung mit Expositionsfaktor	Nutzung eines „Risikoexpositionslevels“ durch Kombination von Eintrittswahrscheinlichkeit und Detektierbarkeit	1

Tabelle 5: Weitere Methoden zur Ermittlung der Kritikalität

Die qualitativen Angaben verdeutlichen, dass einzelne Unternehmen ihre Bewertungssysteme verfeinern, indem sie mehrdimensionale Risikomodelle, beispielsweise in Anlehnung an FMEA-Methoden oder an ISO/IEC 27005 basierte Frameworks, implementieren.

4.5 Auswertungen der Fragen aus Themenkategorie 4 „Technische Maßnahmen“

Dieses Kapitel präsentiert die Ergebnisse und Interpretationen zu den technischen Maßnahmen im Rahmen der NIS-2-Umsetzung.

4.5.1 Frage 11: Welche technischen Cybersicherheitsmaßnahmen haben Sie implementiert um den Anforderungen der NIS-2-Richtlinie zu entsprechen?

Von den 13 antwortenden Unternehmen (N = 13) verzichteten zwei Organisationen (15 %) aus sicherheitstechnischen Gründen vollständig auf Angaben. Das nachfolgende Diagramm visualisiert die Verteilung der implementierten technischen Maßnahmen.

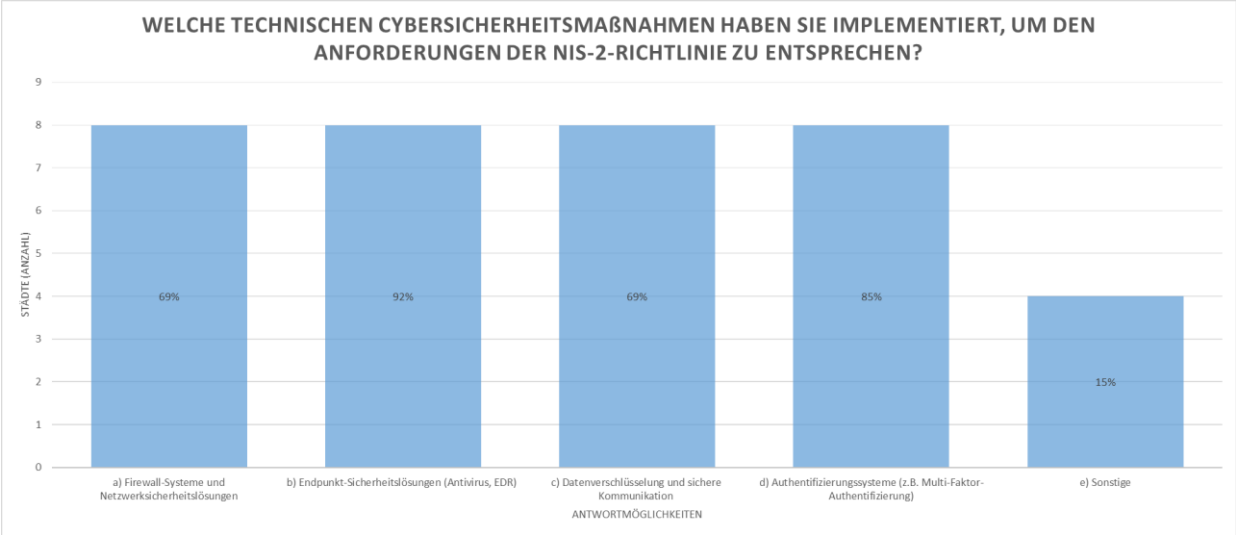

Abbildung 11: Technische Cybersicherheitsmaßnahmen zur Umsetzung der NIS-2-Richtlinie

Die Auswertung zeigt, dass jeweils 62 % der antwortenden Unternehmen (n = 8) diejenigen technischen Cybersicherheitsmaßnahmen einsetzen, die den Anforderungen der NIS-2-Richtlinie entsprechen. Am häufigsten implementiert sind Firewall-Systeme und Netzwerksicherheitslösungen – hierzu zählen Intrusion-Detection-/Prevention-Systeme, VLAN-Strukturen, Network-Access-Control-Mechanismen sowie explizit definierte Firewall-Regeln. Ebenfalls häufig genutzt werden Endpunktschutzlösungen; dazu gehören Antivirus-Software, Extended-Detection-and-Response-Plattformen, automatisierte Isolationsfunktionen bei Vorfällen und eine zentrale Überwachung durch ein Security-Operations- oder Cyber-Defence-Center. Ein weiterer Schwerpunkt liegt auf Datenverschlüsselung und sicherer Kommunikation, beispielsweise über TLS 1.3, HTTPS oder dedizierte Lösungen für externen Datentransfer. Ergänzend kommen Authentifizierungssysteme zum Einsatz, insbesondere Multi-Faktor-Authentifizierung, Identity- and-Access-Management und moderne Authentifizierungsformen wie Passkeys.

Zusätzlich meldeten 31 % der Teilnehmer (n = 4) weitere technische Maßnahmen. Diese reichen von einer strikten Trennung zwischen IT- und OT-Infrastrukturen über OT-spezifische Firewalls und DMZ-Architekturen bis hin zu Security-Information-and-Event-Management-Systemen, USB-Port-Sperren, granularer Segmentierung sowie komplexen Kontrollmechanismen für Zugriffswege.

Die folgenden Freitextangaben verdeutlichen die Bandbreite der sonstigen technischen Maßnahmen. Die qualitative Inhaltsanalyse erfasste jede Maßnahme einmal pro Kategorie, sobald mindestens eine entsprechende Aussage in den Antworten vorkam; die zugehörigen Häufigkeiten sind anhand der Tabelle 6 dargestellt:

Kategorie	Inhaltliche Beschreibung	Technische Maßnahmen aus dem Material	Häufigkeit der Nennungen
1. Netztrennung und Segmentierung	Maßnahmen zur physischen oder logischen Trennung	„Harte Trennung der IT- und OT-Struktur“, „Netzwerksegmentierung“,	4

	von IT- und OT-Strukturen.	„OT-DMZ“, „unterschiedliche Firewalls“	
2. Zugriffskontrolle und Schnittstellenhärtung	Einschränkung und Sicherung von Zugriffspunkten auf Systeme.	„Kein Internetaccess für OT“, „kein freier USB-Bus“, „Jumpserver“, „SW-Datendrehscheibe“	4
3. Externe Sicherheitsinfrastruktur und Konzernlösungen	Nutzung zentral bereitgestellter Sicherheitsservices (z. B. durch Muttergesellschaft).	„SIEM (im Aufbau über Konzernmutter)“, „SzA über Konzernmutter“	2
4. Integration von Mehrschichtsystemen (Defense in Depth)	Nutzung mehrerer, sich ergänzender Schutzmechanismen.	„Fortinet und Sophos“, „CrowdStrike, Sophos, Panda“, „EDR/EPS auf IT und OT“	3
5. Umsetzung vor NIS-2/ strategische Frühadaption	Maßnahmen waren bereits vor der NIS-2-Richtlinie etabliert.	„alle a–d waren bereits vor NIS2 implementiert“	2
6. Schutz von Drittzugängen und Produktionsumgebungen	Spezielle Sicherheitsstandards für Dienstleister oder Lieferanten in kritischen Bereichen.	„Dienstleister/Lieferantenzugang“, „Zugriffsstandard für Produktionsdomäne“	2

Tabelle 6: Sonstige technische Maßnahmen zur Umsetzung der NIS-2-Richtlinie

Die Häufigkeiten beziehen sich auf die Anzahl der Nennungen in den qualitativen Antworten (nicht auf die Zahl der Unternehmen). Pro Antwort wurde jede Kategorie höchstens einmal gezählt.

Interpretation

Die qualitativen Angaben zu den implementierten Cybersicherheitsmaßnahmen verdeutlichen ein hohes Maß an technischer Tiefe sowie organisatorischer Differenzierung der Antwortgeberinnen und Antwortgeber. Auffällig ist insbesondere der Schwerpunkt auf einer strikten Segmentierung und Netztrennung – vor allem in betriebskritischen OT-Umgebungen –, auf stark ausgeprägten Zugriffskontrollen und Maßnahmen zur Reduzierung physischer wie digitaler Schnittstellenrisiken (etwa USB-Kontrollen oder dedizierte Kommunikationspfade). Darüber hinaus setzen viele Organisationen mehrstufige Sicherheitsinfrastrukturen um, was auf ein konsequent angewandtes Defense-in-Depth-Prinzip hinweist. Übergreifende Sicherheitsarchitekturen werden konzernweit gesteuert und implementiert.

Einzelne Maßnahmen wurden bereits vor Inkrafttreten der NIS-2-Richtlinie realisiert. Dies deutet auf proaktives und strategisch vorausschauendes Handeln hin. Insgesamt spiegeln die offenen Antworten ein hohes Reifegradniveau, eine ausgeprägte Individualisierung der Schutzkonzepte und deutliche Branchenspezifika wider. Dies sind Merkmale, die häufig bei Einrichtungen mit KRITIS-Bezug anzutreffen sind.

4.6 Auswertungen der Fragen aus Themenkategorie 5 „Physische Maßnahmen“

Dieses Kapitel enthält die Auswertungen der Fragen zu physischen Schutzmaßnahmen bei der Umsetzung der NIS-2-Richtlinie.

4.6.1 Frage 12: Welche physischen Maßnahmen setzen Sie ein, um den Schutz Ihrer IT- und Netzwerksysteme zu gewährleisten?

Die Frage wurde von 13 Organisationen beantwortet (Mehrfachnennungen waren möglich). Drei Einrichtungen machten keine Angaben. Nachfolgend erfolgt die deskriptiv-statistische Auswertung der Antworten.

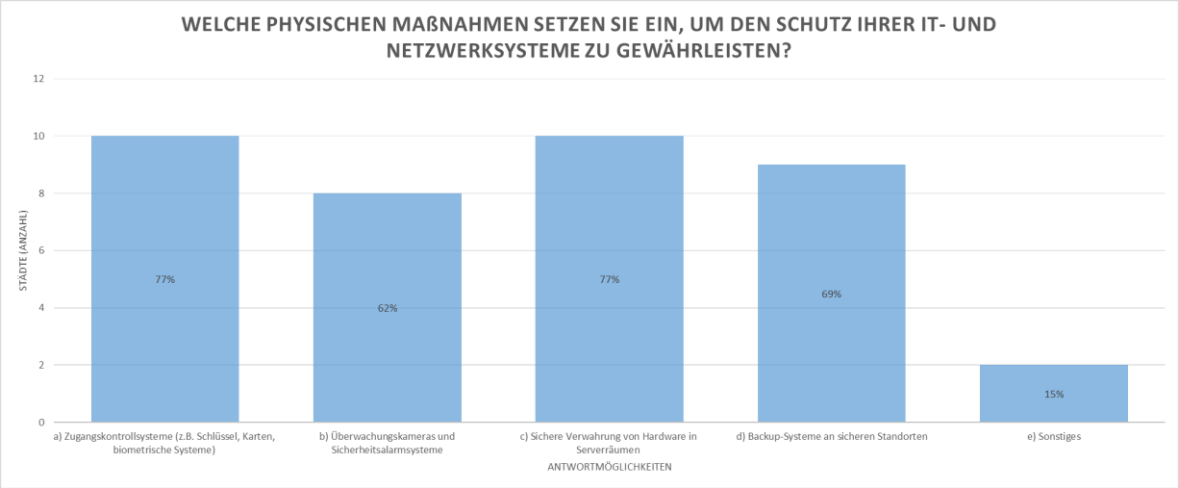

Abbildung 12: Physische Maßnahmen zum Schutz der IT und der Netzwerksysteme

Zugangskontrollsysteme kommen in 77 % der Fälle (n = 10) zum Einsatz und zählen damit zu den am häufigsten realisierten Schutzmaßnahmen. Das Spektrum reicht von klassischen Schlüssellösungen bis zu RFID- oder Transponderverfahren; der Einsatz biometrischer Systeme wurde explizit ausgeschlossen. Ebenfalls 77 % der Unternehmen (n = 10) bewahren Hardware in abgesicherten Serverräumen mit Klimatisierung und Überwachung oder in stahlverstärkten Verwahrungseinrichtungen auf. Backup-Systeme an physisch getrennten Standorten setzen 69 % der Befragten (n = 9) ein. Hierzu zählen Bandsicherungen in anderen Gebäuden sowie Cloud-basierte Redundanzkonzepte, wodurch die Wiederherstellbarkeit kritischer Daten gewährleistet wird. Überwachungskameras und Alarmsysteme finden sich bei 62 % der Organisationen (n = 8), vorzugsweise an Außenstellen und in Serverbereichen; mehrere Unternehmen planen eine Erweiterung hin zu umfassenden Videoüberwachungslösungen. Die Kategorie „Sonstige Maßnahmen“ wurde von 15 % (n = 2) genannt und verweist auf eine strikt zonenbasierte Sicherheitsarchitektur, in der sämtliche Anlagenstufen nach definierten Schutzzielen klassifiziert sind. Dies ist ein Hinweis auf ein fortgeschrittenes, ganzheitlich ausgerichtetes Sicherheitsmanagement.

Interpretation

Die Ergebnisse belegen ein insgesamt hohes Schutzniveau der befragten Organisationen im physischen Bereich. Der häufige Einsatz von Zugangskontrollsystemen und gesicherten Hardwareumgebungen verdeutlicht ein ausgeprägtes Bewusstsein für den Schutz sensibler Infrastruktur. Die beträchtliche Verbreitung physisch getrennter Backup-Systeme zeigt, dass die Gewährleistung von Datenverfügbarkeit und Wiederherstellbarkeit prioritär behandelt wird. Überwachungskameras und Alarmsysteme sind bereits bei einer Mehrheit implementiert, weisen jedoch noch Potenzial für eine flächendeckende Ausdehnung auf. Die vereinzelte Anwendung zonenbasierter Schutzkonzepte dokumentiert einen fortgeschrittenen Reifegrad einzelner Unternehmen, die eine systematische, risikobasierte Segmentierung verfolgen. Insgesamt lassen die Befunde auf eine professionelle und weitgehend umfassende Umsetzung physischer Cybersicherheitsmaßnahmen schließen.

4.6.2 Frage 13: Wie häufig werden physische Sicherheitsmaßnahmen überprüft?

Die Frage nach der Häufigkeit der Überprüfungen beantworteten 13 Organisationen. Drei von ihnen machten keine Angaben.

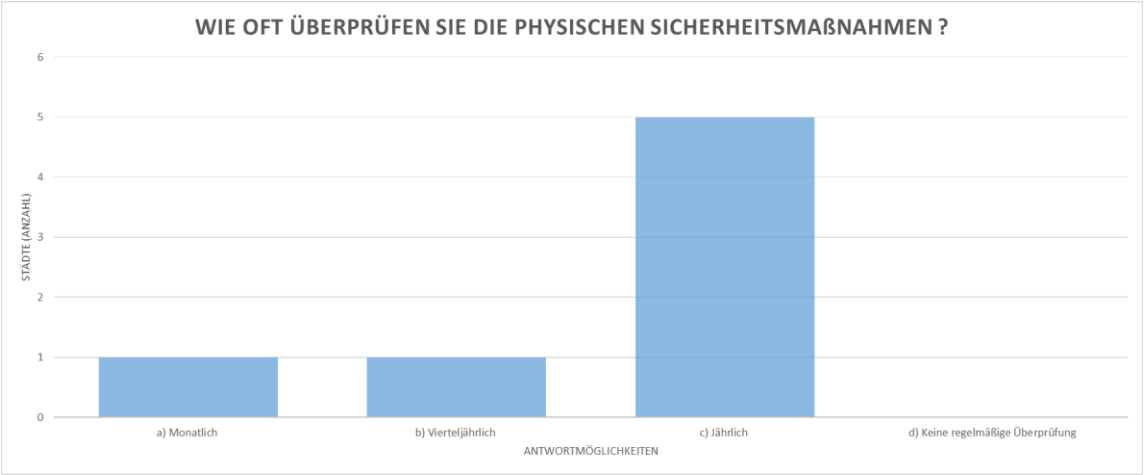

Abbildung 13: Häufigkeiten der Überprüfungen der physischen Sicherheitsmaßnahmen

Die Auswertung zeigt folgende Verteilung: 8 % (n = 1) führen monatliche Überprüfungen durch; ebenfalls acht Prozent (n = 1) kontrollieren vierteljährlich. Die Mehrheit, 38 % (n = 5), überprüft die Maßnahmen jährlich, ergänzt durch anlassbezogene Kontrollen oder externe Audits, beispielsweise durch Datenschutz- oder Informationssicherheitsbeauftragte. Keines der befragten Unternehmen verzichtet gänzlich auf turnusmäßige Prüfungen. Zusätzlich gaben 23 % (n = 3) an, eine permanente Überwachung im laufenden Betrieb vorzunehmen, etwa mittels kontinuierlicher Kameravisualisierung oder täglicher Kontrollgänge.

Interpretation

Die Ergebnisse verdeutlichen, dass die meisten Organisationen klar strukturierte Prüfprozesse etabliert haben; ein Teil setzt darüber hinaus auf eine fortlaufende Überwachung des physischen Sicherheitsniveaus im Tagesbetrieb.

4.7 Auswertungen der Fragen aus Themenkategorie 6 „NIS-2 und Cybersicherheitsstandards“

Dieses Kapitel enthält die Analyse der Fragen zum Einsatz ergänzender Standards bei der Umsetzung der NIS-2-Richtlinie.

4.7.1 Frage 14: Welche zusätzlichen Informations- und Cybersicherheits-standards oder -normen setzen Sie neben der NIS-2-Richtlinie um?

Es wurden 13 gültige Antworten erfasst; Mehrfachnennungen waren zulässig, sodass die Summen der Prozentwerte 100 % übersteigen können. Die folgenden Angaben beruhen auf einer qualitativen Inhaltsanalyse; jede Kategorie wurde pro Antwort maximal einmal gezählt, sofern mindestens eine entsprechende Aussage vorlag:

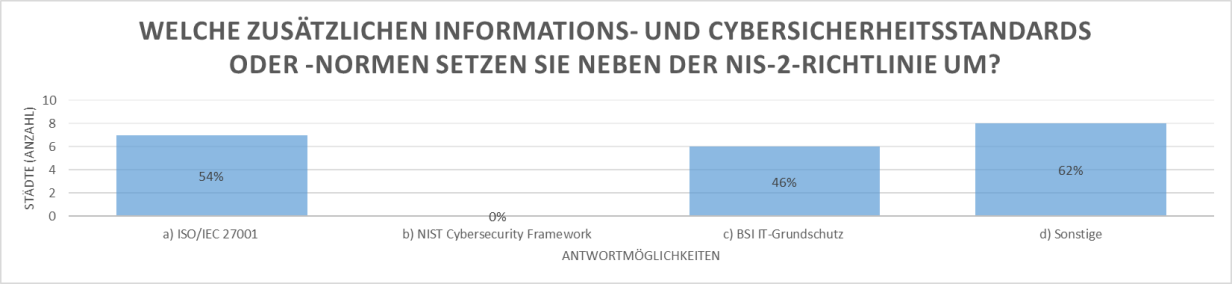

Abbildung 14: Zusätzlich angewandte Cybersicherheitsstandards und Normen

Die Auswertung belegt, dass eine Mehrheit der befragten Unternehmen neben den Anforderungen der NIS-2-Richtlinie weitere etablierte Informations- und Cybersicherheitsstandards implementiert. Am häufigsten nannten 54 % der Antwortgebenden (n = 7) die ISO/IEC 27001, womit diese international anerkannte Norm für Informationssicherheits-Managementsysteme den zentralen Bezugsrahmen bildet. Fast ebenso verbreitet ist der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik, der von 46 % der Organisationen (n = 6) zur ergänzenden Orientierung herangezogen wird.

Die Antwortoption „Sonstige“ wählten 62 % der Teilnehmer (n = 8). In den Freitextfeldern verwiesen sie auf branchenspezifische oder organisationsinterne Regelwerke, darunter ISO/IEC 27019 für den Energiesektor, ISO/IEC 27005 zur Risikoanalyse sowie weitere firmenspezifische Vorgaben.

Standard/Regelwerk	Anmerkung / Kontext	Häufigkeit (von 8)
ISO/IEC 27019	Branchenspezifische Anpassung für Energie/Wasser	4
ISO/IEC 27001	Allgemeiner Standard für ISMS	2
ISO/IEC 27002	Leitlinien zur Umsetzung von Controls	1
ISO/IEC 27005	Risikomanagement	1

ISO/IEC 62443 (tw)	OT-Sicherheit	1
DIN EN 50600	Rechenzentrumsicherheit	1
BSIG § 8a Abs.1 / 1a (BSI)	Rechtliche Vorgabe, inkl. Systeme zur ADA	2
BSI Grundschutz / IT-Grundschutzbausteine	Basisabsicherung, risikoorientiert	2
VdS 10000	Mittelstandsfokus, praxisorientiert	1
B3S Wasser (WA), inkl. DWA-M 1060	Branchenspezifisch für Wasserversorgung	3
WiBA (Grundlagenabsicherung)	Analogie zu Basisabsicherung	1
IT-SiKat (IT-Sicherheitskatalog)	Energiebereichsanforderung (analoger Bezug)	1

Tabelle 7: Sonstige eingesetzte Cybersicherheitsstandards und Normen

Das NIST Cybersecurity Framework wird von keiner der befragten Organisationen eingesetzt (0 %), was auf eine vergleichsweise geringe Relevanz im deutschen bzw. europäischen Kontext schließen lässt. Die Ergebnisse verdeutlichen, dass zahlreiche Organisationen über die Anforderungen der NIS-2-Richtlinie hinaus aktiv sind und ihr Sicherheitsniveau durch international anerkannte Standards absichern; dabei stehen insbesondere ISO/ IEC 27001, der BSI-IT-Grundschutz sowie spezifische Zusatzregelwerke im Mittelpunkt.

Interpretation

Die Auswertung zeigt, dass sich Organisationen häufig gleichzeitig an mehreren Standards orientieren, um unterschiedliche regulatorische, technische und branchenspezifische Anforderungen zu erfüllen.

4.7.2 Frage 15: Für welche Anforderungen der NIS-2-Richtlinie setzen die Informations- und Cybersicherheitsstandards bzw. Teile/Kapitel dieser Standards ein?

Zu dieser geschlossenen Frage wurden 13 Antworten erfasst. Mehrfachnennungen waren möglich, sodass sich die Summe der Prozentwerte auf mehr als 100 % beläuft. Die Häufigkeiten und Anteile lauten wie folgt:

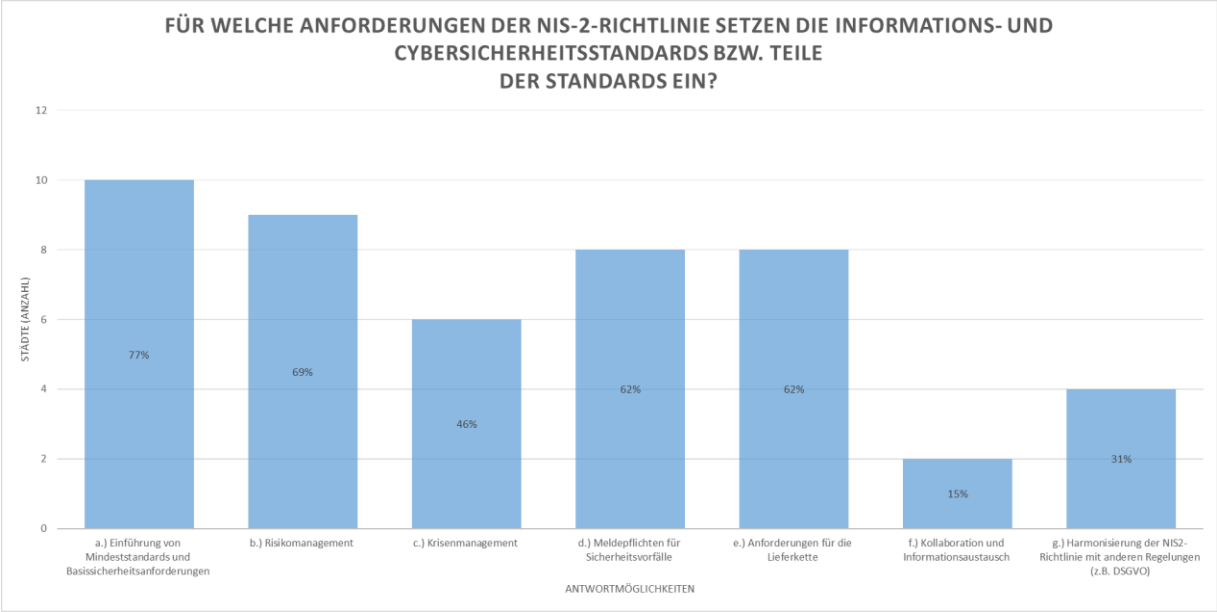

Abbildung 15: NIS-2-Anforderungen für welche Standards eingesetzt werden

Besonders häufig kommen diese Standards bei der Einführung von Mindeststandards und Basissicherheitsanforderungen zum Einsatz (77 %, n = 10). Dies verdeutlicht, dass die Orientierung an etablierten Normen wie ISO/IEC 27001 oder dem BSI-IT-Grundschutz als wesentliche Grundlage dient, um grundlegende Sicherheitsniveaus im Unternehmen zu verankern. Ferner zeigt sich eine intensive Nutzung im Risikomanagement (69 %, n = 9), das als strukturierender Kernbestandteil zahlreicher Sicherheitsstandards gilt.

Meldepflichten für Sicherheitsvorfälle sowie Anforderungen an die Lieferkette werden jeweils von 62 % der Teilnehmer (n = 8) berücksichtigt – beides Bereiche, die durch die NIS-2-Richtlinie besonders hervorgehoben werden und in Standards wie ISO/IEC 27001 bzw. ISO/IEC 27036 konkret operationalisiert sind. Das Krisenmanagement adressieren 46 % der Befragten (n = 6) mithilfe einschlägiger Sicherheitsstandards, was die Relevanz strukturierter Reaktions- und Wiederherstellungspläne unterstreicht.

Die Harmonisierung mit weiteren Regelwerken, etwa der DSGVO, wurde von 31 % der Organisationen (n = 4) genannt und verdeutlicht das wachsende Bewusstsein für interdisziplinäre Compliance-Anforderungen. Vergleichsweise selten genannt wurden Aspekte wie Zusammenarbeit und Informationsaustausch (15 %, n = 2), was auf einen potenziellen Entwicklungsbedarf hinsichtlich sektor- und organisationsübergreifender Kooperationsstrukturen hinweist.

Interpretation

Die Daten illustrieren, in welchen Bereichen Informationssicherheitsstandards bevorzugt zur Erfüllung der NIS-2-Anforderungen herangezogen werden. Insbesondere in den Feldern Risikomanagement und Basisschutz stützen sich Unternehmen intensiv auf etablierte Normen. Gleichzeitig offenbart die geringere Nennungsrate bei Kooperation und Austausch einen möglichen Ausbaubedarf. Insgesamt erfolgt die Umsetzung der NIS-2-Richtlinie in der Praxis

durch den gezielten Einsatz anerkannter Informations- und Cybersicherheitsstandards über mehrere Anforderungsbereiche hinweg.

4.8 Auswertung der Fragen aus Themenkategorie 7 „Anregungen für zukünftige Leitfäden/Standards zur NIS-2-Richtlinie“

In diesem Kapitel werden die Anregungen der Befragten für künftige Leitfäden oder Standards zur Umsetzung der NIS-2-Richtlinie dargestellt und interpretiert.

4.8.1 Frage 16: Welche technischen Herausforderungen haben Sie bei der Implementierung der NIS-2-Richtlinie identifiziert?

Acht der antwortenden Unternehmen (62 %) machten zu dieser Frage keine Angaben. Die verbleibenden fünf Organisationen (38 %) beantworteten diese ausführlich. Zur Auswertung kam erneut eine qualitative Inhaltsanalyse nach Mayring (2015) zum Einsatz. Die Aussagen wurden paraphrasiert, thematisch gebündelt und in Kategorien überführt. Anschließend erfolgte eine Häufigkeitsauszählung, um zentrale technische Herausforderungen sichtbar zu machen.

Kategorie	Beschreibung	Häufigkeit
Systemintegration & Interoperabilität	Probleme bei der Kombination unterschiedlicher Sicherheitslösungen und IT-/OT-Bereiche	2
Herstellerabhängigkeiten/fehlende Updates	Einschränkungen durch fehlende Sicherheitsfreigaben oder veraltete Release-Zyklen	1
Identifikation kritischer Systeme	Schwierigkeiten bei der Festlegung, welche Anlagen besonders zu schützen sind	1
Keine nennenswerten Herausforderungen	Unternehmen gibt an, derzeit keine besonderen technischen Schwierigkeiten zu sehen	1
Keine Angaben	Keine Angaben	8

Tabelle 8: Technische Herausforderungen während der NIS-2-Umsetzung

Dadurch wurde deutlich, dass sich die Organisationen in sehr unterschiedlichen Stadien der Auseinandersetzung mit der NIS-2-Richtlinie befinden. Die am häufigsten genannten Unterstützungswünsche lassen sich drei Hauptthemenbereichen zuordnen. Erstens besteht Bedarf an fachlicher Unterstützung und Expertise: Die Komplexität der NIS-2-Richtlinie wird als Herausforderung beschrieben, deren Bewältigung ohne externe Fachkenntnis schwer möglich erscheint, weshalb wiederholt professionelle Beratung eingefordert wird. Zweitens zeigt sich ein erheblicher Bedarf an interner Befähigung und geeigneten technischen Hilfsmitteln: Die Nennung von Schulungen und Werkzeugen deutet auf einen strukturellen Qualifizierungsbedarf hin, zu dessen Deckung staatliche Stellen oder Konzernzentralen unterstützende Formate,

beispielsweise Workshops oder Checklisten, bereitstellen sollen. Drittens werden Ressourcenengpässe genannt: Der Wunsch nach zusätzlicher Zeit und Personal belegt, dass die Richtlinienanforderungen in vielen Unternehmen bislang nicht vollständig in die vorhandenen Kapazitäten integrierbar sind.

Interpretation

Die Ergebnisse verweisen darauf, dass die technische Umsetzung der NIS-2-Richtlinie vor allem durch Systembrüche zwischen Produktions- und Office-Domänen erschwert wird. Besonders problematisch erweist sich die Interoperabilität: Inkompatible Systeme, Plattformen oder Herstellerlösungen führen zu Schnittstellenproblemen und Sicherheitslücken. Ein weiteres Hindernis liegt in einer unzureichenden Flexibilität auf Seiten der Hersteller, etwa bei veralteten Update-Zyklen und der verzögerten Freigabe aktueller Patches – eine Praxis, die mit den Anforderungen moderner IT-Sicherheitskonzepte wie Zero Trust nicht vereinbar ist. Zudem wurde vereinzelt die Schwierigkeit der Systemidentifikation hervorgehoben, das heißt die Frage, welche Anlagen oder Systeme unter die besonderen Schutzmaßnahmen der NIS-2 fallen sollen. Auffällig ist, dass ein Unternehmen keine wesentlichen Herausforderungen meldete, was auf einen bereits fortgeschrittenen Umsetzungsstand hindeutet.

4.8.2 Frage 17: Welche weiteren Unterstützungsmöglichkeiten oder Ressourcen benötigen Sie, um die Anforderungen der NIS-2-Richtlinie vollständig zu erfüllen?

Diese offene Frage blieb bei sechs Antwortenden (46 %) unbeantwortet. Ein Unternehmen gab an, sich bisher nicht vertieft mit der NIS-2-Richtlinie und den daraus resultierenden Best Practices befasst zu haben. Die Rückmeldungen der verbleibenden sieben Organisationen (54 %) wurden mittels qualitativer Inhaltsanalyse nach Mayring (2015) paraphrasiert, thematisch gebündelt und in Kategorien überführt:

Kategorie	Beschreibung	Häufigkeit
Externe Beratung/ Expertise	Bedarf an fachlicher Begleitung, z. B. durch Cybersecurity-Consultants	3
Schulungen & Zertifizierungen	Weiterbildungsbedarf, internes Kompetenzniveau erhöhen	2
Technische Unterstützung/Tools	Konkrete Werkzeuge, Plattformen, Checklisten	2
Personelle/zeitliche Ressourcen	Wunsch nach mehr Zeit bzw. zusätzlichem Personal	2
Klarheit durch rechtliche Umsetzung	Wunsch nach nationaler Gesetzgebung als Umsetzungshilfe	1

Konzerninterne Hilfestellung	Nutzung von zentralen Vorgaben, Checklisten, z. B. durch Konzernmutter	1
Keine Auseinandersetzung mit NIS-2 bisher	Hinweis auf fehlende Vorbereitung	1

Tabelle 9: Benötigte Unterstützungsmöglichkeiten bzw. Ressourcen zur Umsetzung der NIS-2-Anforderungen

Die Auswertung zeigt fünf zentrale Cluster von Unterstützungsbedarfen. Erstens wurde ein hoher Bedarf an externer Expertise beschrieben. Spezialisierte Beratungsunternehmen sollen die Komplexität der Richtlinie adressieren. Zweitens verweisen zahlreiche Rückmeldungen auf Qualifizierungs- und Wissenstransferformate, etwa Schulungen oder Zertifizierungsangebote, um interne Kompetenzen aufzubauen. Drittens wünschen mehrere Unternehmen eine präzisere Übersetzung der NIS-2-Vorgaben in bindendes nationales Recht, um Rechtsklarheit zu erhalten. Viertens wurden wiederholt Ressourcenengpässe genannt, speziell der Mangel an Zeit und Personal während des laufenden Betriebs. Fünftens profitieren einzelne Unternehmen bereits von konzernweiten Strukturen, beispielsweise von vorliegenden Vorlagen oder Werkzeugen für KRITIS-Zertifizierungen, und sehen hierin einen bedeutenden Erfolgsfaktor.

Interpretation

Die Analyse verdeutlicht, dass sich die betrachteten Organisationen in unterschiedlichen Stadien der Auseinandersetzung mit der NIS-2-Richtlinie befinden. Die drei dominierenden Bedarfsfelder lassen sich wie folgt zusammenfassen: Erstens erweist sich fachliche Unterstützung durch externe Expertinnen und Experten als entscheidender Erfolgsfaktor, um die Richtlinienkomplexität zu bewältigen. Zweitens legt der ausgeprägte Wunsch nach Schulungsprogrammen und anwendungsorientierten Werkzeugen einen strukturellen Qualifizierungsbedarf offen; hierbei richten sich Erwartungen insbesondere an staatliche Stellen und Konzernzentralen. Drittens machen zahlreiche Antworten deutlich, dass fehlende zeitliche und personelle Ressourcen die Umsetzung der Richtlinie hemmen.

Auffällig bleibt, dass mindestens eine Organisation bislang keine vertiefte Beschäftigung mit der NIS-2-Richtlinie begonnen hat. Dieser Befund weist auf Informationsdefizite oder einen bislang geringen internen Handlungsdruck hin und unterstreicht die Relevanz einer verstärkten kommunikativ-strategischen Begleitung durch Politik und Branchenverbände.

4.8.3 Frage 18: Was sind aus Ihrer Sicht die wichtigsten Good Practices bei der Umsetzung der NIS-2-Richtlinie?

Diese offene Frage wurde von fünf der 13 antwortenden Unternehmen (38 %) nicht beantwortet. Ein weiteres Unternehmen erklärte, sich bislang noch nicht intensiv genug mit der NIS-2-Richtlinie befasst zu haben. Die Antworten der acht verbleibenden Organisationen (62 %) wurden gemäß

der zuvor beschriebenen Analysemethode paraphrasiert, inhaltlich codiert und anschließend ausgezählt:

Kategorie	Beschreibung	Häufigkeit
Etablierung von Governance & Managementstrukturen	z. B. Governance, Risikomanagement, Notfallpläne, organisatorische Klarheit	2
Schulung und Sensibilisierung	Maßnahmen zur Awareness und Fortbildung der Belegschaft	1
Technische Sicherheitsstandards & Frameworks	Referenz auf Normen, z. B. ISO/IEC 27001, 27002, BSI Grundschutz, Zero Trust, 27017	6
Externe Unterstützung & Know-how	Empfehlung zur Einbindung externer Dienstleister, Partner oder Erfahrungsaustausch	3
Iterative, pragmatische Umsetzung	Kritik an „erschlagenden“ Standards – stattdessen: schrittweises Vorgehen mithilfe von BSI-WiBa	1
Unterstützung durch Unternehmensführung	Umsetzung erfordert aktiven Rückhalt durch das Top-Management	1
Noch keine intensive Auseinandersetzung	Rückmeldung, dass noch kein tieferer Umgang mit Best Practices erfolgt ist	1

Tabelle 10: Good Practices zur NIS-2-Umsetzung

Die Auswertung ergab fünf thematische Cluster. Erstens betonen zahlreiche Beiträge die Bedeutung von Governance-Strukturen sowie des ausdrücklichen Umsetzungswillens auf Leitungsebene. Die Einbindung spezialisierter externer Partner und Dienstleister wird häufig als sinnvoll erachtet, um die geforderte Expertise abzudecken. Zweitens rückt ein ganzheitliches Risikomanagement in den Vordergrund; hierzu zählen insbesondere Notfall- und Wiederherstellungspläne sowie der geplante Übergang von klassischen „Defense in Depth“-Konzepten hin zu Zero-Trust-Architekturen. Drittens verweisen viele Aussagen auf etablierte normative Rahmen wie ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 oder den BSI-IT-Grundschutz. Gleichzeitig wird kritisch angemerkt, dass ein unmittelbarer Einstieg über umfassende Standardwerke als überfordernd empfunden werde. Stattdessen empfehlen die Befragten einen schrittweisen, praxisorientierten Einstieg, beispielsweise gestützt auf konkrete BSI-Empfehlungen. Viertens wird die kontinuierliche Schulung und Sensibilisierung der Mitarbeiter als entscheidender Erfolgsfaktor hervorgehoben, um sowohl die Anforderungen zu erfüllen als auch deren Akzeptanz zu erhöhen. Fünftens hebt ein Teil der Rückmeldungen den interorganisationalen Austausch mit anderen Unternehmen, zuständigen Behörden und externen Dienstleistern hervor; dieser Austausch soll durch gemeinsame Informationsplattformen erleichtert werden.

Insgesamt zeigt die qualitative Analyse, dass insbesondere die anfängliche Orientierung an umfangreichen Normenwerke als herausfordernd wahrgenommen wird. Mehrere Organisationen äußern den Wunsch nach pragmatischen und sektorspezifischen Lösungen anstelle breit gefasster generischer Vorgaben. Ferner deutet das Fehlen vertiefter Auseinandersetzungen in einzelnen Betrieben auf einen weiterhin hohen Informations- und Unterstützungsbedarf hin, der sowohl politisch als auch wirtschaftlich adressiert werden sollte.

Interpretation

Der inhaltliche Schwerpunkt liegt erkennbar auf der Orientierung an etablierten technischen Sicherheitsstandards, primär an den Normen der ISO/IEC-27000-Reihe sowie am BSI-IT-Grundschutz. Genannt wurden zudem spezialisierte Normen wie ISO/IEC 27005 (Risikomanagement), 27033 (Netzwerksicherheit) und 27017 (Cloud-Sicherheit) sowie branchenspezifische Vorgaben, etwa ISO/IEC 27019 für den Energiesektor.

An zweiter Stelle steht die Zusammenarbeit mit externen Akteuren zur Gewinnung von Fachwissen und zur Begleitung konkreter Maßnahmen, was die Bedeutung von Erfahrungsaustausch und Partnernetzwerken bei der Umsetzung der NIS-2-Richtlinie unterstreicht.

Mehrere Rückmeldungen betonen die Notwendigkeit eines pragmatischen Vorgehens: Statt unmittelbar mit der vollständigen Umsetzung aller Anforderungen der ISO/IEC 27001 zu beginnen, wird empfohlen, zunächst verständliche Einzelmaßnahmen, beispielsweise anhand spezifischer BSI-WiBa-Empfehlungen, einzuführen.

Die Unterstützung durch die Geschäftsführung gilt als kritischer Erfolgsfaktor; eine fehlende strategische Rückendeckung kann Best-Practice-Vorgehensweisen erheblich einschränken.

Ein Teil der Befragten gab an, sich bislang noch nicht vertieft mit der NIS-2-Richtlinie befasst zu haben, was auf bestehenden Orientierungsbedarf hindeutet.

Diese Ergebnisse liefern ein umfassendes Bild des aktuellen Umsetzungsstands der NIS-2-Richtlinie in den befragten Unternehmen. Auf Grundlage dieser Erkenntnisse werden im folgenden Kapitel die Ergebnisse systematisch zusammengeführt und eingeordnet.

5 ERGEBNISSE

In diesem Kapitel werden die Ergebnisse der Befragung nach Themenkategorien strukturiert zusammengefasst. Die wesentlichen Antworten der Teilnehmer werden dargestellt, um in den folgenden Kapiteln belastbare Schlussfolgerungen ableiten zu können.

5.1 Ergebnisse aus Themenkategorie 1: Governance

Die Analyse der Governance-Strukturen zeigt, dass in 85 % der antwortgebenden Unternehmen (n = 11) die Verantwortung für Cybersicherheit in die bestehende IT-Abteilung integriert ist. Dieses Modell versteht Cybersicherheit als Teil der klassischen IT-Aufgaben und setzt auf enge Verzahnung. Gleichzeitig verfügen 38 % der Unternehmen (n = 5) über eigenständige Cybersicherheitsabteilungen – ein Hinweis auf das zunehmende Bewusstsein für die Spezifik und strategische Bedeutung des Themas.

Die Verantwortung für Cybersicherheit und die Umsetzung der NIS-2-Richtlinie liegt in 77 % der Fälle (n = 10) auf Ebene der Geschäftsführung; 54 % (n = 7) nennen spezialisierte Fachfunktionen, 46 % (n = 6) beziehen externe Partner ein. Damit wird Cybersicherheit als organisationsweites Querschnittsthema verstanden, das sowohl strategisch als auch operativ verankert sein muss.

Bei den umgesetzten Governance-Maßnahmen dominieren Meldesysteme und Notfallpläne (85 %, n = 11), Monitoring der Cybersicherheit und Frühwarnsysteme sowie Sensibilisierungsprogramme, die jeweils von 85 % der Unternehmen eingesetzt werden. Strukturierte Instrumente wie Risikomanagementsysteme (77 %, n = 10) und regelmäßige Audits verdeutlichen eine hohe organisatorische Reife, während der Schutz von Lieferketten als weiterhin herausfordernd benannt wird.

5.2 Ergebnisse aus Themenkategorie 2: Organisatorische Maßnahmen

Im Bereich der organisatorischen Maßnahmen zeigt sich eine breite, systematische Umsetzung wesentlicher Sicherheitspraktiken. Regelmäßige Schulungen zur Cybersicherheit führen 92 % der Unternehmen (n = 12) durch; damit wird der Stellenwert von Sensibilisierung und Qualifikation der Mitarbeiter betont.

In 85 % der Unternehmen (n = 11) sind klare Verantwortlichkeiten und Eskalationswege definiert – ein Indikator für ausgeprägte Rollen- und Prozessklarheit. Ergänzend nennen 69 % (n = 9) strukturierte Kommunikationsprozesse für Krisenfälle sowie die Einführung eines Cybersicherheitsmanagementsystems; beide Maßnahmen stärken die Handlungsfähigkeit bei Sicherheitsvorfällen.

Diese Ergebnisse belegen, dass organisatorische Aspekte inzwischen als unverzichtbarer Bestandteil der Cybersicherheitsstrategie gelten und technische Lösungen nicht mehr allein im Vordergrund stehen.

5.3 Ergebnisse aus Themenkategorie 3: Risikomanagement

Im Bereich Risikomanagement ergibt sich ein differenziertes Bild. Ein vollständiges Risikomanagementsystem für Informations- und Cybersicherheit ist bei 54 % der Unternehmen (n = 7) implementiert; 46 % (n = 6) verfügen zumindest über eine partielle Umsetzung. Klassische Risikoabschätzungen für IT-Systeme und Geschäftsprozesse werden von 92 % der Organisationen (n = 12) durchgeführt und bilden damit die Grundlage für eine systematische Risikobewertung. Ergänzend setzen 69 % Bedrohungs- und Schwachstellenanalysen ein, während 62 % Stresstests zur Simulation von Cyberangriffen nutzen.

Bei der Festlegung von Bewertungskriterien dominieren interne Richtlinien (69 %, n = 9) sowie gesetzliche Vorgaben (62 %, n = 8). Als wesentliche Einflussgrößen gelten die Kritikalität der Systeme und Daten (92 %, n = 12) und die aktuelle Bedrohungslage (77 %, n = 10). Eine hybride Anwendung qualitativer und quantitativer Verfahren findet sich bei 69 % der Unternehmen; jedoch wird die begrenzte Verfügbarkeit belastbarer Zahlenwerte als Restriktion genannt. Insgesamt lässt sich feststellen, dass das Risikomanagement in den meisten Fällen strukturiert angelegt ist, gleichwohl weiterhin Entwicklungspotenzial aufweist.

5.4 Ergebnisse aus Themenkategorie 4: Technische Maßnahmen

Die technische Absicherung erreicht ein hohes Umsetzungsniveau. Klassische Schutzmechanismen wie Firewalls, Intrusion-Detection-/Prevention-Systeme, Netzsegmentierung, Endpunktschutzlösungen und Multi-Faktor-Authentifizierung werden von 62 % der Unternehmen (n = 8) konsequent eingesetzt. Darüber hinaus kommen spezialisierte Maßnahmen zum Tragen, darunter die strikte Trennung von IT- und OT-Strukturen, der Einsatz von Security-Information- and-Event-Management-Systemen sowie der gesicherte Zugriff für Drittanbieter. Mehrere Organisationen verfolgen eine Defense-in-Depth-Strategie und implementieren somit mehrschichtige Sicherheitsmechanismen. In einigen Fällen wurden diese Maßnahmen bereits vor Inkrafttreten der NIS-2-Richtlinie etabliert, was auf eine ausgeprägte, proaktive Sicherheitskultur hinweist.

5.5 Ergebnisse aus Themenkategorie 5: Physische Maßnahmen

Die Ergebnisse im Bereich physischer Sicherheitsmaßnahmen zeigen, dass Zugangskontrollsysteme (77 %, n = 10) und die sichere Verwahrung von Hardware (ebenfalls 77 %, n = 10) weit verbreitet sind.

Backup-Systeme an physisch getrennten Standorten kommen bei 69 % der Unternehmen (n = 9) zum Einsatz, was die hohe Priorität der Datenverfügbarkeit unterstreicht. Überwachungskameras und Alarmsysteme werden von 62 % (n = 8) genutzt; mehrere Unternehmen planen eine Ausweitung der Videoüberwachung.

Zusätzlich setzen einzelne Organisationen strukturierte Sicherheitszonen und gestufte Schutzkonzepte um.

Bei der Überprüfung der physischen Maßnahmen zeigt sich, dass 38 % (n = 5) jährliche Prüfungen durchführen, während 23 % (n = 3) auf eine permanente Überwachung im Betriebsalltag setzen, etwa durch tägliche Begehungen. Ein vollständiger Verzicht auf Überprüfungen wurde nicht angegeben.

5.6 Ergebnisse aus Themenkategorie 6: NIS-2 und Cybersicherheitsstandards

Zusätzlich zur NIS-2-Richtlinie nutzen viele Unternehmen etablierte Standards zur Erhöhung ihres Sicherheitsniveaus. 54 % (n = 7) der auskunftgebenden Organisationen setzen ISO/IEC 27001 um, 46 % (n = 6) orientieren sich am BSI-IT-Grundschutz. Darüber hinaus finden branchenspezifische Standards wie ISO/IEC 27019 (Energiesektor) oder der B3S Wasser Anwendung.

Diese Normen dienen primär der Umsetzung von Mindestschutzanforderungen (77 %, n = 10), dem Aufbau von Risikomanagementstrukturen (69 %, n = 9) sowie der Erfüllung von Meldepflichten und der Absicherung von Lieferketten (jeweils 62 %, n = 8).

Die Ergebnisse belegen eine klare Standardorientierung bei der Umsetzung regulatorischer Anforderungen, wobei die Auswahl der Normen an branchenspezifischen Besonderheiten ausgerichtet ist.

5.7 Ergebnisse aus Themenkategorie 7: Herausforderungen und Unterstützungsbedarfe

Die befragten Organisationen identifizieren technische Herausforderungen vor allem in der Systemintegration, der Interoperabilität unterschiedlicher Anwendungen sowie in der eindeutigen Zuordnung kritischer Systeme. Zusätzlich werden Herstellerabhängigkeiten erwähnt, die insbesondere bei der zeitnahen Bereitstellung von Updates zu Problemen führen. Als vorrangige Unterstützungsbedarfe gelten externe Beratung (n = 3), spezifische Schulungsangebote (n = 2) und zusätzliche technische Hilfsmittel (n = 2). Darüber hinaus besteht der Wunsch nach präziseren rechtlichen Vorgaben für die nationale Umsetzung der NIS-2-Richtlinie. Als bewährte Vorgehensweisen werden die Orientierung an etablierten Normen wie ISO/IEC 27001 oder dem BSI-IT-Grundschutz, die frühzeitige Einbindung externer Fachkompetenz sowie die konsequente Etablierung klarer Governance- und Managementstrukturen genannt. Mehrere Unternehmen

betonen zudem, dass ein pragmatisches, schrittweises Vorgehen erforderlich sei, um der Komplexität der Richtlinie angemessen zu begegnen.

5.8 Zusammenfassung und Fazit

Die Auswertung der Befragung zeigt, dass zahlreiche Unternehmen die Anforderungen der NIS-2-Richtlinie bereits strukturell, organisatorisch und technisch adressieren. Häufig erfolgt dies durch die Anwendung etablierter Standards wie ISO/IEC 27001 oder des BSI-IT-Grundschutzes sowie durch umfassende Sensibilisierungs- und Qualifizierungsprogramme. Gleichwohl besteht Optimierungspotenzial bei der formalisierten Risikobewertung, dem systematischen Einbezug externer Sicherheitsanalysen, der Harmonisierung mit weiteren Regelwerken und der konsequenten Einbindung von Lieferkettenaspekten. Die qualitativen Freitextangaben verdeutlichen darüber hinaus eine heterogene Ausgangssituation: Während einzelne Unternehmen bereits über detaillierte, aufeinander abgestimmte Governance- und Risikostrukturen verfügen, befinden sich andere noch im Anfangsstadium einer systematischen Umsetzung. Insgesamt bestätigt die Untersuchung, dass die Implementierung der NIS-2-Richtlinie in der Abwasserwirtschaft Fortschritte zeigt, gleichzeitig aber weiterführende fachliche Unterstützung, klare rechtliche Leitlinien und praxisorientierte Handlungshilfen erforderlich sind, um ein einheitlich hohes Cybersicherheitsniveau zu erreichen.

5.9 Spezifische Anforderungen und Implikationen für den Sektor Abwasser

Die Abwasserwirtschaft stellt innerhalb der Kritischen Infrastrukturen (KRITIS) einen besonders vulnerablen Sektor dar, der durch technologische, organisatorische und strukturelle Besonderheiten gekennzeichnet ist. Die empirischen Ergebnisse dieser Untersuchung zeigen, dass die Umsetzung der NIS-2-Richtlinie in diesem Bereich sowohl spezifische Herausforderungen als auch sektorale Umsetzungspotenziale mit sich bringt. Im Folgenden werden zentrale Besonderheiten des Sektors identifiziert und die relevanten Ergebnisse vor dem Hintergrund dieser Spezifika kontextualisiert.

5.9.1 Strukturelle Fragmentierung und Ressourcenengpässe

Die Analyse der Stichprobe verdeutlicht eine ausgeprägte Heterogenität hinsichtlich der betrieblichen Strukturen, der Ressourcenausstattung und der IT-Sicherheitskompetenzen der befragten Einrichtungen. Vor allem kleinere und mittlere Betreiber weisen häufig eingeschränkte personelle und finanzielle Kapazitäten auf, was die Etablierung umfassender Cybersicherheitsmaßnahmen gemäß NIS-2-Richtlinie erschwert. So verfügen lediglich 54 % der Einrichtungen über ein vollständig implementiertes Risikomanagementsystem, während 46 % von einer teilweisen Umsetzung berichten. Die Erhebung unterstreicht somit die Notwendigkeit zielgruppenspezifischer Unterstützungsmaßnahmen für ressourcenschwache Organisationen.

5.9.2 Technologische Besonderheiten und veraltete Systemlandschaften

Ein wesentliches Charakteristikum des Sektors Abwasser ist die weitreichende Nutzung industrieller Steuerungssysteme (ICS/SCADA), deren Lebenszyklen oftmals über mehrere Jahrzehnte reichen. Die Untersuchung zeigt, dass ein signifikanter Anteil der Systeme nicht oder nur eingeschränkt auf moderne Sicherheitsstandards nachgerüstet werden kann. 69 % der Befragten bestätigen den Einsatz veralteter Systemkomponenten mit eingeschränkter Updatefähigkeit. Hieraus ergibt sich ein erhöhter Schutzbedarf durch netzwerksegmentierende Maßnahmen, Intrusion-Detection-Systeme sowie auf den industriellen Kontext zugeschnittene Monitoringlösungen.

5.9.3 Bedeutung branchenspezifischer Normen und Leitlinien

Die Analyse belegt eine hohe Akzeptanz sektorspezifischer Standards wie dem „Branchenspezifischen Sicherheitsstandard Wasser/Abwasser“ (B3S WA) oder dem ÖWAV-Arbeitsbehelf 67. 77 % der befragten Organisationen gaben an, sich bei der Umsetzung der NIS-2-Anforderungen an mindestens einem dieser Standards zu orientieren. Diese praxisnahen Hilfestellungen ermöglichen eine zielgerichtete Operationalisierung regulatorischer Anforderungen und bieten zugleich Orientierung für Priorisierungsentscheidungen bei der Auswahl technischer und organisatorischer Schutzmaßnahmen.

5.9.4 Kooperationsnetzwerke und sektorspezifischer Wissensaustausch

Die Untersuchung hebt die Relevanz interorganisationaler Kooperationen und des Erfahrungsaustauschs innerhalb des Sektors hervor. 69 % der Einrichtungen pflegen regelmäßige Kooperationen, insbesondere über Fachverbände oder Arbeitskreise. Darüber hinaus setzen 46 % auf externe Dienstleister, um bestehende Ressourcenengpässe auszugleichen und Fachwissen temporär verfügbar zu machen. Die Ergebnisse zeigen, dass sektorale Kooperationsstrukturen maßgeblich zur Bewältigung komplexer sicherheitsrelevanter Anforderungen beitragen und als resilienzstärkender Faktor zu bewerten sind.

5.9.5 Zusammenfassung und sektorale Handlungsperspektiven

Insgesamt verdeutlichen die Befunde, dass die Umsetzung der NIS-2-Richtlinie im Abwassersektor durch eine Vielzahl infrastruktureller, technischer und organisatorischer Besonderheiten geprägt ist. Die fragmentierte Betreiberlandschaft, die technische Heterogenität und die eingeschränkte Ressourcenausstattung erfordern spezifisch angepasste Unterstützungsmechanismen. Gleichzeitig zeigen die Ergebnisse, dass durch den gezielten Einsatz branchenspezifischer Standards und durch die institutionalisierte Kooperation zwischen den Akteuren substantielle Fortschritte erzielt werden können. Für eine nachhaltige Erhöhung der sektoralen Resilienz empfiehlt sich daher die kontinuierliche Weiterentwicklung praxisorientierter

Leitfäden, die Förderung interkommunaler Netzwerke sowie die Bereitstellung gezielter Förder- und Schulungsangebote durch die zuständigen Behörden.

6 BEANTWORTUNG DER FORSCHUNGSFRAGE

Die im Rahmen dieser Arbeit gewonnenen empirischen Erkenntnisse liefern eine fundierte Basis zur Beantwortung der eingangs formulierten Forschungsfrage:

„Wie gestalten und implementieren Abwasserdienstleister im deutschsprachigen Raum strukturelle, organisatorische und technische Maßnahmen zur Einhaltung der NIS-2-Richtlinie, welche Herausforderungen treten dabei auf, und welche Good Practices lassen sich daraus für eine sektorweite Standardisierung der Cybersicherheit ableiten?“

Kapitel 6 fasst die zentralen Ergebnisse der Untersuchung systematisch zusammen und verknüpft diese mit der theoretischen Fundierung der Arbeit. Ziel ist es, die unterschiedlichen Dimensionen der Forschungsfrage differenziert zu beleuchten und die übergeordneten Zusammenhänge zwischen regulatorischen Anforderungen, Umsetzungspraxis und sektorspezifischen Rahmenbedingungen zu analysieren.

Dabei wird auf die in Kapitel 5 dargestellten empirischen Befunde zurückgegriffen und aufgezeigt, inwieweit die formulierte Forschungshypothese durch die Datenauswertung gestützt oder zu modifizieren ist. Zusätzlich erfolgt eine Ableitung von sektoralen Good Practices, die als Grundlage für eine standardisierte Herangehensweise an die NIS-2-Implementierung im Abwassersektor dienen können.

Auf dieser Basis liefert das Kapitel einen Beitrag zur theoriegeleiteten Reflexion der Ergebnisse und bietet praxisorientierte Handlungsperspektiven für Organisationen, Normungsgremien und politische Entscheidungsträger.

6.1 Zusammenfassung der Ergebnisse

Die vorliegende wissenschaftliche Arbeit untersuchte die Umsetzung der NIS-2-Richtlinie im Abwassersektor mittels eines Mixed-Methods-Ansatzes. Ziel war es, den aktuellen Umsetzungsstand differenziert zu erfassen, bestehende Herausforderungen zu identifizieren und daraus Good-Practice-Ansätze sowie Handlungsempfehlungen abzuleiten. Im Mittelpunkt stand eine empirische Befragung von Organisationen, die im Sinne der NIS-2-Richtlinie als wesentliche Einrichtungen klassifiziert werden.

Die Auswertung zeigt, dass ein Großteil der befragten Unternehmen bereits konkrete Maßnahmen zur Stärkung ihrer Cybersicherheitsstrukturen implementiert hat. Regelmäßige Schulungen werden von 92 % der Teilnehmer Organisationen durchgeführt. Klare Zuständigkeiten sind in 85 % der Fälle definiert, und ebenso viele Einrichtungen verfügen über Notfallpläne sowie Frühwarnsysteme. Ein Risikomanagementsystem wurde in 54 % der Unternehmen vollständig und in 46 % zumindest teilweise eingeführt.

Die strukturelle Verankerung der Cybersicherheit ist heterogen: Bei 85 % der Befragten ist diese in der IT-Abteilung integriert, während 38 % darüber hinaus eine spezialisierte Abteilung

unterhalten. Die Verantwortung liegt in 77 % der Fälle auf Ebene der Geschäftsleitung; zugleich greifen 46 % der Unternehmen zur Unterstützung auf externe Dienstleister zurück.

Zur Erfüllung der NIS-2-Anforderungen bedienen sich die Unternehmen vor allem etablierter Normen. Am häufigsten genannt wurden ISO/IEC 27001, der BSI-IT-Grundschutz sowie branchenspezifische Regelwerke wie der B3S Wasser/Abwasser. Diese Standards kommen insbesondere bei der Festlegung von Mindestschutzanforderungen, beim Aufbau von Risikomanagementstrukturen und bei der Umsetzung von Meldepflichten zum Tragen.

Die empirischen Befunde dieser Arbeit zeigen, dass die Umsetzung der NIS-2-Richtlinie im Abwassersektor des deutschsprachigen Raums bereits in weiten Teilen angestoßen wurde, sich jedoch noch in unterschiedlichen Reifegraden befindet. Besonders hervorzuheben ist, dass ein Großteil der befragten Organisationen grundlegende technische und organisatorische Sicherheitsmaßnahmen bereits implementiert hat. So gaben über 90 % der Unternehmen an, regelmäßige Schulungen durchzuführen und klare Zuständigkeiten für die Cybersicherheit definiert zu haben. Diese Ergebnisse verweisen auf ein wachsendes Problembewusstsein und eine strategische Aufwertung der Informationssicherheit innerhalb des Sektors.

Gleichzeitig treten spezifische strukturelle Herausforderungen deutlich zutage: Die kleinteilige Betreiberlandschaft, insbesondere die Vielzahl kommunaler und mittelgroßer Abwasserbetriebe mit begrenzten IT-Ressourcen, wirkt als begrenzender Faktor für die umfassende Umsetzung der Richtlinie. Die Daten belegen zudem, dass veraltete technische Infrastrukturen – insbesondere nicht patchbare Steuerungssysteme – die Implementierung moderner Schutzmaßnahmen erschweren.

Positiv zu vermerken ist die Orientierung an branchenspezifischen Leitlinien wie dem B3S Wasser/Abwasser oder dem ÖWAV-Arbeitsbehelf. Diese Instrumente werden von über drei Viertel der antwortenden Einrichtungen genutzt und dienen somit als tragfähige Grundlage für eine standardisierte Umsetzung der NIS-2-Anforderungen im Abwassersektor. Ergänzend wurden im Rahmen der qualitativen Analyse zahlreiche Good Practices identifiziert, die sowohl für einzelne Betriebe als auch für die sektorweite Koordination nutzbar gemacht werden können.

Insgesamt lässt sich festhalten, dass der Sektor Abwasser in Bezug auf Cybersicherheit zunehmend strukturiert vorgeht, jedoch weiterhin vor erheblichen Umsetzungs- und Ressourcenschwierigkeiten steht, die eine gezielte politische und regulatorische Unterstützung erforderlich machen.

6.2 Beantwortung der Forschungsfrage

Die Befragung der Abwasserdienstleister im deutschsprachigen Raum zeigt, dass strukturelle, organisatorische und technische Maßnahmen zur Einhaltung der NIS-2-Richtlinie bereits in vielen Fällen vorhanden sind oder sich im Aufbau befinden. Zugleich bestehen deutliche Unterschiede im Reifegrad der Umsetzung. Diese Diskrepanz eröffnet Chancen für eine sektorweite Standardisierung, verdeutlicht jedoch auch die Herausforderungen, die bei der Harmonisierung von Vorgehensweisen, der Ressourcenallokation und der Integration branchenspezifischer

Besonderheiten auftreten. Insgesamt bestätigen die Ergebnisse, dass die NIS-2-Konformität zwar ein gemeinsames Ziel darstellt, die konkrete Umsetzung jedoch stark von den individuellen Ausgangsbedingungen und strategischen Prioritäten der jeweiligen Organisation abhängt.

6.2.1 Strukturelle Gestaltung und Verantwortlichkeiten

Die Verantwortung für Cybersicherheit ist in 85 % der Unternehmen (n = 11) innerhalb der bestehenden IT-Abteilung verankert. In 38 % der Unternehmen (n = 5) bestehen zusätzlich spezialisierte Cybersicherheits-abteilungen, was auf eine wachsende strategische Priorisierung hindeutet. Verantwortlichkeiten liegen in 77 % der Fälle auf Geschäftsführungsebene und werden durch spezialisierte Rollen (54 %) sowie externe Dienstleister (46 %) ergänzt. Cybersicherheit ist somit strukturell verankert, allerdings existieren spezialisierte Einheiten noch nicht flächendeckend. Für eine sektorweite Standardisierung wird empfohlen, klare Verantwortlichkeitsmodelle zu etablieren, welche operative und strategische Aspekte gleichermaßen abdecken.

6.2.2 Organisatorische Maßnahmen

Regelmäßige Cybersicherheitsschulungen werden in 92 % der Unternehmen (n = 12) durchgeführt. Klare Verantwortlichkeiten und Eskalationswege sind in 85 % der Unternehmen (n = 11) definiert. Notfallkommunikation und Cybersicherheits-managementsysteme sind in jeweils 69 % der Organisationen etabliert. Diese Ergebnisse verdeutlichen einen systematischen organisatorischen Rahmen. Für eine sektorweite Standardisierung bieten insbesondere die strukturierten Schulungs- und Eskalationskonzepte geeignete Vorbilder.

6.2.3 Technische Maßnahmen

Zentrale Schutzmechanismen wie Firewalls, Netzwerksicherheits-lösungen, Endpunktschutz und Multi-Faktor-Authentifizierung werden in 62 % der Unternehmen (n = 8) eingesetzt. Ergänzend kommen spezialisierte Lösungen, beispielsweise Netzwerksegmentierung, Security-Information-and-Event-Management-Systeme sowie OT-/IT-Segregation, zur Anwendung. Die technische Umsetzung entspricht einem hohen Niveau und orientiert sich vielfach an Defense-in-Depth-Strategien. Eine sektorweite Standardisierung kann auf diesen verbreiteten Technologien aufbauen, sollte allerdings die spezifischen Anforderungen der Abwasserwirtschaft, insbesondere den Schutz von OT-Systemen, stärker berücksichtigen.

6.2.4 Herausforderungen bei der Umsetzung

Die wesentlichen Herausforderungen liegen in der Systemintegration und Interoperabilität Die wesentlichen Herausforderungen betreffen

- die Integration und Interoperabilität von IT- und OT-Systemen,
- Herstellerabhängigkeiten, beispielsweise fehlende Sicherheits-updates,

- die eindeutige Identifikation kritischer Systeme sowie
- Ressourcenengpässe in Bezug auf Personal und Fachwissen.

Diese Ergebnisse verdeutlichen den Bedarf an sektorweiten Unterstützungsangeboten, etwa praxisnahen Leitfäden oder Musterlösungen für typische OT-Umgebungen, um die Umsetzung der NIS-2-Richtlinie effektiv zu fördern.

6.2.5 Good Practices für eine sektorweite Standardisierung

Die Analyse identifiziert mehrere Vorgehensweisen, die als Grundlage einer sektorweiten Standardisierung dienen können. Erstens empfiehlt sich eine frühzeitige Verankerung der Cybersicherheit auf Geschäftsführungsebene, um der Thematik hinreichende strategische Priorität einzuräumen. Zweitens sollte der Aufbau organisatorischer Maßnahmen, darunter regelmäßige Schulungen, eindeutig definierte Eskalationsprozesse und strukturierte Krisenkommunikation, konsequent verfolgt werden. Drittens bewährt sich der Einsatz etablierter technischer Standards, etwa ISO/IEC 27001 oder der BSI IT-Grundschutz, um Sicherheitsmaßnahmen systematisch zu strukturieren. Viertens hat sich ein schrittweises, pragmatisches Vorgehen beim Umsetzen komplexer Anforderungen bewährt; ein sogenannter Bottom-up-Ansatz unter Zuhilfenahme verständlicher Checklisten und Handlungsempfehlungen, beispielsweise der BSI-WiBA-Reihe, erleichtert den Einstieg. Schließlich sollte ein gezielter Ausbau von Awareness-Programmen erfolgen und die Risikoanalyse in bestehende Betriebsprozesse integriert werden.

6.3 Handlungsempfehlungen für die Praxis

Auf Grundlage der empirischen Ergebnisse sowie der theoretischen Analyse lassen sich mehrere praxisorientierte Handlungsempfehlungen ableiten, die die Umsetzung der NIS-2-Richtlinie im Abwassersektor gezielt unterstützen können. Diese Empfehlungen richten sich sowohl an Betreiber von Abwasseranlagen als auch an Aufsichtsbehörden, Fachverbände und politische Entscheidungsträger. Sie adressieren zentrale Defizite und zeigen zugleich konkrete Maßnahmen zur Stärkung der sektoralen Cybersicherheitsresilienz auf.

6.3.1 Entwicklung eines sektorspezifischen, modularen Umsetzungsleitfadens

Einige der befragten Organisationen äußerten den Wunsch nach einem verbindlichen, aber zugleich praxisnahen Leitfaden, der die regulatorischen Anforderungen der NIS-2-Richtlinie in sektorbezogene Handlungsschritte übersetzt. Angesichts der hohen Diversität der Akteurslandschaft empfiehlt sich ein modularer Aufbau, der sowohl große städtische Betriebe als auch kleine, kommunale Einrichtungen adressiert. Die Orientierung am B3S Wasser/Abwasser sowie am ÖWAV-Arbeitsbehelf 67 sollte dabei beibehalten und durch konkrete Fallbeispiele und Umsetzungsmuster ergänzt werden.

6.3.2 Etablierung zentraler Unterstützungs- und Beratungsstellen

Die Untersuchung hat gezeigt, dass insbesondere kleinere Abwasserdienstleister unter erheblichen personellen und fachlichen Engpässen leiden. Die Einrichtung von regionalen oder nationalen Kompetenzzentren für Cybersicherheit im Bereich Wasser/Abwasser könnte hier Abhilfe schaffen. Solche Stellen sollten nicht nur beratend tätig sein, sondern auch Schulungsangebote, Vorlagen für Risikoanalysen sowie regelmäßige Awareness-Kampagnen bereitstellen.

6.3.3 Förderung interkommunaler und verbandlicher Kooperation

Ein weiterer zentraler Befund betrifft die hohe Bedeutung von Netzwerken und Fachverbänden für den Wissensaustausch und die Verbreitung von Good Practices. Dieser sektorinterne Austausch sollte strukturell gefördert und in regelmäßige, qualitätsgesicherte Formate überführt werden – etwa durch standardisierte Benchmarking-Initiativen, digitale Austauschplattformen oder praxisorientierte Peer-Reviews.

6.3.4 Integration von Cybersicherheit in Förderprogramme

Um gezielt Investitionen in IT-Sicherheitsmaßnahmen zu stimulieren, ist eine Verankerung von Cybersicherheit als Förderkriterium in bestehenden oder neuen Programmen der Infrastrukturfinanzierung zu empfehlen. Gefördert werden sollten insbesondere:

- die Modernisierung veralteter ICS/SCADA-Systeme,
- die Einführung von Cybersicherheitsmanagementsystemen (CSMS),
- sowie technische Schutzmaßnahmen wie Netzwerksegmentierung und Angriffserkennung.

Diese finanzielle Unterstützung kann insbesondere für kleinere Einrichtungen einen Anreiz zur proaktiven Umsetzung der Richtlinie darstellen.

6.3.5 Verstärkte Schulungs- und Qualifizierungsinitiativen

Die Qualifikation des Personals wurde in der Befragung mehrfach als erfolgskritischer Faktor identifiziert. Empfohlen wird daher der Aufbau standardisierter Weiterbildungsformate für IT- und Betriebspersonal in Zusammenarbeit mit Bildungseinrichtungen, Fachverbänden und Zertifizierungsstellen. Ziel sollte es sein, einheitliche Kompetenzprofile für Cybersicherheitsverantwortliche im Abwassersektor zu etablieren.

6.3.6 Verpflichtende Integration von Lieferkettenaspekten

Die NIS-2-Richtlinie legt besonderen Fokus auf die Absicherung der Lieferkette – ein Aspekt, der in vielen Organisationen bislang unterrepräsentiert ist. Es wird empfohlen, Mindestanforderungen für die Sicherheitsbewertung von Dienstleistern zu formulieren und standardisierte Vertragsklauseln bereitzustellen, die eine sichere Einbindung externer Partner gewährleisten.

6.3.7 Verankerung von Cybersicherheit auf Leitungsebene

Cybersicherheit sollte als strategisches Handlungsfeld verstanden und auf oberster Führungsebene (C-Level) institutionell verankert werden. Die empirischen Ergebnisse belegen, dass Unternehmen mit expliziter Leitungseinbindung ein höheres Maß an Umsetzungsreife aufweisen. Eine verbindliche Verankerung auf Geschäftsführungsebene erhöht die Priorität sicherheitsrelevanter Themen und verbessert die Allokation von Ressourcen.

6.3.8 Benennung dedizierter Cybersicherheitsbeauftragter

Die Einrichtung und institutionelle Einbindung eines Chief Information Security Officer (CISO) oder vergleichbarer Funktionen ist zentral für den Aufbau einer professionellen Informationssicherheitsorganisation. Die klare Zuweisung von Verantwortlichkeiten fördert die operative Wirksamkeit und gewährleistet eine kohärente Steuerung aller sicherheitsrelevanten Maßnahmen.

6.3.9 Verpflichtende Awareness-Schulungen für Mitarbeitende

Sicherheitsbewusstsein ist ein kritischer Erfolgsfaktor im Umgang mit Cyberrisiken. Die Einführung regelmäßiger, verpflichtender Schulungen für alle Mitarbeitenden trägt entscheidend dazu bei, menschliche Fehler zu minimieren und eine organisationsweite Sicherheitskultur zu etablieren. Inhalte sollten praxisnah, rollenbasiert und auf die spezifischen Risiken des Sektors ausgerichtet sein.

6.3.10 Nutzung kombinierter Sicherheitsstandards als Orientierungsrahmen

Eine standardbasierte Umsetzung der NIS-2-Anforderungen sollte auf einem integrativen Ansatz basieren, der international anerkannte Normen wie ISO/IEC 27001, den BSI IT-Grundschutz sowie sektorspezifische Standards wie den B3S Wasser/Abwasser kombiniert. Diese kombinierte Orientierung bietet Flexibilität, Anschlussfähigkeit und regulatorische Sicherheit.

6.3.11 Etablierung technischer Frühwarn- und Monitoring-Systeme

Zur Erhöhung der technischen Reaktionsfähigkeit empfiehlt sich der flächendeckende Einsatz von Frühwarnsystemen, Intrusion-Detection-Systemen (IDS) sowie automatisierten

Monitoringlösungen. Diese Instrumente ermöglichen eine kontinuierliche Überwachung kritischer Systeme und eine frühzeitige Identifikation von Anomalien oder Angriffen.

6.3.12 Integration von Lieferkettenaspekten in das Risikomanagement

Die Bewertung und Absicherung von Drittanbietern ist verpflichtend in die Risikomanagementprozesse zu integrieren. Es sollten standardisierte Kriterien und vertragliche Anforderungen entwickelt werden, um die Cybersicherheit in vorgelagerten und nachgelagerten Lieferketten nachhaltig sicherzustellen.

6.3.13 Entwicklung eines sektorspezifischen, modularen Umsetzungsleitfadens

Ein modular aufgebauter Leitfaden, der regulatorische Anforderungen in praxisnahe Handlungsanleitungen übersetzt, kann die Umsetzung insbesondere für kleine und mittlere Betriebe erheblich erleichtern. Der Leitfaden sollte differenzierte Umsetzungsniveaus abbilden und mit konkreten Maßnahmenkatalogen, Best-Practice-Beispielen und Mustervorlagen ergänzt werden.

6.3.14 Etablierung zentraler Unterstützungs- und Beratungsstellen

Die Einrichtung von überregionalen Kompetenzzentren für Cybersicherheit im Bereich Wasser/Abwasser würde insbesondere ressourcenschwachen Organisationen gezielte Unterstützung bieten. Diese Stellen sollten Beratung, Weiterbildung, Vorlagenbereitstellung und Plattformangebote für den sektoralen Austausch bündeln.

6.3.15 Förderung interkommunaler und verbandlicher Kooperation

Fachverbände und regionale Netzwerke fungieren als Wissensvermittler und Multiplikatoren. Der strukturierte Austausch bewährter Verfahren sowie die Durchführung gemeinsamer Übungen, Peer-Assessments und Benchmarking-Initiativen sollten ausgebaut und institutionell gefördert werden.

6.3.16 Integration von Cybersicherheit in Förderprogramme

Die Verankerung von IT- und Cybersicherheitsmaßnahmen als explizite Fördertatbestände in bestehenden Infrastrukturprogrammen stellt einen wesentlichen Anreiz für Investitionen dar. Förderfähig sollten insbesondere Maßnahmen zur Modernisierung industrieller Steuerungssysteme, zur Einführung von Cybersicherheitsmanagementsystemen sowie zur Härtung der Netzwerkinfrastruktur sein.

6.3.17 Verstärkung von Schulungs- und Qualifizierungsinitiativen

Es ist notwendig, branchenspezifische Weiterbildungsformate für IT- und Betriebspersonal zu entwickeln, zu standardisieren und regelmäßig anzubieten. Ziel ist der Aufbau sektorspezifischer Kompetenzprofile für Cybersicherheitsverantwortliche und die Etablierung eines kontinuierlichen Qualifizierungsprogramms.

6.3.18 Intensivierung des sektorinternen und sektorübergreifenden Informationsaustauschs

Der Austausch zwischen Abwasserdienstleistern sowie mit angrenzenden KRITIS-Sektoren (z. B. Energie, Wasser, Kommunen) sollte systematisch verstärkt werden. Durch den Aufbau von Informations- und Frühwarnnetzwerken, etwa über Computer Emergency Response Teams (CERTs), kann die kollektive Resilienz gegenüber Cyberbedrohungen signifikant gesteigert werden.

Zusammenfassend lässt sich festhalten, dass die erfolgreiche Umsetzung der NIS-2-Richtlinie im Sektor Abwasser ein koordiniertes Zusammenspiel von Standardisierung, Führung, Qualifizierung und sektorübergreifender Kooperation erfordert. Die formulierten Empfehlungen zielen darauf ab, strukturelle Barrieren abzubauen, handlungsleitende Orientierung zu bieten und die sektorale Widerstandsfähigkeit gegenüber zukünftigen Cyberrisiken nachhaltig zu stärken.

7 CONCLUSIO UND AUSBLICK

Die vorliegende Arbeit untersuchte die Umsetzung der NIS-2-Richtlinie im Abwassersektor im deutschsprachigen Raum und analysierte bestehende Strukturen, Herausforderungen sowie Good Practices im Umgang mit Cybersicherheitsanforderungen. Die Ergebnisse liefern sowohl theoretische Erkenntnisse als auch praxisrelevante Implikationen für die Weiterentwicklung der Informationssicherheit in einem besonders vulnerablen KRITIS-Sektor.

Die Arbeit zeigt eindrücklich, dass die Cybersicherheit im Abwassersektor nicht nur eine technische Herausforderung darstellt, sondern ein strategisches Querschnittsthema ist, das Governance, Ressourcenverfügbarkeit und Kooperationsfähigkeit gleichermaßen betrifft. Die systematische Umsetzung der NIS-2-Richtlinie bietet die Chance, den Sektor nachhaltig zu professionalisieren und widerstandsfähiger gegenüber zukünftigen Bedrohungen zu machen – vorausgesetzt, die entsprechenden organisatorischen, normativen und politischen Rahmenbedingungen werden geschaffen und kontinuierlich weiterentwickelt.

Kapitel 7 fasst zentrale Schlussfolgerungen zusammen, reflektiert die wissenschaftliche und praktische Relevanz der Arbeit, benennt bestehende Limitationen und eröffnet Perspektiven für zukünftige Forschungsvorhaben.

7.1 Wissenschaftlicher und praktischer Beitrag

Die Arbeit leistet einen substantiellen Beitrag zur bislang nur rudimentär erforschten Umsetzung regulatorischer Cybersicherheitsanforderungen im Bereich der Abwasserwirtschaft. Der gewählte Mixed-Methods-Ansatz erlaubt eine differenzierte Betrachtung der organisationalen Umsetzungspraxis und adressiert eine signifikante Forschungslücke an der Schnittstelle von Wirtschaftsinformatik, Verwaltungswissenschaft und Infrastrukturforschung.

Aus wissenschaftlicher Perspektive zeigt die Arbeit, wie regulatorische Vorgaben – im vorliegenden Fall die NIS-2-Richtlinie – durch Akteure in kritischen Infrastrukturen rezipiert, interpretiert und operationalisiert werden. Die Ergebnisse belegen, dass die Implementierung nicht als rein technisches Vorhaben, sondern als komplexer, sozio-technischer Prozess verstanden werden muss, der von strukturellen Rahmenbedingungen, institutionellen Ressourcen und kulturellen Faktoren beeinflusst wird. Der verhaltensorientierte Ansatz der Wirtschaftsinformatik hat sich dabei als geeigneter konzeptioneller Rahmen erwiesen, um sowohl individuelle als auch organisationale Handlungslogiken abzubilden.

Für die Praxis liefert die Arbeit konkrete und differenziert aufbereitete Erkenntnisse zu bestehenden Umsetzungsstrategien, typischen Problemfeldern und bewährten Lösungsansätzen in der Abwasserwirtschaft. Diese Informationen bieten eine tragfähige Grundlage für politische Entscheidungsträger, Fachverbände und Betreiberorganisationen, um bestehende Maßnahmen weiterzuentwickeln, neue Standards zu formulieren und Unterstützungsangebote zielgruppengerecht zu gestalten. Die Ableitung von insgesamt zwölf Handlungsempfehlungen stellt einen praxisnahen Beitrag zur sektorspezifischen Standardisierung von

Cybersicherheitsmaßnahmen dar und unterstützt eine strukturierte Umsetzung der Richtlinienvorgaben.

7.2 Limitationen und Kritikpunkte

Trotz ihres wissenschaftlichen Anspruchs unterliegt die Arbeit gewissen Limitationen, die im Sinne wissenschaftlicher Transparenz kritisch zu reflektieren sind. Zunächst ist auf den explorativen Charakter der empirischen Erhebung hinzuweisen. Die quantitative Datenerhebung basiert auf einer nicht-repräsentativen Stichprobe aus dem deutschsprachigen Raum, wodurch die Generalisierbarkeit der Ergebnisse eingeschränkt ist. Die Teilnahme erfolgte freiwillig, sodass ein potenzieller Self-Selection-Bias nicht auszuschließen ist. Es ist denkbar, dass insbesondere Organisationen mit bereits höherem Sicherheitsbewusstsein oder Umsetzungsstand zur Teilnahme tendierten.

Darüber hinaus beschränkte sich die Datenerhebung auf eine Momentaufnahme im Jahr 2025, in einer Phase, in der viele Organisationen sich noch in der Umsetzungsplanung oder in frühen Implementierungsphasen befanden. Dies erschwert die Bewertung langfristiger Wirksamkeit einzelner Maßnahmen oder die Einschätzung tatsächlicher Compliance-Niveaus. Zukünftige Langzeitstudien oder Panel-Erhebungen könnten hier wertvolle Ergänzungen leisten.

Methodisch ist zudem anzumerken, dass qualitative Aussagen zwar durch systematische Inhaltsanalyse strukturiert wurden, aber naturgemäß auf subjektiven Einschätzungen der Befragten beruhen. Eine Validierung durch triangulierende Datenquellen (z. B. technische Audits, Dokumentenanalysen) konnte im Rahmen dieser Arbeit nicht erfolgen, wäre aber für tiefergehende Analysen zielführend.

7.3 Potenziale für weiterführende Forschung

Die vorliegenden Ergebnisse eröffnen verschiedene Forschungsansätze, die auf eine vertiefende Auseinandersetzung mit der Cybersicherheit kritischer Infrastrukturen im Allgemeinen und des Abwassersektors im Speziellen abzielen. Ein naheliegender nächster Schritt wäre die Durchführung repräsentativer, länderübergreifender Vergleichsstudien zur Umsetzung der NIS-2-Richtlinie in verschiedenen Sektoren und Verwaltungskontexten. Dabei könnte untersucht werden, wie politische, rechtliche und kulturelle Unterschiede die Umsetzungspraxis beeinflussen.

Ein weiteres Forschungspotenzial liegt in der Evaluation der Effektivität einzelner Cybersicherheitsmaßnahmen unter realen Bedingungen. Hierfür wären feldexperimentelle Designs, Case Studies oder Simulationen denkbar, die beispielsweise untersuchen, welche Kombinationen von Maßnahmen (z. B. organisatorisch vs. technisch) besonders wirksam zur Erhöhung der Resilienz beitragen. Ergänzend dazu wäre die Entwicklung und Validierung eines sektorspezifischen Reifegradmodells für die Cybersicherheit in der Abwasserwirtschaft ein

lohnendes Ziel – etwa in Anlehnung an existierende Modelle wie COBIT, TISAX oder das CAF (Cyber Assessment Framework).

Darüber hinaus eröffnet die zunehmende Konvergenz von physischer und digitaler Infrastruktur neue Forschungsfragen an der Schnittstelle von Cybersecurity, Smart Water Systems und Industrie 4.0. Hier könnten technologische Entwicklungen (z. B. Sensorintegration, KI-gestützte Bedrohungserkennung) ebenso wie Fragen der Governance und Ethik (z. B. Datensouveränität, Überwachung) in den Blick genommen werden.

7.4 Ausblick auf die Zukunft der Cybersicherheit im Sektor Abwasser

Mit Blick auf die kommenden Jahre zeichnet sich ab, dass die Anforderungen an Cybersicherheit im Abwassersektor weiter zunehmen werden – sowohl durch regulatorischen Druck als auch durch wachsende Bedrohungslagen. Die zunehmende Vernetzung von Betriebstechnologie (Operational Technology, OT) und Informationstechnologie (IT), die Integration cloudbasierter Systeme sowie die zunehmende Abhängigkeit von externen Dienstleistern erhöhen die potenziellen Angriffsflächen erheblich.

Die Umsetzung der NIS-2-Richtlinie stellt hierbei nur einen ersten Schritt dar. Langfristig wird es darauf ankommen, Cybersicherheit nicht als reaktive Compliance-Maßnahme, sondern als integralen Bestandteil der betrieblichen Strategie zu verankern. Dies setzt voraus, dass nicht nur Technik und Prozesse, sondern auch Organisationskultur, Führungsverständnis und Qualifizierungsstrategien weiterentwickelt werden.

Besonders im Sektor Abwasser wird es darauf ankommen, strukturelle Unterstützungsmechanismen auszubauen. Dazu gehören der flächendeckende Zugang zu branchenspezifischem Wissen, die finanzielle Förderung sicherheitsrelevanter Investitionen und die Etablierung verlässlicher Kooperationsnetzwerke. Eine Schlüsselrolle kommt dabei den Fachverbänden zu, die als Brückenakteure zwischen Regulierung, Technik und Praxis fungieren können.

Langfristig sollten sektorübergreifende Synergien im KRITIS-Kontext stärker genutzt werden. Ein kooperativer Sicherheitsansatz, der Wissen, Werkzeuge und Standards aus angrenzenden Infrastrukturbereichen aufgreift und überträgt, kann die Resilienz des Sektors Abwasser nachhaltig erhöhen.

ANHANG A - 1. Anhang: Fragenkatalog der Befragung

Fragen aus Themenkategorie 1 „Governance“

Frage 1: Wie ist die Cybersicherheit in Ihrem Unternehmen strukturell organisiert?

a) Es gibt eine dedizierte Abteilung für Cybersicherheit

b) Cybersicherheit wird von der IT-Abteilung mitverantwortet

c) Cybersicherheit ist Aufgabe eines externen Dienstleisters

d) Es gibt keine dedizierte Abteilung für Cybersicherheit

Frage 2: Welche Führungsebene ist in ihrem Unternehmen für Cybersicherheit bzw. die Umsetzung der NIS-2-RL verantwortlich?

a) Geschäftsführung

b) IT-Abteilung

c) Informationssicherheitsbeauftragte (CISO/ISO)

d) Externer Dienstleister

e) Sonstiges (bitte spezifizieren:)

Frage 3: Welche Governance-Maßnahmen setzen sie zur Erfüllung der NIS-2-Richtlinie um?

a.) Ernennung Sicherheitsverantwortlichen

b.) Entwicklung und Umsetzung IS-Policies

c.) Etablierung eines Risikomanagement-Systems

d.) Sicherstelllung eines Incident Response Plans

e.) Durchführung von Audits

f.) Zusammenarbeit und Informationsaustausch

g.) Schutz von Lieferketten

h.) Meldesysteme und Notfallpläne

i.) Cybersicherheitsmonitoring und Frühwarnsysteme

j.) Schulung und Sensibilisierungsprogramme

Fragen aus Themenkategorie 2 „Organisatorische Maßnahmen“

Frage 4: Welche organisatorischen Maßnahmen haben Sie zur Sicherstellung der Cybersicherheit gemäß der NIS-2-Richtlinie implementiert?

a) Etablierung eines Cybersicherheitsmanagementsystems

b) Durchführung regelmäßiger Schulungen zur Cybersicherheit

c) Einführung klarer Kommunikationsprozesse im Krisenfall

d) Festlegung von Verantwortlichkeiten und Eskalationswegen

e) Sonstiges (bitte spezifizieren)

Fragen aus Themenkategorie 3 „Risikomanagement“

Frage 5: Haben Sie ein Risikomanagementsystem für Informations- und Cybersicherheit implementiert?

a) Ja

b) Nein

c) Teilweise

Frage 6: Welche der folgenden Risikoanalyseverfahren setzen Sie ein?

a) Bedrohungsanalyse und Schwachstellenbewertung

b) Risikoabschätzungen für IT-Systeme und Prozesse

c) Stresstests und Simulationen von Cyberangriffen

d) Sonstige Verfahren

Frage 7: Wie definieren Sie die Risikobewertungskriterien für die Cybersicherheit in Ihrem Unternehmen?

a) Basierend auf gesetzlichen Vorgaben (z.B. NIS-2)

b) Interne Richtlinien und Standards

c) Externe Beratung durch Sicherheitsdienstleister

d) Sonstige Verfahren

Frage 8: Welche Faktoren berücksichtigen Sie bei der Festlegung der Risikobewertungskriterien?

a) Bedrohungslandschaft (z.B. Arten von Cyberangriffen)

b) Kritikalität der Systeme und Daten

c) Geschäftsauswirkungen (finanziell, rechtlich, reputationsbezogen)

d) Anforderungen von Drittanbietern/Dienstleistern

e) Sonstige

Frage 9: Welche Methoden zur Risikobeurteilung setzen Sie in Ihrem Unternehmen ein?

a) Qualitative Risikobeurteilung (subjektive Einschätzungen)

b) Quantitative Risikobeurteilung (numerische Bewertungen)

c) Kombination aus beidem

d) Keine formale Methode zur Risikobeurteilung

Frage 10: Wie wird die Kritikalität der einzelnen Bedrohungen in Ihrem Unternehmen ermittelt?“

a) Basierend auf der Eintrittswahrscheinlichkeit

b) Basierend auf dem potenziellen Schaden für das Unternehmen

c) Durch externe Sicherheitsanalysen

d) Andere Methoden

Fragen aus Themenkategorie 4 „Technische Maßnahmen“

Frage 11: Welche technischen Cybersicherheitsmaßnahmen haben Sie implementiert um den Anforderungen der NIS-2-Richtlinie zu entsprechen?

a) Firewall-Systeme und Netzwerksicherheitslösungen

b) Endpunkt-Sicherheitslösungen (Antivirus, EDR)

c) Datenverschlüsselung und sichere Kommunikation

d) Authentifizierungssysteme (z.B. Multi-Faktor-Authentifizierung)

e) Sonstige

Fragen aus Themenkategorie 5 „Physische Maßnahmen“

Frage 12: Welche physischen Maßnahmen setzen Sie ein, um den Schutz Ihrer IT- und Netzwerksysteme zu gewährleisten?

a) Zugangskontrollsysteme (z.B. Schlüssel, Karten, biometrische Systeme)

b) Überwachungskameras und Sicherheitsalarmsysteme

c) Sichere Verwahrung von Hardware in Serverräumen

d) Backup-Systeme an sicheren Standorten

e) Sonstiges

Frage 13: Wie häufig werden physische Sicherheitsmaßnahmen überprüft?

a) Monatlich

b) Vierteljährlich

c) Jährlich

d) Keine regelmäßige Überprüfung

Fragen aus Themenkategorie 6 „NIS-2 und Cybersicherheitsstandards“

Frage 14: Welche zusätzlichen Informations- und Cybersicherheits-standards oder -normen setzen Sie neben der NIS-2-Richtlinie um?

a) ISO/IEC 27001

b) NIST Cybersecurity Framework

c) BSI IT-Grundschutz

d) Sonstige

Frage 15: Für welche Anforderungen der NIS-2-Richtlinie setzen die Informations- und Cybersicherheitsstandards bzw. Teile/Kapitel dieser Standards ein?

a.) Einführung von Mindeststandards und Basissicherheitsanforderungen

b.) Risikomanagement

c.) Krisenmanagement

d.) Meldepflichten für Sicherheitsvorfälle

e.) Anforderungen für die Lieferkette

f.) Kollaboration und Informationsaustausch

g.) Harmonisierung der NIS2-Richtlinie mit anderen Regelungen (z.B. DSGVO)

h.) Sonstige (bitte spezifizieren:)

Fragen aus Themenkategorie 7 „Anregungen für zukünftige Leitfäden/Standards zur NIS-2-Richtlinie“

Frage 16: Welche technischen Herausforderungen haben Sie bei der Implementierung der NIS-2-Richtlinie identifiziert?

Frage 17: Welche weiteren Unterstützungsmöglichkeiten oder Ressourcen benötigen Sie, um die Anforderungen der NIS-2-Richtlinie vollständig zu erfüllen?

Frage 18: Was sind aus Ihrer Sicht die wichtigsten Good Practices bei der Umsetzung der NIS-2-Richtlinie?

ANHANG B - 2. Anhang: Befragungsantworten Rohdaten

Befragungsantworten Rohdaten

	Stadt 1	Stadt 2	Stadt 3	Stadt 4	Stadt 5	Stadt 6	Stadt 7	Stadt 8	Stadt 9	Stadt 10	Stadt 11	Stadt 12	Stadt 13	Anzahl der Städte (n)	Städte (%)	Anzahl Städte (ohne Zusatzangaben)	Städte (ohne Zusatzangaben) (%)	Keine Angaben	Keine Angaben (%)
Themenkategorie 1: Governance																			
Frage 1: Wie ist die Cybersicherheit in Ihrem Unternehmen strukturell organisiert?																			
a) Es gibt eine dedizierte Abteilung für Cybersicherheit						x		x Cybersicherheit ist in einer Stabsstelle direkt an der Geschäftsführung eingeo	x Bei der Konzernmutter wird das Thema durch einen CISO mit 3 Mitarbeitern verantwortet und von dort werden wir mit betreut.	x			x	5	38%	3	23%	0	0%
b) Cybersicherheit wird von der IT-Abteilung mitverantwortet	x		x (extern:SOC, SIRT)	x	x	x	x			x	x	x	x	11	85%	9	69%	0	0%
c) Cybersicherheit ist Aufgabe eines externen Dienstleisters				x										1	8%	1	8%	0	0%
d) Es gibt keine dedizierte Abteilung für Cybersicherheit										x				1	8%	0	0%	0	0%
Frage 2: Welche Führungsebene ist für die Cybersicherheit verantwortlich?																			
a) Geschäftsführung	x	x				x	x	x	x Geschäftsführung ist lt. deutschem Entwurf zur NIS-2-Richtlinie persönlich haftend und daher verantwortlich. Alle anderen Möglichkeiten übernehmen Tätigkeiten und führen diese aus Sicht der GF auch aus – also auch b) c) und d)	x	x	x	x	10	77%	9	69%	0	0%
b) IT-Abteilung	x		x		x				x				x	5	38%	5	38%	0	0%
c) Informationssicherheitsbeauftragte (CISO/ISO)	x (in Prüfung)	x	x			x			x			x	x	7	54%	6	46%	0	0%
d) Externer Dienstleister	x		x	x	x				x				x	6	46%	6	46%	0	0%
e) Sonstiges (bitte spezifizieren:)	x aktuell noch a); b) u. d) - in Prüfung zukünftig c										x Aktuell besteht noch keine interne Vorgabe dazu. Dies ist aber in Arbeit.			2	15%	0	0%	0	0%
Frage 3: Welche Governance-Maßnahmen setzen Sie zur Erfüllung der NIS-2-Richtlinie um?																			
a.) Ernennung Sicherheitsverantwortlichen		x	x	x	x	KA			x	x	x	x	x	9	69%	9	69%	1	8%
b.) Entwicklung und Umsetzung IS-Policies			x	x	x	KA			x	x	x	x	x	8	62%	8	62%	1	8%
c.) Etablierung eines Risikomanagement-Systems		x	x	x	x	KA	x		x	x	x	x	x	10	77%	10	77%	1	8%
d.) Sicherstelllung eines Incident Response Plans			x	x	x	KA	x		x	x	x	x	x	9	69%	9	69%	1	8%
e.) Durchführung von Audits		x	x	x	x	KA	x		x	x	x	x	x	10	77%	10	77%	1	8%
f.) Zusammenarbeit und Informationsaustausch		x	x	x	x	KA			x	x	x	x	x	9	69%	9	69%	1	8%
g.) Schutz von Lieferketten		x	x		x	KA			tbc	x	x			6	46%	5	38%	1	8%
h.) Meldesysteme und Notfallpläne	x	x	x	x	x	KA	x		x	x	x	x	x	11	85%	11	85%	1	8%
i.) Cybersicherheitsmonitoring und Frühwarnsysteme	x	x	x	x	x	KA	x		x	x	x	x	x	11	85%	11	85%	1	8%
j.) Schulung und Sensibilisierungsprogramme	x	x	x	x	x	KA	x		x	x	x	x	x	11	85%	11	85%	1	8%
k.) Sonstige (bitte spezifizieren:)			x Werden bereits durch ISO/ IEC 27001:2022 umgesetzt – NISv2UmsuCG erweitert den Scope auf das gesamte Unternehmen)			KA		x Alle Forderungen sind bereits durch die ISO 27001 Zertifizierung abgedeckt. Stellenweise sind Erweiterungen notwendig.						2	15%	0	0%	1	8%
Themenkategorie 2: Organisatorische Maßnahmen																			
Frage 4: Welche organisatorischen Maßnahmen haben Sie zur Sicherstellung der Cybersicherheit gemäß der NIS-2-Richtlinie implementiert?																			
a) Etablierung eines Cybersicherheitsmanagementsystems				x	x		x	x	x Hinweis vorab: Security ist nicht nur Cybersicherheit. Die Umsetzung von NIS-2 in der BR Deutschland wird sich nach der DIN/ISO 27001 orientieren und diese fordert hierzu auch z. B. ganz klassische Zutrittssicherungen. Beides ist etabliert	x	x	x	x	9	69%	8	62%	0	0%
b) Durchführung regelmäßiger Schulungen zur Cybersicherheit	x	x		x	x	x	x	x	x ja – online mit Onlinetest	x	x	x	x	12	92%	11	85%	0	0%
c) Einführung klarer Kommunikationsprozesse im Krisenfall		x		x			x	x	x ja – online mit Onlinetest	x	in Arbeit	x	x	9	69%	7	54%	0	0%
d) Festlegung von Verantwortlichkeiten und Eskalationswegen		x	x	x	x		x	x	x gibt das BSI vor und wird in der BRD diese neben KRITIS auch für NIS-2 vorgeben	x	in Arbeit	x	x	11	85%	9	69%	0	0%
e) Sonstiges (bitte spezifizieren)			x Bindung SOC und SIRT-Dienstleister inkl. 24/7 Überwachung für Sicherheitsereignisse und Sicherheitsvorfälle)					x						2	15%	1	8%	0	0%
Themenkategorie 3: Risikomanagement und Incidentmanagement																			
Frage 5: Haben Sie ein Risikomanagementsystem für Informations- und Cybersicherheit implementiert?																			
a) Ja			x	x		1		x	x das sowieso vorhandene Risikomgmt. wurde um diese Bereiche erweitert			x	x	7	54%	5	38%	0	0%
b) Nein														0	0%	0	0%	0	0%
c) Teilweise	x	x			x		x Teilweise (ISMS; für die KRITIS-Anlagen)			x	x			6	46%	5	38%	0	0%
Frage 6: Welche der folgenden Risikoanalyseverfahren setzen Sie ein?																			
a) Bedrohungsanalyse und Schwachstellenbewertung	x		x zyklisch und anlassbezogen/ für Schwachstellenbewertung Matching CVSS V3.1 und BSI CSW)	x	x	KA	x	x			x	x	x	9	69%	8	62%	1	8%
b) Risikoabschätzungen für IT-Systeme und Prozesse	x	x	x zyklisch und anlassbezogen nach ISO/ IEC 27005 und BSI elementare Gefährdungen)	x	x	KA	x	x	x	x	x	x	x	12	92%	11	85%	1	8%
c) Stresstests und Simulationen von Cyberangriffen	x		x anlassbezogen		x	KA	x	x		x	x	x		8	62%	7	54%	1	8%
d) Sonstige Verfahren			x reduzierte Risikobewertung im Change-Management-Prozeß			KA							x Assetbewertungen, Szenarioansatz	2	15%	0	0%	1	8%
Frage 7: Wie definieren Sie die Risikobewertungskriterien für die Cybersicherheit in Ihrem Unternehmen?																			
a) Basierend auf gesetzlichen Vorgaben (z.B. NIS-2)	x	x	x		x			x			x	x	x	8	62%	8	62%	0	0%
b) Interne Richtlinien und Standards		x	x			x	x	x	x auf Grundlage von Gesetzgebung und Best-Praxis. Unsere Konzernmutter ist ein internationales Unternehmen und es existieren Erfahrungen im Risikomgmt. auch in z. B. Energie- und Waste-Sektor.		x	x	x	9	69%	8	62%	0	0%
c) Externe Beratung durch Sicherheitsdienstleister		x		x							x			3	23%	3	23%	0	0%
d) Sonstige Verfahren			x ISO/ IEC 31000 und ISO/ IEC 27005					x Anforderungen der interessierten Parteien		x gemäß B3S, DWA M-1060				3	23%	0	0%	0	0%
Frage 8: Welche Faktoren berücksichtigen Sie bei der Festlegung der Risikobewertungskriterien? (Mehrfachantworten möglich)																			
a) Bedrohungslandschaft (z.B. Arten von Cyberangriffen)	x	x	x	x		x		x	x		x	x	x	10	77%	10	77%	0	0%
b) Kritikalität der Systeme und Daten	x	x	x	x	x	x	x	x	x		x	x	x	12	92%	12	92%	0	0%
c) Geschäftsauswirkungen (finanziell, rechtlich, reputationsbezogen)	x	x	x (finanziell, rechtlich, reputationsbezogen) – Bezogen auf die Kritische Infrastrukturen, die kritischen Dienstleistungen und kritischen Anlagen (NICHT Finanziell)	x	x		x	x	x		x		x	10	77%	9	69%	0	0%
d) Anforderungen von Drittanbietern/Dienstleistern		x						x	x				x	4	31%	4	31%	0	0%
e) Sonstige								x		x gemäß B3S, DWA M-1060				2	15%	1	8%	0	0%
Frage 9: Welche Methoden zur Risikobeurteilung setzen Sie in Ihrem Unternehmen ein?																			
a) Qualitative Risikobeurteilung (subjektive Einschätzungen)		x	x (subjektive Einschätzungen)			x				x			x	5	38%	4	31%	0	0%
b) Quantitative Risikobeurteilung (numerische Bewertungen)		x	x (numerische Bewertungen)		x								x	4	31%	3	23%	0	0%
c) Kombination aus beidem		x	x (abhängig vom Risikoszenario – i.d.R qualitativ Anmerkung: Quantitativ erfordert umfangreiches statistisches Material – dies liegt oft außerhalb Sektor „Finanzen und Versicherungen" nicht vor und zu Risiken aus neuen/ geänderten Angriffsvektoren liegen i.d.R. keine Daten vor)	x			x	x	x Auswirkung des Schadens und Aufwände zur Wiederherstellung, aber auch nicht monitär bezifferbare Reputationsverluste.		x	x	x	9	69%	7	54%	0	0%
d) Keine formale Methode zur Risikobeurteilung	x													1	8%	1	8%	0	0%
Frage 10: Wie wird die Kritikalität der einzelnen Bedrohungen in Ihrem Unternehmen ermittelt?																			
a) Basierend auf der Eintrittswahrscheinlichkeit	x		x	x	x	x	x	x		x	x	x	x	11	85%	11	85%	0	0%
b) Basierend auf dem potenziellen Schaden für das Unternehmen	x			x	x	x	x	x		x	x		x	9	69%	9	69%	0	0%
c) Durch externe Sicherheitsanalysen			x			x					x			3	23%	3	23%	0	0%

Befragungsantworten Rohdaten

	Stadt 1	Stadt 2	Stadt 3	Stadt 4	Stadt 5	Stadt 6	Stadt 7	Stadt 8	Stadt 9	Stadt 10	Stadt 11	Stadt 12	Stadt 13	Anzahl der Städte (n)	Städte (%)	Anzahl Städte (ohne Zusatzangaben)	Städte (ohne Zusatzangaben) (%)	Keine Angaben	Keine Angaben (%)
d) Andere Methoden			x Detektierbarkeit Anmerkung: Detektierbarkeit und Eintrittswahrscheinlichkeit bilden ein Risikoexpositionslevel das wiederum mit der potenzielle Schadenshöhe das Risikolevel ergibt)						x Eintrittswahrscheinlichkeit * Auswirkung = Schadenshöhe Schadenshöhe entspricht der Kritikalität				x Entdeckbarkeit	3	23%	0	0%	0	0%
Themenkategorie 4: Technische Maßnahmen				x Ich bitte um Verständnis, dass wir grundsätzlich keine detaillierten Angaben zu unseren konkret eingesetzten technischen Lösungen machen.		KA		KA						1	8%	0	0%	2	15%
Frage 11: Welche technischen Cybersicherheitsmaßnahmen haben Sie implementiert, um den Anforderungen der NIS-2-Richtlinie zu entsprechen? (Mehrfachantworten möglich)						KA		KA											
a) Firewall-Systeme und Netzwerksicherheitslösungen	x	x	x (Produkt wird nicht veröffentlicht)			KA	x IDS/IPS	KA		x	x Explizite FW-Regeln, VLAN, NAC, 802.1X)	x	x	8	62%	5	38%	2	15%
b) Endpunkt-Sicherheitslösungen (Antivirus, EDR)	x	x	x EDR in der Produktion und Anti-Virus noch in Office-Domäne			KA	x EDR, Antivirus	KA		x	x Endpoint Protection mit XDR, Automatische Isolation bei High Alerts, SOC/CDC Überwachung, Härtung von Clients und Servern	x	x	8	62%	5	38%	2	15%
c) Datenverschlüsselung und sichere Kommunikation	x	x	x (Produkt wird nicht veröffentlicht)			KA	x TLS 1.3, HTTPS	KA		x	x 802.1X, NoSPamProxy, Dracoon für externen Datenaustausch	x	x	8	62%	5	38%	2	15%
d) Authentifizierungssysteme (z.B. Multi-Faktor-Authentifizierung)	x	x	x IAM und MFA Pro Domäne in Umsetzung			KA	x 2FA für interne und externe	KA		x	x AD, MFA, Passkey	x	x	8	62%	5	38%	2	15%
e) Sonstige			x Dienstleister/ Lieferantenzugang und Zugriffsstandard für Produktionsdomäne		x Als Kritis-Unternehmen veröffentlichen wir keine genauen Details zu unseren Maßnahmen	KA	x alle a-d waren bereits vor NIS2 implementiert	KA	x Wir haben eine harte Trennung der IT- und OT-Struktur realisiert. Kein OT-Client hat eine Kommunikation zum Internet. Die Anbindung geschieht über eine OT-DMZ an das Officenetz (eigener PC). Nur von dort gibt es Internetzugang und Mails. Securtiy ist sowohl im IT, als auch im OT im Einsatz. Zwischen beiden gibt es eine DMZ und unterschiedliche Firewalls (Fortinet und Sophos), auf beiden gibt es unterschiedliche EDR/EPS (Crowstrike, Sophos, Panda) ... Die Aufzählung folgende ist nicht abschließend: Netzwerksegmentierung, redundante Firewall, unterschiedliche Firewalls, SzA (über Konzernmutter), SIEM (im Aufbau über Konzernmutter), EPS, kein Internetaccess für OT, Kommunikation zum IT-Netz über DMZ und nur von dort Zugriff auf Mails und Internet, KEIN (!) freier USB-Bus, sondern SW-Datendrehscheibe zum IT-Client, Jumpserver zum Ausschalten auf die Server, ...					4	31%	0	0%	2	15%
Themenkategorie 5: Physische Maßnahmen																			
Frage 12: Welche physischen Maßnahmen setzen Sie ein, um den Schutz Ihrer IT- und Netzwerksysteme zu gewährleisten? (Mehrfachantworten möglich)																			
a) Zugangskontrollsysteme (z.B. Schlüssel, Karten, biometrische Systeme)	x	x	x Online/ offline Schließung, auf Sicherheitszonen ausgerichtete Schließsystemanforderungen) x keine biometrischen Daten	x		KA	x Transponder, weitere Schlüsselsysteme	KA	x RFID – Zugangssysteme zum Gelände und den Räumen mit OT-Technologie x Ja – Videokameras mit Bewegungserkennung und Aufzeichnung in den Serverräumen,	x	x Chips für Büroräume. Karte und Schlüssel für das RZ	x	x	10	77%	6	46%	2	15%
b) Überwachungskameras und Sicherheitsalarmsysteme	x		x wird nicht veröffentlicht	x		KA	x Überwachung an den kritischen Außenstellen	KA	Ja -Überwachung der Zugangsbereiche zur Anlage mit Videokameras, Bewegungserkennung und Aufzeichnung (vollumfängliche Videoausstattung ist in Planung)	x	x BMA, Alarmanalge	x		8	62%	4	31%	2	15%
c) Sichere Verwahrung von Hardware in Serverräumen	x	x	x wird nicht veröffentlicht	x		KA	x Ausgestattet mit Schliessystemen	KA	x abgeschlossene Serverräume mit Videoüberwachung, Klimaanlage, Umweltmonitoring, ...	x	x Hardware für das RZ wird im Rechenzentrum gelagert. Hardware für Büroräume in einem Stahlschrank.	x	x	10	77%	6	46%	2	15%
d) Backup-Systeme an sicheren Standorten	x	x	x wird nicht veröffentlicht	x		KA		KA	x ja, Backupsystem sind selber außerhalb der ADS, - tägliche Datensicherung auf HDD, - Auslagerung der Wochensicherung auf Band in einem 3ten Gebaude (Wandtresor), - Auslagerung der Monatssicherung in einem anderen Standort und dort im Tresor.	x	x Veeam LinuxRepository RZ1, Veeam Windows Repository RZ2, Cloud Backup für VMs, Tape Backup für VMs, Separates Cloud Backup für M365	x	x	9	69%	6	46%	2	15%
e) Sonstiges			x ganzheitliche Betrachtung aller Anlagen > alle Anlagen der gesamten Firma wurde in 10 Anlagenstufen klassifiziert und per Sicherheitszone die Sicherheitsmaßnahmen nach Schutzziel definiert)		x Als Kritis-Unternehmen veröffentlichen wir keine genauen Details zu unseren Maßnahmen	KA		KA						2	15%	0	0%	2	15%
Frage 13: Wie häufig werden die physischen Sicherheitsmaßnahmen überprüft?				KA		KA		KA						0 (0%)	0x (0%)	3 (23%)			
a) Monatlich		x		KA	KA	KA		KA						1 (8%)	1x (8%)	4 (31%)	1	8%	1
b) Vierteljährlich				KA	KA	KA	x	KA						1 (8%)	1x (8%)	4 (31%)	1	8%	1
c) Jährlich	x		x (und anlassbezogen)	KA	KA	KA		KA		x	durch die Audits von DSB und ISB		x	5 (38%)	3x (23%)	4 (31%)	5	38%	3
d) Keine regelmäßige Überprüfung				KA	KA	KA		KA						0 (0%)	0x (0%)	4 (31%)	0	0%	0
									x Hier eher eine neue Variante als Antwort, die nicht aufgeführt ist: Da es täglich in Verwendung ist, die Kameras auch an unterschiedlichen Standorten als Videobildschirm visualisiert werden, erfolgt eine Überprüfung laufend durch die Anwender*innen. Auch die Serverräume werden von Montag – Freitag täglich von den Admins pro-aktiv begangen und somit wird der Perimeterschutz durch Gebrauch getestet.			x permanent durch die Benutzung		2 (15%)	0x (0%)	0 (0%)	2	15%	0
Themenkategorie 6: NIS-2 und Cybersicherheitsstandards																			
Frage 14:Welche zusätzlichen Informations- und Cybersicherheitsstandards oder -normen setzen Sie neben der NIS-2-Richtlinie um? (Mehrfachantworten möglich)																			
a) ISO/IEC 27001		x	x			x		x	x ISO/IEC 27001 + -2 und daraus basierend IT-SiKat (wir gehören zu einem KRITIS-Pflichtigen Energiedienstleister, der die Strukturen für KRITIS-Zertifizierungen und Basisabsicherung in dem Sektor erfüllt und uns nach diesem „Grund"-Standard mit unterstützt.			x	x	7	54%	6	46%	0	0%
b) NIST Cybersecurity Framework														0	0%	0	0%	0	0%
c) BSI IT-Grundschutz	x	x			x		x				x		x	6	46%	6	46%	0	0%
d) Sonstige			x ISO/ IEC 27019 (umgeschrieben von Sektor Energie auf Sektor Wasser), BSI §8a Abs1. (Stand der Technik) sowie BSIG §8a Abs.1a (Systeme zur Angriffserkennung – separates Reifegradmodell) – risikobasiert: BSI Grundschutzbausteine	x VDS 10000			x B3S WA-Sicherheitskompendium	x ISO 27002, ISO 27019, IT_SiKat	x Grundlagenabsicherung analog zu WiBa	x B3S WA, DWA M-1060		x Teilweise die Iso 27019 zum Schutz spezieller Liegenschaften	x ISO 27001, ISO 27005, ISO 62443 (tw), DIN EN 50600	8	62%	0	0%	0	0%
Frage 15: Für welche Anforderungen der NIS-2-Richtlinie setzen die Informations- und Cybersicherheitsstandards bzw. Teile/Kapitel dieser Standards ein?																			
a.) Einführung von Mindeststandards und Basissicherheitsanforderungen	x		x	x	x		x		x	x	x	x	x	10	77%	10	77%	0	0%
b.) Risikomanagement		x	x	x			x		x	x	x	x	x	9	69%	9	69%	0	0%
c.) Krisenmanagement				x			x		x		x	x	x	6	46%	6	46%	0	0%
d.) Meldepflichten für Sicherheitsvorfälle		x	x		x		x		x		x	x	x	8	62%	8	62%	0	0%
e.) Anforderungen für die Lieferkette		x	x		x		x		x		x	x	x	8	62%	8	62%	0	0%
f.) Kollaboration und Informationsaustausch									x				x	2	15%	2	15%	0	0%
g.) Harmonisierung der NIS2-Richtlinie mit anderen Regelungen (z.B. DSGVO)						x			x		x		x	4	31%	4	31%	0	0%

Befragungsantworten Rohdaten

	Stadt 1	Stadt 2	Stadt 3	Stadt 4	Stadt 5	Stadt 6	Stadt 7	Stadt 8	Stadt 9	Stadt 10	Stadt 11	Stadt 12	Stadt 13	Anzahl der Städte (n)	Städte (%)	Anzahl Städte (ohne Zusatzangaben)	Städte (ohne Zusatzangaben) (%)	Keine Angaben	Keine Angaben (%)
h.) Sonstige (bitte spezifizieren:)								x NIS 2 bedeutet für Betreiber Kritischer Anlagen eine Erweiterung der ISMS-Umsetzung auf der bestehenden Basis der oben genannten Regelwerke			x Personalsicherheit, Sensibilisierung und Awareness, Anlagensicherheit (kritische Räume, Zutrittsregelungen			2	15%	0	0%	0	0%
Themenkategorie 7: Anregungen für zukünftige Leitfäden/Standards zur NIS-2-Richtlinie																			
Frage 16: Welche technischen Herausforderungen haben Sie bei der Implementierung der NIS-2-Richtlinie identifiziert?	kA	kA	x Bestehende Sicherheitsstandard der Produktions-Domäne in die Office-Domäne zu überführen	KA	KA	KA	x Interoperabilität diverser Lösungen	KA	x Die Herstellervorgaben sind oft sehr systemabsichernd und berücksichtigen nicht das rasche und hohe Tempo der IT-Security-Umwelt. Also z. B. keine zeitgemäßen Freigaben der Hersteller (z.B. Siemens) für aktuelle Betriebssysteme und monatliche Securitypatche.	KA	x Aktuell keine nennenswerten Herausforderungen	KA	Festlegung der zu schützenden Anlagen	5	38%	0	0%	8	62%
Frage 17: Welche weiteren Unterstützungsmöglichkeiten oder Ressourcen benötigen Sie, um die Anforderungen der NIS-2-Richtlinie vollständig zu erfüllen?	x Beratung durch externe Experten / Unternehmen Schulungsangebote ggf. Zertifizierungen Technische Unterstützung / Tools	x Derzeit haben wir uns mit der NIS-2 Richtlinie und den daraus resultierenden Best Practices noch nicht intensiv genug auseinander gesetzt.	x Da das firmenspezifische Maß an Cybersicherheit definiert werden muss und damit auch das Schutzniveau, welches erreicht werden soll/ muss, sind qualifizierte Ressourcen notwendig.	x	KA	KA	KA	KA	x Bei uns unterstützt die Konzernmutter mit Checklisten, Templates und Systemen, da von dort bereits Konzernbestandteile mit KRITIS-Zertifizierungspflicht betreut werden.	x Umsetzung in nationales Recht, damit die konkreten Anforderungen verbindlich benannt sind	x Mehr Zeit und mehr Personal	KA	KA	7	54%	1	8%	6	46%
Frage 18: Was sind aus Ihrer Sicht die wichtigsten Best Practices, die bei der Umsetzung der NIS-2-Richtlinie berücksichtigt werden sollten?	x Klar definierte Governance-Strukturen Ganzheitliches Risikomanagement Technische Sicherheitsmaßnahmen Schulung und Sensibilisierung der Mitarbeiter Notfall und Wiederherstellungspläne Zusammenarbeit und Informationsaustausch	x Derzeit haben wir uns mit der NIS-2 Richtlinie und den daraus resultierenden Best Practices noch nicht intensiv genug auseinander gesetzt.	x Priorisierung der Umstellung von Defense in Depth auf Zero-Trust Leitlinien und Architektur in der Office- und Produktionsdomäne. ISO/ IEC 27002:2022 und BSI Grundschutzbausteine (NICHT Kompendium) ISO/ IEC 27019 Sektor Energie > für weitere Sektoren umschreiben und keine B3S erstellen) ISO/ IEC 27017 und ISO/ IEC 27033 ISO/ IEC 27005:2022	x Wir empfehlen unterstützendes Know-how und Ressourcen in Form eines spezialisierten externen Partners/Dienstleisters.	x Die Umsetzung der ISO27001 oder des BSI Grundschutzkompendium bilden eine solide Grundlage.	KA	KA	KA	x Es gibt viele „einfache" Standards und Empfehlungen, wie IT-Systeme abgesichert werden können. Gleich mit dem BSI-Grundschutz oder der DIN/ISO 27001 zu beginnen, betrachten wir als „erschlagend" und nicht praxisnah. Begonnen werden könnte bei einzelnen Baustellen, wo auch vom BSI einzelne x Empfehlungen vorgegeben werden. Dann erweiternd um die BSI-Gruppenrichtlinienempfehlungen und die BSI-WiBa: Wege in die Basisabsicherung. Wenn diese Schritte gegangen werden, dann ist eine vernünftige Grundstruktur und auch das Verständnis / Akzeptanz vorhanden, die NIS-2 Anforderungen in der Größenordnung einer 27001 zu betrachten.	KA	x BSI IT-Grundschutz /ISO27001 Praktiken und Empfehlungen Austausch mit externen Dienstleistern und anderen Parteien zu der Umsetzung einzelner Maßnahmen	x Umsetzungswillen der Geschäftsführung	KA	8	62%	0	0%	5	38%

ABKÜRZUNGSVERZEICHNIS

ADA	Angriffserkennungssysteme
API	Application Programming Interface
APP	Applikationen bzw. Anwendungen
B3S	Branchenspezifischer Sicherheitsstandard
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BIM	Building Information Modeling
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CAF	Cyber Assessment Framework
CELEX	Communautaire Elektronique Lex (EU-Dokumentenkennzeichen)
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSMS	Cyber-Sicherheitsmanagementsystem
CVSS	Common Vulnerability Scoring System
DIN	Deutsches Institut für Normung
DMZ	Demilitarisierte Zone
DVGW	Deutscher Verein des Gas- und Wasserfaches
DWA	Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
EPS	Endpoint Protection System
EU	Europäische Union
FMEA	Failure Mode and Effects Analysis
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnologie
IND	Industrielle IT
IP	Internet Protocol
IS-Policies	Informationssicherheitspolicies
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
IT-SiG	IT-Sicherheitsgesetz
JTC	Joint Technical Committee
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastrukturen

LAN	Local Area Network
NAC	Network Access Control
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
NIS-2	Network and Information Security Directive 2
NISG	Netz- und Informationssystemsicherheitsgesetz
NIST	National Institute of Standards and Technology
OGC	Open Geospatial Consortium
OT	Operational Technology
OT-DMZ	OT-Demilitarisierte Zone
ÖWAV	Österreichischer Wasser- und Abfallwirtschaftsverband
PASSKEY	Passwortlose Authentifizierung
SCADA	Supervisory Control and Data Acquisition
SCW	Sicherheitskonzept Wasserwirtschaft
SIEM	Security Information and Event Management
SOC	Security Operations Center
SzA	Sicherheitszentrale/Analyse
TLS	Transport Layer Security
TLS 1.3	Transport Layer Security Version 1.3
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen
USB	Universal Serial Bus
VDE	Verband der Elektrotechnik Elektronik Informationstechnik
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VdS	Verband der Schadenversicherer
WA	Wasser/Abwasser
WiBA	Wirtschaftliche Basisabsicherung

ABBILDUNGSVERZEICHNIS

Abbildung 1: Strukturelle Organisation der Cybersicherheit 20
Abbildung 2: Für Cybersicherheit verantwortliche Führungsebenen 21
Abbildung 3: Governance-Maßnahmen zur Umsetzung der NIS-2-Anforderungen 22
Abbildung 4: Organisatorische Maßnahmen zur Sicherstellung der Cybersicherheit 24
Abbildung 5: Implementierung eines Risikomanagementsystems 25
Abbildung 6: Eingesetzte Risikoanalyseverfahren 26
Abbildung 7: Risikobewertungskriterien für Cybersicherheitsrisiken 28
Abbildung 8: Faktoren bei der Festlegung der Risikobewertungskriterien 29
Abbildung 9: Methoden zur Risikobeurteilung 30
Abbildung 10: Kritikalitätsermittlungsverfahren 31
Abbildung 11: Technische Cybersicherheitsmaßnahmen zur Umsetzung der NIS-2-Richtlinie 33
Abbildung 12: Physische Maßnahmen zum Schutz der IT und der Netzwerksysteme 35
Abbildung 13: Häufigkeiten der Überprüfungen der physischen Sicherheitsmaßnahmen 36
Abbildung 14: Zusätzlich angewandte Cybersicherheitsstandards und Normen 37
Abbildung 15: NIS-2-Anforderungen für welche Standards eingesetzt werden 39

TABELLENVERZEICHNIS

Tabelle 1: Sonstige eingesetzte Risikoanalysepraktiken 27
Tabelle 2: Sonstige eingesetzte Risikobewertungsverfahren 28
Tabelle 3: Sonstige Faktoren für die Festlegung der Risikobewertungskriterien 30
Tabelle 4: Sonstige eingesetzte Methoden zur Risikobeurteilung 31
Tabelle 5: Weitere Methoden zur Ermittlung der Kritikalität 32
Tabelle 6: Sonstige technische Maßnahmen zur Umsetzung der NIS-2-Richtlinie 34
Tabelle 7: Sonstige eingesetzte Cybersicherheitsstandards und Normen 38
Tabelle 8: Technische Herausforderungen während der NIS-2-Umsetzung 40
Tabelle 9: Benötigte Unterstützungsmöglichkeiten bzw. Ressourcen zur Umsetzung der NIS-2-Anforderungen 42
Tabelle 10: Good Practices zur NIS-2-Umsetzung 43

LITERATURVERZEICHNIS

Bücher

Atteslander, P. (2010). *Methoden der empirischen Sozialforschung* (12. Aufl.). Erich Schmidt Verlag.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research* (3rd ed.). Sage Publications.

Flick, U. (2019). *Qualitative Sozialforschung: Eine Einführung* (8. Aufl.). Rowohlt Taschenbuch Verlag.

Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12. Aufl.). Beltz.

Bossong, R., & Wagner, B. (2019). *A Typology of Cybersecurity and Public–Private Partnerships in the Context of the EU*. *European Foreign Affairs Review, 24*(3), 395–414.

ENISA. (2023). *NIS Investments 2023: A comparative study of cybersecurity budgets across sectors and Member States*. https://www.enisa.europa.eu/publications/nis-investments-2023

Müller, R., Disterer, G., & Wundram, M. (2021). *Informationssicherheit in kritischen Infrastrukturen – Anforderungen und Umsetzung im Kontext der NIS-2-Richtlinie*. *Zeitschrift für IT-Sicherheit, 8*(2), 95–102.

Pflüger, F., & Pohlmann, N. (2020). *Cybersicherheit in Kritischen Infrastrukturen: Herausforderungen und Lösungsansätze am Beispiel der Wasserwirtschaft.* Datenschutz und Datensicherheit – DuD, 44(5), 299–304.

Tikk, E., & Kerttunen, M. (2021). *Comparative Cybersecurity Regimes in the European Union*. Journal of Cyber Policy, 6(2), 189–211.

ENISA. (2023). *NIS Investments 2023: A comparative study of cybersecurity budgets across sectors and Member States*. https://www.enisa.europa.eu/publications/nis-investments-2023

Bossong, R., & Wagner, B. (2019). *A Typology of Cybersecurity and Public–Private Partnerships in the Context of the EU*. European Foreign Affairs Review, 24(3), 395–414.

Pflüger, F., & Pohlmann, N. (2020). *Cybersicherheit in Kritischen Infrastrukturen: Herausforderungen und Lösungsansätze am Beispiel der Wasserwirtschaft*. Datenschutz und Datensicherheit – DuD, 44(5), 299–304.

Bossong, R., & Wagner, B. (2019). *A Typology of Cybersecurity and Public–Private Partnerships in the Context of the EU.* European Foreign Affairs Review, 24(3), 395–414.

Tikk, E., & Kerttunen, M. (2021). *Comparative Cybersecurity Regimes in the European Union*. Journal of Cyber Policy, 6(2), 189–211.

BDEW – Bundesverband der Energie- und Wasserwirtschaft. (2023). *Cyber-Sicherheit in der Wasserwirtschaft – Herausforderungen und Handlungsempfehlungen*. https://www.bdew.de

Bendiek, A., & Metzger, T. (2021). *Kritische Infrastrukturen und Cybersicherheit in Deutschland*. Stiftung Wissenschaft und Politik. https://www.swp-berlin.org

Bortz, J., & Döring, N. (2006). *Forschungsmethoden und Evaluation (4. Aufl.)*. Springer.

Diekmann, A. (2017). *Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen (21. Aufl.)*. Rowohlt.

Porst, R. (2014). *Fragebogen: Ein Arbeitsbuch (4. Aufl.)*. Springer VS.

Schnell, R., Hill, P. B., & Esser, E. (2013). *Methoden der empirischen Sozialforschung (9. Aufl.)*. Oldenbourg Wissenschaftsverlag.

Journale

Pointl, M., Winkelbauer, A., Krampe, J., & Fuchs-Hanusch, D. (2019). *Aspekte der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft. Österreichische Wasser- und Abfallwirtschaft,* 71(6), 374–384. https://doi.org/10.1007/s00506-019-0584-y

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.* Electronics, 12(6), 1333. MDPI AG. Abgerufen am 28.10.2023 von http://dx.doi.org/10.3390/electronics12061333

Gesetze und Verordnungen

Europäische Union. (2022). *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*. Amtsblatt der Europäischen Union, **L 333**, 80–152. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555