FERDINAND PORSCHE
FERNFH

# Netz- und Informationssystemsicherheitsgesetz: Herausforderungen und Chancen für Betreiber wesentlicher Dienste

## Bachelorarbeit

eingereicht von: **Christian Hauer**
Matrikelnummer: 09225689

im Fachhochschul-Bachelorstudiengang Wirtschaftsinformatik (0470)
der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades <einer/eines>

**Bachelor of Arts in Business**

Betreuung und Beurteilung: Dieter Brennsteiner, BA

Wiener Neustadt, 03. Juni 2025

# Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Bachelorarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

Korneuburg, 03.06.2025

Unterschrift

| SIGNATURINFORMATIONEN | | |
|---|---|---|
| | **Unterzeichner** | Christian Karl Hauer |
| | **Datum/Zeit-UTC** | 2025-06-03T14:46:37+0200 |
| | **Prüfinformation** | Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at |
| **Hinweis** | Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument. | |



Die Kapitel 2 bis 2.5.4 der vorliegenden Bachelorarbeit wurden im Rahmen der Lehrveranstaltung „Bachelor Seminar 1“ eingereicht und am 14.05.2025 als Bachelorarbeit 1 angenommen.

**Kurzzusammenfassung:** Netz- und Informationssystemsicherheitsgesetz: Herausforderungen und Chancen für Betreiber wesentlicher Dienste

Die vorliegende Bachelorarbeit untersucht die Herausforderungen und Chancen des Netz- und Informationssystemsicherheitsgesetzes (NIS-G) für Betreiber wesentlicher Dienste in Österreich. Im Mittelpunkt steht die Frage, welche fünf Sicherheitsmaßnahmen gemäß der Norm EN ISO/IEC 27001 in der Praxis bevorzugt zur Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) herangezogen werden.

Zur Beantwortung dieser Frage wurde eine qualitative Forschungsmethodik gewählt. Halbstrukturierte Interviews mit Cybersicherheitsverantwortlichen aus verschiedenen kritischen Sektoren lieferten praxisnahe Einblicke. Die erhobenen Daten wurden mittels Inhaltsanalyse nach Mayring systematisch ausgewertet.

Die Ergebnisse zeigen, dass kryptographische Maßnahmen als besonders prioritär angesehen werden. Gleichzeitig wurde deutlich, dass wirtschaftliche, organisatorische und regulatorische Rahmenbedingungen die Umsetzung maßgeblich beeinflussen. Die Arbeit trägt zum besseren Verständnis der praktischen Anwendung internationaler Sicherheitsstandards bei und bietet praxisorientierte Empfehlungen zur Priorisierung von Maßnahmen. Damit unterstützt sie Betreiber wesentlicher Dienste bei der nachhaltigen Erhöhung ihrer Cyberresilienz angesichts wachsender digitaler Bedrohungen.

**Schlagwörter:**

Netz- und Informationssystemsicherheitsgesetz (NIS-G), Betreiber wesentlicher Dienste, Informationssicherheitsmanagementsystem (ISMS), ISO/IEC 27001, Inhaltsanalyse nach Mayring, NIS2-Richtlinie

**Abstract:** Network and Information Systems Security Act: Challenges and Opportunities for Operators of Essential Services

This bachelor thesis examines the challenges and opportunities arising from the Network and Information Systems Security Act (NIS-G) for operators of essential services in Austria. The study focuses on identifying the five most important security measures implemented in accordance with the EN ISO/IEC 27001 standard to establish an effective Information Security Management System (ISMS).

Qualitative research approach was applied, using semi-structured expert interviews with cybersecurity professionals from critical infrastructure sectors. The data were evaluated through a structured content analysis following Mayring's methodology. Findings indicate that cryptographic controls are the most prioritized measures.

However, their implementation is significantly influenced by economic constraints, organizational structures, and regulatory uncertainty.

Thesis provides practical insights into how international standards are applied under national regulatory frameworks and offers recommendations to support operators in enhancing their cyber resilience and aligning with evolving legal and threat landscapes.

**Keywords:**

Network and Information Systems Security (NIS), ISO/IEC 27001, Critical Infrastructure Protection, Information Security Management Systems (ISMS)

# Inhaltsverzeichnis


**1. EINLEITUNG 7**

**1.1 Problemstellung und Forschungsfrage 7**

**1.2 Ziele der Arbeit 8**

**1.3 Aufbau der Arbeit 8**

**2. THEORETISCHE GRUNDLAGEN 10**

**2.1 Einführung in die Netz- und Informationssicherheit 10**

**2.2 Definition und Bedeutung wesentlicher Dienste 11**

2.2.1 Cyberbedrohungen und Sicherheitsanforderungen 13

2.2.2 Regulatorische Anforderungen und Compliance 13

2.2.3 Herausforderungen und Zukunftsperspektiven 14

**2.3 Aktueller Forschungsstand und bisherige Arbeiten 15**

2.3.1 Regulatorische Rahmenbedingungen und ISMS 15

2.3.2 Priorisierung von Sicherheitsmaßnahmen 16

2.3.3 Abgrenzung zur bestehenden Forschung 16

2.3.4 Technologische Herausforderungen und neue Bedrohungen 17

2.3.5 Menschliche Faktoren in der Informationssicherheit 18

2.3.6 Erfahrungen aus Cyberangriffen und wirtschaftliche Auswirkungen 18

2.3.7 Zusammenarbeit und Informationsaustausch 18

**2.4 Gesetzliche Rahmenbedingungen: Das Netz- und Informationssystemsicherheitsgesetz (NIS-G) 18**

2.4.1 Historische Entwicklung und Hintergründe 18

2.4.2 Wesentliche Inhalte und Anforderungen des NIS-G 19

2.4.3 Vergleich mit internationalen Standards (z.B. NIST, ISO/IEC 27001) 20

**2.5 ISO/IEC 27001 – Aufbau und Inhalte der Norm 21**

2.5.1 Zielsetzung der Norm 21

2.5.2 Aufbau und Struktur der ISO/IEC 27001 22

2.5.3 Anhang A – Sicherheitsmaßnahmen (Controls) 23

2.5.4 Zertifizierung 26

**3. METHODIK 29**

**3.1 Forschungsmethode: Qualitative Befragung 29**
**3.2 Auswahl der Befragungsteilnehmer (Kriterium: Betreiber wesentlicher Dienste) 30**
**3.3 Struktur des Interviewleitfadens 31**
3.3.1 Interviewleitfaden 32
**3.4 Durchführung und Dokumentation der Befragungen 35**
**3.5 Inhaltsanalyse nach Mayring 35**

**4. HERAUSFORDERUNGEN UND CHANCEN DURCH DAS NIS-G 37**
**4.1 Identifikation der größten Herausforderungen 37**
**4.2 Erfahrungsberichte der Betreiber (Ergebnisse der Befragungen) 38**
4.2.1 A.10 Kryptographie 41
4.2.2 A.11 Physische und umgebungsbezogene Sicherheit 41
4.2.3 A.5 Informationssicherheitsrichtlinien 41
4.2.4 A.12 Betriebssicherheit 42

**5. DISKUSSION 43**
**5.1 Synthese der Erfahrungen und Ergebnisse 43**
5.1.1 Ziel der Analyse 43
5.1.2 Bewertung der Sicherheitsmaßnahmen im Einzelnen 43
5.1.3 Einflussfaktoren auf die Umsetzung 44
5.1.4 Gesamteinschätzung 45

**6. FAZIT UND AUSBLICK 46**
**6.1 Zusammenfassung der zentralen Erkenntnisse 46**
**6.2 Beantwortung der Forschungsfrage 46**
**6.3 Ausblick auf zukünftige Entwicklungen in der Netz- und Informationssicherheit 48**

**LITERATURVERZEICHNIS 49**

# 1. Einleitung

## 1.1 Problemstellung und Forschungsfrage

Die Digitalisierung und Vernetzung kritischer Infrastrukturen erhöhen die Bedeutung der Informationssicherheit, machen Betreiber wesentlicher Dienste aber auch anfälliger für Cyberangriffe. Diese Bedrohungen können nicht nur wirtschaftliche Schäden verursachen, sondern auch ganze Sektoren destabilisieren.

Als Reaktion darauf wurde in der EU die NIS-Richtlinie eingeführt, die in Österreich durch das Netz- und Informationssystemsicherheitsgesetz (NIS-G) umgesetzt wurde. Betreiber wesentlicher Dienste sind verpflichtet, Sicherheitsmaßnahmen zu ergreifen und ein Informationssicherheitsmanagementsystem (ISMS) nach internationalen Normen wie EN ISO/IEC 27001 zu implementieren.

Die Herausforderung liegt in der wirtschaftlich sinnvollen Umsetzung dieser Sicherheitsmaßnahmen. Besonders kleinere Unternehmen oder Organisationen mit begrenzten IT-Budgets müssen priorisieren, um mit begrenzten Ressourcen die größtmögliche Nutzen (Kersten & Schröder, 2023, S. 81-83) zu gewährleisten.

**Hypothese:** Die fünf wichtigsten Sicherheitsmaßnahmen unter Berücksichtigung der Norm EN ISO/IEC 27001) welche vorzugsweise bei Betreiber wesentlicher Dienste zur Anwendung kommen sind:

1. Kryptographische Maßnahmen
2. Handhabung technischer Schwachstellen
3. Datensicherung
4. Schutz vor Schadsoftware
5. Steuerung von Software im Betrieb

Die Hypothese wird durch qualitative Interviews mit cybersicherheitsrelevanten Mitarbeitern von Betreibern wesentlicher Dienste überprüft. Ziel ist es, wirkungsvolle Sicherheitsmaßnahmen sowie Herausforderungen bei deren Implementierung zu identifizieren. Zudem wird untersucht, wie wirtschaftliche, regulatorische und betriebliche Faktoren die Entscheidungsfindung beeinflussen.

**Forschungsfrage:** Was sind die fünf wichtigsten Sicherheitsmaßnahmen, welche bei Betreibern wesentlicher Dienste zur Umsetzung eines Informationssicherheits-managementsystems (ISMS) unter der Berücksichtigung der Norm EN ISO/IEC 27001 vorzugsweise zur Anwendung kommen?

Ein zentrales Problem ist die Dynamik von Cyberbedrohungen, wodurch Sicherheitsmaßnahmen kontinuierlich angepasst werden müssen. Die Arbeit soll Unternehmen dabei unterstützen, fundierte Entscheidungen zur Sicherheitsstrategie zu treffen und Best Practices für die Implementierung eines ISMS abzuleiten.

Neben akademischen Erkenntnissen liefert die Untersuchung praxisrelevante Einblicke für Unternehmen, insbesondere zur Priorisierung von Maßnahmen und möglichen branchenspezifischen Unterschieden in der Umsetzung des NIS-G.

## 1.2 Ziele der Arbeit

Das Hauptziel dieser Arbeit ist die Identifizierung und Analyse der fünf wichtigsten Sicherheitsmaßnahmen, die Betreiber wesentlicher Dienste bei der Implementierung eines Informationssicherheits-Managementsystems (ISMS) gemäß der Norm EN ISO/IEC 27001 priorisieren sollten. Diese Maßnahmen sollen nicht nur die regulatorischen Anforderungen des Netz- und Informationssystemsicherheitsgesetzes (NIS-G) erfüllen, sondern auch dazu beitragen, Cybersicherheitsrisiken zu minimieren, die Resilienz im Unternehmen zu stärken und das Vertrauen in kritische Infrastrukturen zu erhöhen (Kersten & Schröder, 2023, S. 91-93).

Ein zentrales Anliegen der Arbeit ist die Bereitstellung eines evidenzbasierten Rahmens, der Unternehmen dabei unterstützt, die Herausforderungen bei der Implementierung eines ISMS zu bewältigen. Insbesondere wird untersucht, wie verschiedene Sektoren (z.B. Energie, Gesundheitswesen, Transport) Sicherheitsmaßnahmen umsetzen und priorisieren. Dabei werden Gemeinsamkeiten und Unterschiede in der Anwendung der Norm EN ISO/IEC 27001 analysiert.

Ein weiteres Ziel ist es, die Lücke zwischen theoretischen Anforderungen und der praktischen Umsetzung zu schließen. Durch qualitative Interviews mit relevanten Entscheidungsträgern werden reale Entscheidungsprozesse und Herausforderungen erfasst, die sich auf die Auswahl und Umsetzung von Sicherheitsmaßnahmen auswirken. Die gewonnenen Erkenntnisse fließen in praxisorientierte Empfehlungen ein, die Unternehmen dabei helfen, strategische Sicherheitsentscheidungen zu treffen und ihre Ressourcen effizient einzusetzen.

Schließlich trägt diese Arbeit zum akademischen Diskurs über Informationssicherheit bei, indem sie ein tieferes Verständnis für die Anwendung der EN ISO/IEC 27001 im Kontext der NIS-G vermittelt. Die Ergebnisse bieten eine Grundlage für zukünftige Forschung und können als Vergleichsrahmen für Sicherheitspraktiken in unterschiedlichen regulatorischen Umgebungen dienen (Brenner et al., 2024, S. 132-134). Dieser Beitrag ist insbesondere angesichts der zunehmenden Vernetzung kritischer Infrastrukturen und der Notwendigkeit harmonisierter Sicherheitspraktiken zur Bewältigung globaler Herausforderungen der Cybersicherheit von Bedeutung.

## 1.3 Aufbau der Arbeit

Die Arbeit ist in theoretische und empirische Abschnitte unterteilt und verfolgt eine systematische Struktur, um die Forschungsziele zu erreichen. Sie beginnt mit einer

Einleitung, die den Kontext, die Problemstellung, die Forschungsfrage und die Ziele der Arbeit darlegt.

Das zweite Kapitel, **Theoretische Grundlagen**, bietet eine Einführung in die Netzwerk- und Informationssicherheit, erläutert die Bedeutung wesentlicher Dienste und stellt den aktuellen Forschungsstand dar. Ein zentraler Bestandteil ist die Analyse des Netz- und Informationssystemsicherheitsgesetzes (NIS-G), einschließlich seiner Entwicklung, Anforderungen und seiner Verbindung zur EN ISO/IEC 27001.

Im dritten Kapitel, **Methodik**, wird das Forschungsdesign beschrieben. Die qualitative Untersuchung erfolgt durch Interviews mit IT- und Finanzmanagern wesentlicher Dienste. Das Kapitel erläutert die Auswahlkriterien für die Teilnehmer, den Interviewleitfaden und die methodische Inhaltsanalyse nach Mayring zur strukturierten Auswertung der Daten.

Ein Literaturverzeichnis führt alle zitierten Quellen auf. Diese Struktur stellt sicher, dass die Arbeit eine logische und kohärente Analyse bietet – von der theoretischen Fundierung über die empirische Untersuchung bis hin zu praktischen Schlussfolgerungen.

# 2. Theoretische Grundlagen

## 2.1 Einführung in die Netz- und Informationssicherheit

Die zunehmende Digitalisierung und Vernetzung kritischer Infrastrukturen hat die Netzwerk- und Informationssicherheit zu einem essenziellen Bestandteil der betrieblichen Resilienz gemacht. Digitale Systeme sind in nahezu allen wesentlichen Diensten – darunter Energieversorgung, Gesundheitswesen, Transport und Finanzwesen – tief verwurzelt. Damit einher geht eine steigende Bedrohung durch Cyberangriffe, die nicht nur wirtschaftliche Schäden verursachen, sondern auch gesellschaftliche Stabilität und nationale Sicherheit gefährden können (Schryen, 2013, S. 33-35). Die Herausforderung für Betreiber wesentlicher Dienste besteht darin, robuste Sicherheitsmaßnahmen zu implementieren, um ihre Systeme vor Angriffen zu schützen und gleichzeitig den regulatorischen Anforderungen gerecht zu werden.

Die Kernziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen. Diese Grundsätze bilden die Basis für internationale Sicherheitsstandards wie die EN ISO/IEC 27001, die eine systematische Implementierung von Sicherheitsmaßnahmen in Form eines Informationssicherheits-Managementsystems (ISMS) vorschreibt. Für Finanzdienstleistungen wird ebenfalls der Schwerpunkt noch auf die Authentizität der Transaktionen gelegt. In der Praxis bedeutet dies, dass Betreiber wesentlicher Dienste eine Vielzahl an Sicherheitsmaßnahmen priorisieren und umsetzen müssen, um Risiken zu minimieren und gleichzeitig betriebliche Effizienz und Wirtschaftlichkeit zu gewährleisten.

Die Bedrohungen für digitale Infrastrukturen sind vielfältig und entwickeln sich ständig weiter. Cyberkriminelle, staatlich unterstützte Akteure und Hackergruppen nutzen Schwachstellen gezielt aus, um Daten zu stehlen, Systeme zu sabotieren oder Lösegelder zu erpressen (Fischer, 2015, S. 46-48). Besonders Ransomware-Angriffe, Advanced Persistent Threats (APTs) und DDoS-Angriffe haben in den letzten Jahren stark zugenommen und stellen eine ernsthafte Gefahr für Betreiber wesentlicher Dienste dar.

Ein weiteres Problem ergibt sich durch die zunehmende Vernetzung von IoT-Geräten (Internet of Things) in kritischen Infrastrukturen. Diese Geräte, die oft unzureichend gesichert sind, erhöhen die Angriffsfläche erheblich und erfordern neue Sicherheitskonzepte wie Netzwerksegmentierung, starke Authentifizierung und regelmäßige Firmware-Updates (Pohlmann, 2014, S. 79-81). Darüber hinaus erfordert die fortschreitende Entwicklung von Quantencomputern eine Neuausrichtung kryptografischer Verfahren, um langfristige Sicherheit zu gewährleisten (Schneider, 2017, S. 42-44).

Um der steigenden Bedrohungslage entgegenzuwirken, wurden sowohl auf europäischer als auch auf nationaler Ebene regulatorische Rahmenwerke entwickelt. In Österreich bildet das Netz- und Informationssystemsicherheitsgesetz (NIS-G) die gesetzliche Grundlage für die Sicherstellung der Cybersicherheit in kritischen Sektoren. Es verpflichtet Betreiber wesentlicher Dienste zur Implementierung eines ISMS und orientiert sich dabei an der NIS-Richtlinie der EU. Diese Vorgaben sind eng mit internationalen Sicherheitsstandards wie der EN ISO/IEC 27001 verknüpft, die als Best-Practice-Framework zur Risikominderung dienen.

Ein weiteres bedeutendes Regelwerk ist der Digital Operational Resilience Act (DORA) (Verordnung (EU) 2022/2554), der speziell für den Finanzsektor entwickelt wurde. Während das NIS-G auf eine breite Gruppe kritischer Infrastrukturen abzielt, fokussiert sich DORA auf die operationelle Resilienz von Finanzinstituten. Banken, Versicherungen und andere Finanzdienstleister sind durch DORA verpflichtet, umfassende Maßnahmen zur Cybersicherheit und zur Bewältigung operationeller Risiken zu ergreifen. Ein zentraler Bestandteil von DORA ist die Authentizitätssicherung von Finanztransaktionen, was zusätzliche Anforderungen an kryptografische Verfahren und digitale Identitätskontrollen stellt. Die parallelen Entwicklungen von NIS-G und DORA zeigen, dass Cybersicherheit nicht mehr nur eine rein technische Herausforderung ist, sondern zunehmend eine regulatorische und wirtschaftliche Dimension erhält.

## 2.2 Definition und Bedeutung wesentlicher Dienste

Wesentliche Dienste sind ein integraler Bestandteil der modernen Gesellschaft, da sie das Funktionieren kritischer Infrastrukturen gewährleisten und somit zur öffentlichen Ordnung, Sicherheit und wirtschaftlichen Stabilität beitragen. Sie sind in der NIS-Richtlinie der Europäischen Union definiert und in nationalen Gesetzen wie dem österreichischen Netz- und Informationssystemsicherheitsgesetz (NIS-G) verankert. Ein Betreiber wesentlicher Dienste im Sinne des NISG gilt als solcher, wenn er einen Dienst erbringt, der für das Funktionieren grundlegender gesellschaftlicher oder wirtschaftlicher Prozesse von zentraler Bedeutung ist. Der Ausfall oder die Störung dieses Dienstes würde erhebliche Auswirkungen auf das öffentliche Leben, die Versorgungssicherheit oder das wirtschaftliche Gefüge haben.

Voraussetzung ist außerdem, dass der betreffende Dienst in hohem Maß von Netzwerk- und Informationssystemen abhängig ist – also nur durch funktionierende IT-Infrastrukturen zuverlässig bereitgestellt werden kann. Eine Störung dieser Systeme muss gravierende Folgen für die Erbringung des Dienstes haben, etwa durch große Reichweite, lange Ausfallzeiten oder hohe Anzahl betroffener Personen. Ob diese Kriterien erfüllt sind, wird durch eine behördliche Bewertung festgestellt und mit einem Bescheid formell bestätigt.

Das NIS-G (Netz- und Informationssystemsicherheitsgesetz § 2, 2018) sieht Unternehmen als Betreiber wesentlicher Dienste aus den Bereichen:

- Energie,
- Verkehr,
- Bankwesen,
- Finanzmarktinfrastrukturen,
- Gesundheitswesen,
- Trinkwasserversorgung und
- Digitale Infrastruktur
- Anbietern digitaler Dienste
- Einrichtungen der öffentlichen Verwaltung

vor.

Die im NIS-G § 2 genannten Bereiche umfassen eine Vielzahl kritischer Sektoren, die für das Funktionieren der Gesellschaft und Wirtschaft von zentraler Bedeutung sind. Eine systematische Gruppierung der Sektoren in übergeordnete Kategorien, wie sie in der vorliegenden Arbeit vorgenommen wurde, dient der besseren Strukturierung und Fokussierung der Analyse. Dabei werden die Sektoren nach funktionalen und risikobezogenen Gemeinsamkeiten gebündelt.

1. **Energieversorgung** (z. B. Strom- und Gasnetze) bildet eine zentrale Säule kritischer Infrastrukturen, da sie die Grundlage für nahezu alle anderen Sektoren darstellt. Ein Ausfall hätte unmittelbare Auswirkungen auf die Versorgungssicherheit in weiteren Bereichen wie Gesundheitswesen, Transport oder digitale Infrastruktur.
2. **Gesundheitswesen** (z. B. Krankenhäuser, medizinische Notfalldienste) ist essenziell für die Aufrechterhaltung der öffentlichen Gesundheit und Sicherheit. Dieser Sektor zeichnet sich durch hohe Anforderungen an Verfügbarkeit und Datenschutz sensibler Informationen aus.
3. **Transport** (z. B. Schienen-, Straßen- und Luftverkehr) stellt die physische Mobilität sicher und ist für den Warenverkehr und die Versorgungsketten unverzichtbar. In diesem Sektor ist insbesondere die Echtzeit-kommunikation und Steuerung sicherheitskritischer Systeme von großer Bedeutung.
4. **Finanzdienstleistungen** (z. B. Banken, Zahlungsinfrastrukturen) gewähr-leisten die Stabilität des Zahlungsverkehrs und der Kapitalmärkte. Hier ist vor allem die Integrität und Verfügbarkeit von Daten entscheidend, um Vertrauen in wirtschaftliche Transaktionen zu sichern.

Diese Gruppierung orientiert sich also an den funktionalen Gemeinsamkeiten, der Systemrelevanz sowie an den sicherheitsrelevanten Anforderungen der jeweiligen Dienste. Sie erleichtert es, branchenspezifische Risiken und Sicherheitsbedarfe differenziert zu analysieren und geeignete Maßnahmen gezielt zu identifizieren. Darüber

hinaus wird so eine praxisnahe Ableitung von Maßnahmen ermöglicht, die sich an der tatsächlichen Bedrohungslage und Kritikalität der einzelnen Sektoren orientiert.

Um als systemrelevant zu gelten, müssen Betreiber bestimmte Kriterien erfüllen, darunter der Umfang ihrer Tätigkeit, die Abhängigkeit anderer Sektoren und die möglichen Folgen von Ausfällen. Beispielsweise spielt die Energieversorgung eine zentrale Rolle für die gesamte Wirtschaft (Hämmerli, 2015, S. 77-79), während das Gesundheitswesen besonders hohe Sicherheitsanforderungen hat, da Störungen der medizinischen Versorgung unmittelbare Auswirkungen auf das Leben der Menschen haben.

### 2.2.1 Cyberbedrohungen und Sicherheitsanforderungen

Da wesentliche Dienste stark auf digitale Netzwerke und vernetzte Systeme angewiesen sind, sind sie besonders anfällig für Cyberangriffe. Bedrohungen wie Datenlecks, Ransomware oder Denial-of-Service-Angriffe (DDoS) können kritische Prozesse massiv beeinträchtigen. Insbesondere der Einsatz von IoT-Technologien vergrößert die Angriffsfläche, etwa in intelligenten Stromnetzen, die auf Echtzeit-Datenaustausch angewiesen sind. Störungen in diesen Bereichen können weitreichende wirtschaftliche und gesellschaftliche Folgen haben (Böhm, 2014, S. 26-28).

Ein besonderes Merkmal wesentlicher Dienste ist ihre kaskadierende Wirkung bei Ausfällen. Ein Cyberangriff auf ein Transportnetzwerk könnte beispielsweise die Lieferketten unterbrechen, medizinische Versorgung verzögern oder Notfalldienste beeinträchtigen. Dies unterstreicht die Notwendigkeit robuster Sicherheitsmaßnahmen und einer stärkeren sektorübergreifenden Zusammenarbeit.

### 2.2.2 Regulatorische Anforderungen und Compliance

Zur Gewährleistung der Sicherheit wesentlicher Dienste wurden auf europäischer Ebene umfassende gesetzliche Regelungen eingeführt. Mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union – der sogenannten NIS-Richtlinie – wurden Betreiber wesentlicher Dienste verpflichtet, geeignete Maßnahmen zur Risikobewältigung zu treffen. Konkret sind sie angehalten, Risiken für die Sicherheit ihrer Netz- und Informationssysteme systematisch zu identifizieren, geeignete technische und organisatorische Sicherheitsvorkehrungen zu implementieren sowie erhebliche Sicherheitsvorfälle an die zuständigen Behörden zu melden.

In Österreich erfolgt die nationale Umsetzung dieser Vorgaben durch das Netz- und Informationssystemsicherheitsgesetz (NISG, 2018), welches die Anforderungen der NIS-Richtlinie präzisiert und verschärft. Insbesondere verpflichtet das NISG Betreiber wesentlicher Dienste zur Einführung und Aufrechterhaltung eines Informationssicherheits-Managementsystems (ISMS) auf Basis der international

anerkannten Norm EN ISO/IEC 27001. Dadurch wird ein strukturiertes und risikobasiertes Vorgehen zur Sicherstellung der Informationssicherheit institutionalisiert.

Die Umsetzung dieser regulatorischen Anforderungen stellt viele Betreiber jedoch vor erhebliche Herausforderungen. Einerseits erfordert der Aufbau eines normkonformen ISMS beträchtliche personelle, technische und finanzielle Ressourcen. Andererseits nehmen die regulatorischen Anforderungen kontinuierlich zu, etwa durch den Digital Operational Resilience Act (DORA), der insbesondere Unternehmen des Finanzsektors betrifft und weitreichende Vorgaben für die digitale Resilienz einführt. Diese zunehmende Komplexität verlangt von den betroffenen Organisationen eine sorgfältige Balance zwischen der Erfüllung von Compliance-Anforderungen und der Aufrechterhaltung betrieblicher Effizienz. Die Einhaltung regulatorischer Vorgaben darf dabei nicht zu Lasten der operativen Leistungsfähigkeit gehen, weshalb ein integrativer und pragmatischer Ansatz bei der Implementierung von Sicherheitsmaßnahmen erforderlich ist.

### 2.2.3 Herausforderungen und Zukunftsperspektiven

Trotz ihrer herausragenden Bedeutung für die gesellschaftliche und wirtschaftliche Infrastruktur sehen sich Betreiber wesentlicher Dienste mit einer Vielzahl von Herausforderungen konfrontiert. Besonders kleinere Organisationen kämpfen häufig mit einer ausgeprägten Ressourcenknappheit, was sowohl finanzielle Mittel als auch qualifiziertes Personal im Bereich der Informationssicherheit betrifft. Diese Limitierungen erschweren es ihnen, die geforderten Sicherheitsstandards aufrechtzuerhalten und fortlaufend an neue Bedrohungslagen anzupassen.

Hinzu kommt die stetige Zunahme an Cyberbedrohungen, die eine kontinuierliche Weiterentwicklung und Anpassung bestehender Sicherheitsstrategien erforderlich macht. Angesichts der Dynamik und Komplexität der Bedrohungslandschaft sind statische Sicherheitsmaßnahmen zunehmend unzureichend; vielmehr bedarf es flexibler, risikobasierter Ansätze, die proaktiv auf neue Angriffsmuster reagieren können.

Darüber hinaus stellt die zunehmende Komplexität regulatorischer Anforderungen eine erhebliche Belastung für Betreiber dar. Neben der Umsetzung der Vorgaben der NIS-Richtlinie und nationaler Gesetze wie dem NISG müssen Betreiber auch neue europäische Regelwerke, wie etwa den Digital Operational Resilience Act (DORA) im Finanzsektor, berücksichtigen. Diese parallelen regulatorischen Stränge verlangen umfassende Compliance-Managementstrukturen und stellen eine nicht zu unterschätzende Herausforderung für die betroffenen Organisationen dar.

Ein zentraler Bestandteil zukunftsorientierter Sicherheitsstrategien ist die verstärkte Zusammenarbeit und der gezielte Informationsaustausch zwischen den relevanten Akteuren. Wie Kleinhans (2016, S. 106–108) betont, tragen Mechanismen wie sektorübergreifende Kooperationen, gemeinsame Bedrohungsanalysen und die

Durchführung von Sicherheitsübungen maßgeblich zur Stärkung der Resilienz bei. Durch eine strukturierte und vertrauensbasierte Zusammenarbeit können Synergieeffekte genutzt, Schwachstellen frühzeitig erkannt und die Stabilität wesentlicher Dienste langfristig gesichert werden.

## 2.3 Aktueller Forschungsstand und bisherige Arbeiten

Die Forschung zur Netzwerk- und Informationssicherheit, insbesondere im Hinblick auf Betreiber wesentlicher Dienste, hat in den letzten Jahren stark zugenommen. Dies ist vor allem auf die fortschreitende Digitalisierung kritischer Infrastrukturen und die damit verbundenen Cyberbedrohungen zurückzuführen. Die wissenschaftliche Auseinandersetzung mit diesem Thema konzentriert sich auf gesetzliche Vorschriften, Risikomanagement und die Implementierung von Informationssicherheits-Managementsystemen (ISMS) (Rudolph, 2013, S. 72-74). Dabei kombiniert die Forschung theoretische Konzepte mit empirischen Analysen, um die Widerstandsfähigkeit kritischer Infrastrukturen zu stärken.

### 2.3.1 Regulatorische Rahmenbedingungen und ISMS

Ein zentraler Forschungsbereich untersucht gesetzliche Vorgaben wie die NIS-Richtlinie der Europäischen Union und deren nationale Umsetzung, etwa im Netz- und Informationssystemsicherheitsgesetz (NIS-G) in Österreich. Studien (ENISA (European Union Agency for Cybersecurity), NIS Investments Report (2021)) zeigen, dass diese Regularien Unternehmen helfen, Cybersicherheitsstandards zu harmonisieren, bringen aber auch Herausforderungen mit sich – insbesondere in Bezug auf die Einhaltung von Vorschriften und die praktische Umsetzung. Besonders relevant ist hierbei die Einführung eines ISMS gemäß EN ISO/IEC 27001, das Unternehmen eine strukturierte Herangehensweise an Informationssicherheit ermöglicht.

Forschungen zu Best Practices (Tjader, Y. C., & Thomas, S. P. (2021), Assessing Organizational Change through ISMS Implementation) und Implementierungserfolgen in Unternehmen liefern wertvolle Erkenntnisse über die Wirksamkeit dieser Maßnahmen. Unternehmen, die ein ISMS implementieren, berichten über eine signifikante Verbesserung in der Sicherheitskultur und beim Risikomanagement. Mitarbeiter entwickeln ein besseres Bewusstsein für Sicherheitsrisiken, was zu einer Reduktion von Sicherheitsvorfällen führt (Tjader & Thomas (2021), S. 45-63). Obwohl die Einführung eines ISMS mit hohen anfänglichen Kosten verbunden ist, zeigen Studien, dass sich die Investition langfristig auszahlt, insbesondere durch die Vermeidung von Strafen, Reputationsverlusten und geschäftlichen Ausfällen (Kersten & Schröder, 2023).

### 2.3.2 Priorisierung von Sicherheitsmaßnahmen

Ein weiteres wichtiges Forschungsfeld betrifft die Priorisierung von Sicherheitsmaßnahmen innerhalb eines ISMS. Aufgrund der Vielzahl an Kontrollmaßnahmen in der EN ISO/IEC 27001 müssen Unternehmen strategisch entscheiden, welche Maßnahmen den größten Schutz bieten. Studien (Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023) *Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheits-Managementsysteme*) haben gezeigt, dass besonders die Vorbeugung von Informationssicherheitsfällen und die Forderung von Kundenseite zu den Hauptmotiven zählen. (Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023) Nutzung und Wirkung der Norm EN ISO/IEC 27001 für Informationssicherheits-Managementsysteme)

### 2.3.3 Abgrenzung zur bestehenden Forschung

Die in Abschnitt 2.3.2 dargestellten Ausführungen beleuchten die allgemeine Notwendigkeit zur Priorisierung von Sicherheitsmaßnahmen im Rahmen eines Informationssicherheits-Managementsystems (ISMS) gemäß EN ISO/IEC 27001. Dabei wird insbesondere auf strategische Überlegungen bei der Auswahl von Schutzmaßnahmen sowie auf externe Einflussfaktoren – wie Kundenanforderungen und die Prävention von Sicherheitsvorfällen – Bezug genommen. Die entsprechenden Studien verdeutlichen, dass Unternehmen häufig aus einer Vielzahl möglicher Maßnahmen diejenigen auswählen, die einerseits die größten Risiken adressieren und andererseits den externen Erwartungen gerecht werden.

Im Unterschied dazu fokussiert sich die vorliegende Arbeit auf eine spezifische Zielgruppe – nämlich Betreiber wesentlicher Dienste in Österreich im Sinne des NIS-Gesetzes – und stellt die Hypothese auf, dass sich aus der EN ISO/IEC 27001 fünf besonders relevante Maßnahmen ableiten lassen, die für diese Betreiber vorrangig zur Anwendung kommen sollten. Die Hypothese beruht auf der Annahme, dass bestimmte Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen bei kritischen Infrastrukturen eine abweichende Gewichtung innerhalb der Vielzahl an Steuerungsmaßnahmen erfordern.

Im Zentrum steht daher nicht die generelle Strategie zur Priorisierung von Maßnahmen, sondern vielmehr die Identifikation und Bewertung konkreter Maßnahmen, die unter den besonderen Rahmenbedingungen für Betreiber wesentlicher Dienste eine herausgehobene Rolle spielen. Die Hypothese kann somit einen Beitrag zur Konkretisierung der allgemeinen Forschung und unterstützt eine zielgerichtete Umsetzung der Norm im Kontext kritischer Infrastrukturen leisten.

### 2.3.4 Technologische Herausforderungen und neue Bedrohungen

Neben den regulatorischen Anforderungen rückt die Forschung zunehmend technologische Risiken und neue Bedrohungsszenarien in den Fokus. Insbesondere der rasante technologische Fortschritt in den Bereichen Internet of Things (IoT) und künstliche Intelligenz (KI) hat die Bedrohungslandschaft erheblich verändert und erweitert. Die Integration dieser Technologien in kritische Infrastrukturen sowie in Unternehmensnetzwerke eröffnet vielfältige Innovationspotenziale, schafft jedoch gleichzeitig neue Angriffsflächen für Cyberkriminelle.

**Internet of Things (IoT) als Risikofaktor:**

IoT-Geräte, die in immer größerer Zahl in Unternehmensumgebungen, Produktionsstätten und sogar sicherheitskritischen Infrastrukturen eingesetzt werden, stellen eine besondere Herausforderung dar. Viele dieser Geräte verfügen über nur rudimentäre oder veraltete Sicherheitsfunktionen. Häufig mangelt es an standardisierten Mechanismen für Authentifizierung, Verschlüsselung oder sichere Updates, wodurch IoT-Umgebungen zu bevorzugten Angriffszielen werden.

Studien des National Institute of Standards and Technology (NIST) (2021) unter dem Titel Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks belegen, dass die Bedrohungen im IoT-Bereich insbesondere durch folgende Faktoren verstärkt werden:

- Fehlende Sicherheitsvorgaben bei der Entwicklung: Viele Hersteller priorisieren Markteinführungszeit und Kosteneffizienz über Sicherheitsaspekte.
- Mangelhafte Wartung: Updates und Patches zur Behebung von Schwachstellen werden oft nicht oder nur verzögert bereitgestellt.
- Standardpasswörter und unsichere Konfigurationen: Viele IoT-Geräte werden mit voreingestellten Zugangsdaten betrieben, die leicht kompromittiert werden können.
- Fehlende Transparenz: Nutzer haben häufig keinen vollständigen Überblick über die Funktionsweise und die Kommunikation der Geräte.

**Künstliche Intelligenz (KI) als Chance und Risiko:**

Parallel zu den Herausforderungen im IoT-Bereich gewinnt der Einsatz von künstlicher Intelligenz im Bereich der Cybersicherheit an Bedeutung. KI kann einerseits helfen, Bedrohungen schneller zu erkennen und abzuwehren, indem sie Muster in großen Datenmengen analysiert und Anomalien identifiziert. Andererseits eröffnen KI-Technologien auch neue Angriffsmöglichkeiten, etwa durch automatisierte Phishing-Kampagnen, Deepfakes oder gezielte Angriffe auf KI-Modelle selbst (sogenannte Adversarial Attacks).

Die Forschung (Hasan, K., Hossain, F., Amin, A., Sutradhar, Y., Jeny, I. J., & Mahmud, S. (2025)) weist darauf hin, dass der Schutz von KI-Systemen künftig integraler

Bestandteil umfassender Sicherheitskonzepte sein muss. Dazu gehören Maßnahmen wie die Sicherstellung der Datenintegrität in Trainingsprozessen, Schutzmechanismen gegen Manipulationen und die Implementierung robuster Modelle, die gegenüber adversarialen Eingaben resilient sind.

### 2.3.5 Menschliche Faktoren in der Informationssicherheit

Ein weiteres wichtiges Forschungsgebiet betrifft die Rolle des Menschen in der Cybersicherheit. Studien haben gezeigt, dass Organisationskultur, Schulungen und Führungskräfteverhalten einen direkten Einfluss auf die Wirksamkeit von Sicherheitsmaßnahmen haben (Industrie.de (2024) Die Effektivität von Cybersicherheitstrainings). Regelmäßige Phishing-Tests, Mitarbeiterschulungen und Sicherheitsrichtlinien werden als entscheidende Maßnahmen zur Verbesserung des Sicherheitsbewusstseins identifiziert.

### 2.3.6 Erfahrungen aus Cyberangriffen und wirtschaftliche Auswirkungen

Empirische Studien (BSI (Bundesamt für Sicherheit in der Informationstechnik) (2021): Die Themen des 17. Deutschen IT-Sicherheitskongresses. BSI, Bonn) haben Cyberangriffe wie Ransomware-Angriffe oder Datendiebstähle analysiert, um häufige Schwachstellen zu identifizieren. Im Gesundheitswesen wurde beispielsweise gezeigt, dass Backup-Strategien und Notfallpläne entscheidend sind, um Angriffe abzumildern. Auch die wirtschaftlichen Aspekte der Cybersicherheit sind Gegenstand der Forschung – insbesondere die Kosten-Nutzen-Analyse von Investitionen in Sicherheitsmaßnahmen.

### 2.3.7 Zusammenarbeit und Informationsaustausch

Forschungen betonen zudem die Bedeutung von Zusammenarbeit und Informationsaustausch zwischen Unternehmen, Behörden und internationalen Partnern (Weber, 2014, S. 52-54). Plattformen für gemeinsame Bedrohungsanalysen, öffentliche-private Partnerschaften und sektorübergreifende Kooperationen werden als effektive Strategien zur Verbesserung der kollektiven Sicherheitslage angesehen.

## 2.4 Gesetzliche Rahmenbedingungen: Das Netz- und Informationssystemsicherheitsgesetz (NIS-G)

### 2.4.1 Historische Entwicklung und Hintergründe

Das Netz- und Informationssystemsicherheitsgesetz (NIS-G) wurde in Österreich als Reaktion auf die NIS-Richtlinie der Europäischen Union (2016/1148) eingeführt. Diese Richtlinie zielte darauf ab, eine harmonisierte Cybersicherheitsstrategie in der EU

(Steiger, 2022, S. 36-38) zu etablieren, da nationale Sicherheitsansätze zuvor fragmentiert waren und eine koordinierte Reaktion auf Cyberbedrohungen erschwerten.

Der historische Hintergrund dieser Entwicklung ist eng mit der zunehmenden Abhängigkeit von digitalen Technologien und der steigenden Zahl hochentwickelter Cyberangriffe verbunden. Besonders der Cyberangriff auf Estland im Jahr 2007 und der Stuxnet-Wurm 2010 verdeutlichten die Verwundbarkeit kritischer Infrastrukturen. Diese Vorfälle führten zur Erkenntnis, dass nationale Alleingänge nicht ausreichen, um Cyberbedrohungen (Schulze & Wollinger, 2020, S. 29-31) wirksam zu bekämpfen.

Mit der Verabschiedung der NIS-Richtlinie 2016 wurden alle EU-Staaten verpflichtet, sie in nationales Recht zu überführen. In Österreich trat das NIS-G im Jahr 2018 in Kraft und baute auf bestehenden Cybersicherheitsmaßnahmen auf. Es verschärfte die Anforderungen für Betreiber wesentlicher Dienste (OES) und Anbieter digitaler Dienste (DSP), indem es verbindliche Vorgaben für Risikomanagement, Vorfallmeldungen und die Implementierung eines ISMS (gemäß EN ISO/IEC 27001) einführte.

Bereits vor der NIS-Richtlinie hatte Österreich mit der Österreichischen Strategie für Cyber-Sicherheit (2013) erste Maßnahmen ergriffen, um Sensibilisierung, Zusammenarbeit und Reaktionsfähigkeit auf Cybervorfälle (Voigt & Bussche, 2024, S. 63-65) zu verbessern. Das NIS-G vertiefte diese Ansätze und legte rechtlich bindende Verpflichtungen fest.

Ein zentraler Aspekt der NIS-G-Entwicklung ist die internationale Zusammenarbeit. Österreich erkannte früh die Notwendigkeit, sich mit anderen EU-Mitgliedstaaten auszutauschen, um gemeinsame Bedrohungsanalysen, Best Practices und Sicherheitsstrategien (Steiger, 2022, S. 44-46) zu etablieren. Dieses Vorgehen trägt zur kollektiven Widerstandsfähigkeit in der EU bei und verhindert, dass einzelne Länder zum Schwachpunkt in der europäischen Cybersicherheitsarchitektur werden.

### 2.4.2 Wesentliche Inhalte und Anforderungen des NIS-G

Das Netz- und Informationssystemsicherheitsgesetz (NIS-G) stärkt die Cybersicherheit wesentlicher Dienste in Österreich, indem es klare Vorgaben für Betreiber wesentlicher Dienste (OES) und Anbieter digitaler Dienste (DSP) hinsichtlich Risikomanagement, Vorfallmeldung und Sicherheitsmaßnahmen definiert. Es verpflichtet Unternehmen zur Einführung eines Informationssicherheits-Managementsystems (ISMS) nach EN ISO/IEC 27001, um Cyberrisiken systematisch zu erkennen und zu minimieren. Zudem besteht eine Meldepflicht für schwerwiegende Sicherheitsvorfälle, um eine schnelle Reaktion auf Bedrohungen zu ermöglichen. Betreiber müssen geeignete technische und organisatorische Sicherheitsmaßnahmen umsetzen, darunter z.B. Netzwerksicherheit, Kryptografie, Datensicherung und Notfallpläne (ISO/IEC (2022): ISO/IEC 27001:2022, Anhang A). Die nationale Cybersicherheitsbehörde überwacht die Einhaltung des Gesetzes und kann bei

Verstößen Sanktionen verhängen. Das NIS-G trägt somit zur Erhöhung der Cyberresilienz kritischer Infrastrukturen und zur Harmonisierung der Sicherheitsstandards innerhalb der EU bei.

### 2.4.3 Vergleich mit internationalen Standards (z.B. NIST, ISO/IEC 27001)

Das NIS-G orientiert sich an etablierten internationalen Cybersicherheitsstandards wie ISO/IEC 27001 und dem NIST Cybersecurity Framework (Voigt & Bussche, 2024, S. 84-86), unterscheidet sich jedoch in einigen wesentlichen Aspekten.

Die EN ISO/IEC 27001 ist ein weltweit anerkannter Standard für Informationssicherheits-Managementsysteme (ISMS), der Unternehmen eine strukturierte Methodik zur Identifizierung, Bewertung und Minderung von Cybersicherheitsrisiken bietet. Das NIS-G fordert Betreiber wesentlicher Dienste (OES) und Anbieter digitaler Dienste (DSP) zur Implementierung eines ISMS nach EN ISO/IEC 27001 auf, geht aber darüber hinaus, indem es eine gesetzlich verpflichtende Vorfallmeldung und die staatliche Aufsicht durch nationale Behörden vorschreibt.

Im Gegensatz dazu bietet das NIST Cybersecurity Framework (National Institute of Standards and Technology (NIST) (2018): Framework for Improving Critical Infrastructure Cybersecurity) einen flexiblen und freiwilligen Ansatz für das Management von Cybersicherheitsrisiken. Es basiert auf fünf Kernfunktionen (Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen) (Steiger, 2022, S. 115-117) und lässt Unternehmen größere Gestaltungsfreiheit bei der Implementierung. Das NIS-G hingegen setzt verbindliche Vorgaben und fordert eine Koordinierung auf nationaler und EU-Ebene, um die Cybersicherheit sektorenübergreifend zu harmonisieren.

Ein weiterer Unterschied besteht in der internationalen Zusammenarbeit. Während sowohl EN ISO/IEC 27001 als auch das NIST-Framework die Bedeutung des Informationsaustauschs anerkennen, schreibt das NIS-G explizit die Zusammenarbeit zwischen Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und staatlichen Behörden vor (Schulze & Wollinger, 2020, S. 127-129).

Zusammenfassend kombiniert das NIS-G bewährte Praktiken aus internationalen Standards mit verbindlichen regulatorischen Anforderungen. Durch die Pflicht zur Vorfallmeldung, behördliche Kontrolle und sektorübergreifende Zusammenarbeit stellt es einen umfassenden Rahmen zur Verbesserung der Cyberresilienz kritischer Infrastrukturen dar.

## 2.5 ISO/IEC 27001 – Aufbau und Inhalte der Norm

Die ISO/IEC 27001 ist ein international anerkannter Standard für das Management der Informationssicherheit in Organisationen jeder Art und Größe. Sie definiert die Anforderungen an ein sogenanntes Informationssicherheits-Managementsystem (ISMS), dessen Ziel es ist, Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch ein systematisches Risikomanagement nachhaltig zu gewährleisten.

### 2.5.1 Zielsetzung der Norm

Die Norm ISO/IEC 27001 verfolgt das grundlegende Ziel, in Organisationen ein systematisches, risikobasiertes und kontinuierlich weiterentwickeltes Niveau an Informationssicherheit zu etablieren. Im Mittelpunkt steht dabei nicht ausschließlich die technische Absicherung von IT-Systemen, sondern ein ganzheitlicher Managementansatz, der alle wesentlichen Dimensionen der Informationssicherheit integriert – einschließlich organisatorischer, physischer und personeller Aspekte.

Ziel der Norm ist es, Organisationen ein strukturiertes Rahmenwerk zur Verfügung zu stellen, mit dem sie ihre Informationswerte systematisch schützen können. Hierzu gehören Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) von Informationen, unabhängig davon, in welcher Form diese Informationen gespeichert, verarbeitet oder übertragen werden.

Wesentliche Zielsetzungen der ISO/IEC 27001 im Detail:

- **Etablierung eines Informationssicherheits-Managementsystems (ISMS):**
  Die Norm fordert den Aufbau eines umfassenden Managementsystems, das Prozesse, Rollen, Verantwortlichkeiten und Ressourcen definiert, um die Informationssicherheit dauerhaft und systematisch zu gewährleisten.
- **Risikoorientierung:**
  Organisationen sollen Risiken für ihre Informationssicherheit frühzeitig erkennen, systematisch bewerten und angemessene Maßnahmen zu ihrer Steuerung oder Reduktion umsetzen. Das Risikomanagement bildet das zentrale Steuerungselement des ISMS.
- **Ganzheitlicher Ansatz:**
  Die Norm betrachtet Informationssicherheit nicht isoliert als rein technisches Thema. Sie verlangt die Berücksichtigung organisatorischer Strukturen, menschlicher Faktoren (z. B. Schulung, Sensibilisierung) sowie physischer Sicherheitsmaßnahmen (z. B. Zugangskontrollen zu Gebäuden).
- **Klar definierte Verantwortlichkeiten:**
  ISO/IEC 27001 betont die Verantwortung der obersten Leitung für die Informationssicherheit. Management Commitment und die aktive Unterstützung des ISMS sind zwingende Voraussetzungen für den Erfolg der Sicherheitsstrategie.

- **Kontinuierliche Verbesserung:**
  Informationssicherheit wird als dynamischer Prozess verstanden. Organisationen müssen ihr ISMS regelmäßig überwachen, bewerten und an veränderte Rahmenbedingungen anpassen. Der PDCA-Zyklus („Plan-Do-Check-Act“) bildet hierbei die methodische Grundlage.
- **Flexibilität und Skalierbarkeit:**
  Die Norm ist bewusst branchenneutral und skalierbar gestaltet. Sie eignet sich sowohl für kleine Organisationen als auch für große multinationale Konzerne. Anpassungen an die spezifischen Rahmenbedingungen und Risiken der jeweiligen Organisation sind explizit vorgesehen.

**Praktischer Nutzen der Umsetzung:**

Die Einführung eines ISMS nach ISO/IEC 27001 bietet Organisationen neben der Erhöhung der Sicherheitsresilienz weitere Vorteile:

- Erfüllung gesetzlicher und regulatorischer Anforderungen (z. B. NISG, DSGVO)
- Erhöhung des Vertrauens bei Kunden, Partnern und Aufsichtsbehörden
- Reduktion von Schadenspotenzialen durch proaktives Risikomanagement
- Wettbewerbsvorteile durch die Zertifizierung nach einer international anerkannten Norm
- Förderung einer Sicherheitskultur innerhalb der gesamten Organisation

Insgesamt ermöglicht die ISO/IEC 27001 Unternehmen, einen strukturierten und nachvollziehbaren Weg zu beschreiten, um Informationsrisiken beherrschbar zu machen und die Sicherheit ihrer geschäftskritischen Informationen nachhaltig zu stärken.

### 2.5.2 Aufbau und Struktur der ISO/IEC 27001

Die ISO 27001 folgt der High Level Structure (HLS), einer einheitlichen Struktur für alle modernen ISO-Managementsystemnormen (wie ISO 9001 oder ISO 14001). Dies erleichtert die Integration verschiedener Managementsysteme. Die Norm ist in 10 Hauptkapitel (Clauses) gegliedert, wobei die Anforderungen an ein ISMS insbesondere in den Kapiteln 4 bis 10 beschrieben werden:

1. **Einleitung** – Grundsätzliche Informationen zur Norm.
2. **Normative Verweise** – Bezug zu anderen Normen.
3. **Begriffe** – Definition zentraler Begriffe.
4. **Kontext der Organisation** – Analyse interner und externer Rahmenbedingungen sowie der Bedürfnisse von interessierten Parteien (z. B. Kunden, Aufsichtsbehörden).
5. **Führung** – Verpflichtung der obersten Leitung, Festlegung der Informationssicherheitspolitik und Rollenverteilung.
6. **Planung** – Risikoanalyse und Ableitung von Zielen und Maßnahmen.
7. **Unterstützung** – Ressourcen, Kompetenzen, Schulungen, Kommunikation, Dokumentation.

8. **Betrieb** – Umsetzung der geplanten Maßnahmen im operativen Tagesgeschäft.
9. **Bewertung der Leistung** – Monitoring, interne Audits, Managementbewertungen.
10. **Verbesserung** – Maßnahmen zur Korrektur und kontinuierlichen Verbesserung des ISMS.

### 2.5.3 Anhang A – Sicherheitsmaßnahmen (Controls)

Ein zentraler Bestandteil der Norm ISO/IEC 27001:2022 ist der Anhang A, der eine strukturierte Liste von 93 Sicherheitsmaßnahmen (Controls) bereitstellt. Diese Maßnahmen dienen als umfassender Katalog zur Unterstützung der Organisation bei der Auswahl geeigneter Schutzvorkehrungen im Rahmen ihres individuellen Risikomanagementprozesses. Der Anhang A stellt damit eine systematische Referenz dar, um sicherzustellen, dass alle relevanten Aspekte der Informationssicherheit berücksichtigt werden.

**Aufbau und Struktur:**

Die 93 Controls im Anhang A sind in vier thematische Bereiche („Themengruppen“) gegliedert:

1. **Organisatorische Maßnahmen (Organizational Controls)**
   Maßnahmen, die sich auf die Struktur, Richtlinien und Prozesse innerhalb der Organisation beziehen, beispielsweise Management von Informationssicherheitsrollen oder Supplier Relationships Management.
2. **Personenbezogene Maßnahmen (People Controls)**
   Kontrollen, die den sicheren Umgang von Mitarbeitenden mit Informationen sicherstellen, etwa durch Schulungen, Verhaltensrichtlinien und Disziplinarmaßnahmen.
3. **Physische Maßnahmen (Physical Controls)**
   Schutz von physischen Infrastrukturen wie Rechenzentren, Serverräumen und Arbeitsplätzen gegen unbefugten Zutritt, physische Schäden oder Diebstahl.
4. **Technologische Maßnahmen (Technological Controls)**
   Technische Sicherheitsvorkehrungen, wie z. B. Verschlüsselung, Zugriffskontrollen und Überwachungssysteme.

Die folgende Tabelle zeigt tabellarische Übersicht der vier Themengruppen aus Anhang A der ISO/IEC 27001:2022 mit der Anzahl der Controls pro Themengruppe.

| Themengruppe | Anzahl Controls | Inhalt/Beschreibung |
|---|---|---|
| **Organisatorische Maßnahmen** (Organizational Controls) | 37 Controls | Steuerung der Informationssicherheit durch Richtlinien, Prozesse und Verantwortlichkeiten innerhalb der Organisation. Umfasst auch Lieferantenmanagement und Compliance-Themen. |
| **Personenbezogene Maßnahmen** (People Controls) | 8 Controls | Sicherheitsanforderungen im Umgang mit Mitarbeitenden, z. B. Bewusstsein, Schulungen, Sicherheitsüberprüfungen und Rollenmanagement. |
| **Physische Maßnahmen** (Physical Controls) | 14 Controls | Schutz der physischen Umgebung, wie Zutrittskontrollen, Schutz vor Naturkatastrophen und Gerätesicherheit. |
| **Technologische Maßnahmen** (Technological Controls) | 34 Controls | Anwendung technischer Schutzmechanismen, z. B. Zugriffskontrollen, Kryptografie/Verschlüsselung, Überwachungssysteme und Management von technischen Schwachstellen. |

**Tabelle 1:** tabellarische Übersicht der vier Themengruppen aus Anhang A der ISO/IEC 27001:2022

**Beispiele für wichtige Themenbereiche:**

- **Zugriffskontrolle:** Maßnahmen zur Sicherstellung, dass nur autorisierte Benutzer Zugriff auf Informationen und Systeme erhalten (z. B. Authentifizierungsmechanismen, Benutzerberechtigungsmanagement).
- **Kryptografie:** Vorgaben für die Nutzung kryptografischer Verfahren zur Sicherung der Vertraulichkeit, Integrität und Authentizität von Informationen.
- **Sicherheitsrichtlinien für Mitarbeitende:** Vorgaben zur Sensibilisierung, Schulung und zur Festlegung sicherheitsrelevanter Verhaltensweisen im Unternehmen.

- **Physische und Umwelt-Sicherheit:** Maßnahmen zum Schutz von Gebäuden und Infrastruktur, inklusive Zutrittskontrollen, Überwachungseinrichtungen und Schutzvorkehrungen gegen Umweltgefahren wie Feuer oder Überschwemmungen.
- **Betriebssicherheit:** Maßnahmen zur Gewährleistung eines sicheren Betriebs von Informationssystemen, darunter Backup-Strategien, Protokollierung sicherheitsrelevanter Ereignisse und Patch-Management.
- **Kommunikations- und Lieferantenmanagement:** Schutz von Kommunikationsverbindungen und sorgfältige Auswahl sowie Überwachung von Dienstleistern, die Zugriff auf sensible Informationen haben.
- **Notfallmanagement:** Vorgaben zur Vorbereitung auf Störungen und Krisen, inklusive Plänen für die Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs (Business Continuity Management).

**Anwendung der Maßnahmen:**

Die im Anhang A aufgeführten Maßnahmen sind nicht verpflichtend im Sinne einer vollständigen Umsetzung. Stattdessen dienen sie als strukturierte Auswahlhilfe im Rahmen des Risikomanagements. Organisationen müssen auf Basis ihrer individuellen Risikoanalyse entscheiden, welche der vorgeschlagenen Maßnahmen für sie relevant und angemessen sind.

Die Ergebnisse dieser Auswahl werden in der sogenannten **Erklärung zur Anwendbarkeit (Statement of Applicability, SoA)** dokumentiert.

Die SoA listet auf:

- Alle in Anhang A enthaltenen Maßnahmen
- Ob die jeweilige Maßnahme angewendet wird
- Begründungen für die Auswahl oder Nichtauswahl
- Hinweise auf die Implementierung der Maßnahme innerhalb des ISMS

Die SoA ist damit ein zentrales Dokument im Rahmen des Zertifizierungsprozesses, da sie eine nachvollziehbare Verbindung zwischen Risikobewertung, Risikobehandlung und den getroffenen Sicherheitsmaßnahmen herstellt.

Wesentliche Neuerungen gegenüber der Vorgängerversion:

Mit der Überarbeitung der ISO/IEC 27001 im Jahr 2022 wurde der Anhang A grundlegend modernisiert. Frühere Kategorien wie „A.5 Informationssicherheits-richtlinien“ oder „A.13 Kommunikationssicherheit“ wurden neu gruppiert, und moderne Aspekte wie „Cloud Services“, „Threat Intelligence“ und „Information Security for Use of Cloud Services“ wurden explizit integriert. Damit trägt die Norm aktuellen technologischen Entwicklungen und neuen Bedrohungsszenarien Rechnung.

### 2.5.4 Zertifizierung

Eine Organisation kann ihr Informationssicherheits-Managementsystem (ISMS) nach der internationalen Norm ISO/IEC 27001 zertifizieren lassen. Die Zertifizierung erfolgt durch eine unabhängige, akkreditierte Zertifizierungsstelle und dient als anerkannter Nachweis für die wirksame Implementierung und den kontinuierlichen Betrieb eines risikobasierten Informationssicherheitsmanagements. Sie wird zunehmend von Geschäftspartnern, Kunden und Aufsichtsbehörden gefordert und stellt einen entscheidenden Wettbewerbsvorteil dar.

**Vorbereitung auf die Zertifizierung:**

Vor dem eigentlichen Zertifizierungsprozess sind umfassende Vorbereitungen erforderlich:

- **Definition des Geltungsbereichs (Scope):** Die Organisation legt genau fest, auf welche Standorte, Abteilungen, Prozesse und Informationssysteme sich das ISMS bezieht. Der Geltungsbereich wird später auch im Zertifikat ausgewiesen.
- **Risikobewertung und Risikobehandlung:** Die Organisation identifiziert systematisch Risiken für die Informationssicherheit, bewertet deren Eintrittswahrscheinlichkeit und potenzielle Auswirkungen und entwickelt angemessene Maßnahmen zur Risikobehandlung. Die Ergebnisse werden dokumentiert, typischerweise in einem sogenannten Risiko- und Maßnahmenplan.
- **Festlegung der Sicherheitsziele und Erstellung relevanter Dokumentationen:** Zentrale ISMS-Dokumente wie Informationssicherheits-richtlinien, Rollen- und Verantwortlichkeitsbeschreibungen, Verfahrensanweisungen sowie Nachweise zur Umsetzung (z. B. Schulungsnachweise, Protokolle von Sicherheitsereignissen) müssen erstellt und gepflegt werden.
- **Durchführung interner Audits:** Vor der externen Auditierung führt die Organisation interne Audits durch, um die Wirksamkeit und Konformität des ISMS mit der Norm sicherzustellen und etwaige Abweichungen frühzeitig zu erkennen und zu beheben.
- **Management-Review:** Die oberste Leitung bewertet die Leistung des ISMS regelmäßig im Rahmen eines formellen Management-Reviews. Dabei werden unter anderem Audit-Ergebnisse, die Erreichung von Sicherheitszielen und relevante Veränderungen der Risikosituation betrachtet.
- **Umsetzung eines kontinuierlichen Verbesserungsprozesses:** Die Organisation muss darlegen, wie sie aus Vorfällen, Prüfungen und neuen Bedrohungen lernt und ihr ISMS fortlaufend optimiert.

**Ablauf des Zertifizierungsprozesses:**

Der Zertifizierungsprozess selbst gliedert sich typischerweise in folgende Phasen:

1. **Voraudit (optional):** Viele Organisationen nutzen ein freiwilliges Voraudit, um Schwachstellen im ISMS vor dem eigentlichen Zertifizierungsaudit zu identifizieren.
2. **Stufe-1-Audit (Dokumentenprüfung):** Die Zertifizierungsstelle prüft zunächst die Dokumentation des ISMS. Ziel ist es zu beurteilen, ob die grundlegenden Anforderungen der ISO/IEC 27001 erfüllt sind und ob das ISMS bereit für die vollständige Auditierung ist. Schwerpunkt liegt auf der formellen Vollständigkeit und Plausibilität der Dokumente.
3. **Stufe-2-Audit (Systemaudit vor Ort):** Im Rahmen des Hauptaudits erfolgt eine eingehende Überprüfung der praktischen Umsetzung des ISMS vor Ort. Auditoren prüfen, ob die dokumentierten Verfahren tatsächlich gelebt werden, führen Interviews mit Mitarbeitenden, nehmen Stichproben von Prozessen und bewerten die Effektivität der implementierten Kontrollen. Besondere Aufmerksamkeit gilt typischerweise den Bereichen Risikomanagement, Zugriffskontrolle, Schulung und Sensibilisierung sowie dem Umgang mit Sicherheitsvorfällen.
4. **Auditbericht und Entscheidung:** Nach Abschluss des Audits erstellt die Zertifizierungsstelle einen Bericht. Werden schwerwiegende Abweichungen ("Major Non-Conformities") festgestellt, müssen diese innerhalb einer festgelegten Frist behoben werden. Kleinere Abweichungen ("Minor Non-Conformities") müssen dokumentiert und im Rahmen des kontinuierlichen Verbesserungsprozesses adressiert werden. Über die Zertifikatserteilung entscheidet die Zertifizierungsstelle auf Basis des Auditberichts.
5. **Erteilung des Zertifikats:** Bei erfolgreichem Abschluss wird das Zertifikat mit einer Gültigkeitsdauer von in der Regel drei Jahren ausgestellt.
6. **Überwachungsaudits:** Während der Gültigkeitsdauer des Zertifikats finden jährlich sogenannte Überwachungsaudits statt. Hierbei wird geprüft, ob das ISMS weiterhin wirksam betrieben und verbessert wird.
7. **Rezertifizierung:** Nach Ablauf der Zertifikatslaufzeit ist ein vollständiges Rezertifizierungsaudit erforderlich, um die Gültigkeit des Zertifikats zu verlängern.

**Schwerpunkte im Rahmen der ISO/IEC 27001-Zertifizierung:**

Im Verlauf der Zertifizierung werden insbesondere folgende Aspekte besonders geprüft:

- Strukturierter Risikomanagementprozess
- Integration von Informationssicherheit in alle relevanten Geschäftsprozesse
- Verpflichtung der obersten Leitung zur Informationssicherheit
- Effektive Umsetzung technischer und organisatorischer Schutzmaßnahmen
- Nachweisbare Schulung und Sensibilisierung der Mitarbeitenden

- Handhabung und Nachverfolgung von Sicherheitsvorfällen
- Fortlaufende Überprüfung und Verbesserung des ISMS

Die Zertifizierung stellt somit nicht nur einen formalen Nachweis dar, sondern fördert auch nachhaltig eine Sicherheitskultur innerhalb der Organisation.

# 3. Methodik

## 3.1 Forschungsmethode: Qualitative Befragung

Die Untersuchung basiert auf qualitativen Interviews als primäre Forschungsmethode, um tiefgehende Einblicke in die Erfahrungen und Herausforderungen von Betreibern wesentlicher Dienste (OES) bei der Implementierung von Informationssicherheits-Managementsystemen (ISMS) gemäß den Anforderungen des Netz- und Informationssystemsicherheitsgesetzes (NIS-G) (Wegener & Mikos, 2017, S. 63-65) zu gewinnen. Die Wahl dieser Methode begründet sich in ihrem explorativen Charakter, da sie komplexe Prozesse und Kontexte erfasst, die mit quantitativen Methoden nur schwer messbar wären. Besonders im Bereich der Cybersicherheit kritischer Infrastrukturen sind die individuellen Erfahrungen, Praktiken und Perspektiven entscheidend, um die Wirksamkeit der regulatorischen Anforderungen zu bewerten.

Für die Erhebung der Daten wurden halbstrukturierte Interviews verwendet, um eine Balance zwischen Standardisierung und Flexibilität zu gewährleisten. Diese Form ermöglicht einerseits eine Vergleichbarkeit der Antworten, erlaubt es aber andererseits, detaillierte Nachfragen zu stellen, um spezifische Herausforderungen einzelner Sektoren (z. B. Energie, Gesundheitswesen, Transport) zu vertiefen. Der Interviewleitfaden wurde auf Basis der Forschungsziele und einer Literaturrecherche entwickelt und deckte neben den allgemeinen Themen wie die Umsetzung des ISMS, die Einhaltung des NIS-G, die Priorisierung von spezifischen Sicherheitsmaßnahmen und bestehende Herausforderungen ab, welche in Bezug auf die Hypothese betrachtet werden. Offene Fragen sollten es den Teilnehmern ermöglichen, reflektierte und detaillierte Antworten zu geben, ohne durch vordefinierte Kategorien eingeschränkt zu sein.

**Teilnehmerauswahl und Durchführung der Interviews**

Die Auswahl der Studienteilnehmer erfolgte gezielt, um eine hohe Relevanz und Glaubwürdigkeit der erhobenen Daten sicherzustellen. Die Zielgruppe bestand aus Cybersicherheitsbeauftragten (z.B. Chief Information Security Officers) und Finanzmanagern, die direkt mit der Implementierung und Verwaltung eines ISMS in ihren Unternehmen befasst sind. Durch diese Auswahl wurde eine technische und strategische Perspektive auf die Herausforderungen der NIS-G-Compliance gewährleistet. Um eine breite Repräsentation verschiedener Sektoren sicherzustellen, wurden Teilnehmer aus verschiedenen kritischen Infrastrukturen rekrutiert. Der Zugang zu den Teilnehmern erfolgte über branchenbezogene Netzwerke, Unternehmensverzeichnisse und Fachverbände.

Vor den Interviews erhielten die Teilnehmer eine Einladung, die die Forschungsziele, den Ablauf der Interviews sowie Datenschutz- und Vertraulichkeitsrichtlinien erklärte. Die freiwillige Teilnahme wurde betont, und alle Teilnehmer gaben eine informierte

Einwilligung zur anonymisierten Analyse ihrer Antworten. Die Interviews wurden entweder persönlich oder über sichere Videokonferenzplattformen durchgeführt und dauerten in der Regel zwischen 45 und 60 Minuten. Während der Interviews wurden neben Tonaufnahmen auch Notizen gemacht, um nonverbale Hinweise und Kontextinformationen zu erfassen.

**Datenanalyse und ethische Überlegungen**

Die erhobenen Interviewdaten wurden nach der Methode der Inhaltsanalyse ausgewertet, um Muster, Themen und Zusammenhänge zu identifizieren. Die Transkription der Interviews erfolgte sorgfältig, um die Nuancen der Antworten zu erhalten. Der Kodierungsprozess war sowohl deduktiv als auch induktiv, das heißt, dass bereits aus der Literatur bekannte Kategorien mit neu aufgetretenen Themen ergänzt wurden. Dadurch konnten branchenspezifische Sicherheitsprioritäten und Compliance-Herausforderungen systematisch erfasst werden.

Ethische Überlegungen spielten eine zentrale Rolle im Forschungsprozess. Um die Vertraulichkeit der Teilnehmer zu wahren, wurden alle Namen und organisatorischen Details anonymisiert. Die Daten wurden verschlüsselt gespeichert. Zudem hatten alle Teilnehmer das Recht, ihre Teilnahme jederzeit ohne Angabe von Gründen zu beenden. Diese Maßnahmen stellten sicher, dass die Studie den ethischen Standards der Forschung entsprach.

Die gewonnenen Erkenntnisse tragen zur wissenschaftlichen und praktischen Diskussion über Cybersicherheit und NIS-G-Compliance bei. Sie liefern wertvolle Einblicke in die Herausforderungen und Optimierungsmöglichkeiten für Unternehmen, die sich an die regulatorischen Anforderungen des NIS-G anpassen müssen.

## 3.2 Auswahl der Befragungsteilnehmer (Kriterium: Betreiber wesentlicher Dienste)

Die Auswahl der Interviewteilnehmer war ein zentraler Bestandteil des Forschungsdesigns, um sicherzustellen, dass die gewonnenen Daten relevant und aussagekräftig für die Untersuchung der Implementierung von Informationssicherheits-Managementsystemen (ISMS) im Rahmen des NIS-G sind. Die Teilnehmer wurden aus Organisationen rekrutiert, die als Betreiber wesentlicher Dienste (OES) gemäß dem NIS-G eingestuft sind. Die zentrale Voraussetzung für die Teilnahme war die direkte Verantwortlichkeit der Befragten für die Implementierung und Verwaltung von Informationssicherheitsmaßnahmen, insbesondere im Hinblick auf die NIS-G-Compliance.

**Gesamtzahl der Teilnehmer und Auswahlprozess**

Insgesamt wurden 99 Betreiber wesentlicher Dienste (BwD) (Blauensteiner BMI, 2024) identifiziert, die in Österreich unter das NIS-G fallen. Die Studie zielte darauf ab, eine

repräsentative Auswahl dieser Betreiber in die Untersuchung einzubeziehen, um ein möglichst umfassendes Bild bzgl. der Hypothese zu erhalten.

Neben den beruflichen Rollen und branchenspezifischen Kriterien spielte auch die geografische Verteilung der Teilnehmer eine wichtige Rolle. Die Studie berücksichtigte Organisationen aus verschiedenen Regionen Österreichs, um mögliche regionale Unterschiede in der Umsetzung des NIS-G zu identifizieren. Zudem wurde ein Gleichgewicht zwischen öffentlichen und privaten Organisationen angestrebt, da beide Gruppen mit unterschiedlichen Herausforderungen und Prioritäten in der Cybersicherheit konfrontiert sind. Während öffentliche Einrichtungen oft mit begrenzten Budgets und behördlichen Vorgaben umgehen müssen, sind private Unternehmen stärker auf Wirtschaftlichkeit und Wettbewerbsvorteile fokussiert.

Durch diese methodische Auswahl konnte sichergestellt werden, dass die Ergebnisse der Studie repräsentativ und übertragbar auf die breite Gruppe der OES in Österreich sind und eine detaillierte Analyse der Herausforderungen und Strategien bei der Umsetzung des NIS-G ermöglichen.

## 3.3 Struktur des Interviewleitfadens

Der Interviewleitfaden wurde sorgfältig entwickelt, um die Forschungsziele bestmöglich zu unterstützen und aussagekräftige Antworten von den Teilnehmern zu erhalten. Er besteht aus drei Hauptabschnitten: Einführungsfragen, Kernthemenfragen und Abschlussfragen. Diese Struktur sorgt für einen logischen Gesprächsfluss und ermöglicht es den Teilnehmern, ihre Erfahrungen mit der ISMS-Implementierung unter dem NIS-G detailliert zu teilen.

Der Einführungsabschnitt dient dazu, eine offene Gesprächsatmosphäre zu schaffen. Er enthält Fragen zum beruflichen Hintergrund, zur Rolle des Teilnehmers und zu allgemeinen Cybersicherheitspraktiken in der Organisation. Dies hilft, einen Kontext für die Antworten zu gewinnen.

Der Hauptteil des Interviews konzentriert sich auf spezifische Forschungsfragen, insbesondere zur Risikobewertung, Priorisierung von Sicherheitsmaßnahmen und Herausforderungen bei der NIS-G-Compliance. Fragen sind offen formuliert, um detaillierte Einblicke zu ermöglichen. Zudem werden Hindernisse bei der Umsetzung des NIS-G sowie die Wirksamkeit des ISMS thematisiert.

Im Schlussabschnitt können Teilnehmer zusätzliche Erkenntnisse teilen und Empfehlungen für zukünftige Cybersicherheitsstrategien geben. Abschließend wird ihnen für ihre Teilnahme gedankt. Diese strukturierte Herangehensweise gewährleistet eine tiefergehende Analyse der Herausforderungen und Best Practices bei der Umsetzung des NIS-G.

### 3.3.1 Interviewleitfaden

**Einführende Fragen**

1. Können Sie Ihre Rolle und Verantwortung in Ihrer Organisation kurz beschreiben, insbesondere im Hinblick auf die Informationssicherheit?
2. Wie lange sind Sie schon an der Implementierung und Verwaltung von ISMS in Ihrer Organisation beteiligt?

| kleiner 1 Jahr | 2-3Jahre | größer 3 Jahre |
|---|---|---|
| | | |

3. Könnten Sie einen Überblick über den Ansatz Ihrer Organisation hinsichtlich Cybersicherheit und Einhaltung des NIS-G geben?

**Zentrale thematische Fragen**

**Risikobewertung und Priorisierung**

4. Wie identifiziert und bewertet Ihre Organisation Cybersicherheitsrisiken?
5. Welche Faktoren beeinflussen die Priorisierung von Sicherheitsmaßnahmen innerhalb Ihres ISMS?

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | **Informationssicherheitsrichtlinien (A.5)** | | | | | | | | | |
| | ▪ Definition und Steuerung von Richtlinien zur Informationssicherheit<br>▪ Regelmäßige Überprüfung und Aktualisierung der Richtlinien | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Organisation der Informationssicherheit (A.6)** | | | | | | | | | |
| | ▪ Festlegung von Verantwortlichkeiten für die Informationssicherheit<br>▪ Integration der Sicherheitsanforderungen in Projekte und externe Partner | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Personalsicherheit (A.7)** | | | | | | | | | |
| | ▪ Sicherheitsüberprüfung von Mitarbeitern vor und nach der Einstellung<br>▪ Bewusstseinsbildung und Schulung zu Cybersicherheitsrisiken<br>▪ Disziplinarmaßnahmen bei Sicherheitsverstößen | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Asset-Management (A.8)** | | | | | | | | | |
| | ▪ Erstellung eines Inventars von Informationswerten (Assets)<br>▪ Klassifizierung und Schutz von Informationen basierend auf Sensibilität | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | ▪ Richtlinien zur Handhabung, Speicherung und Entsorgung von Informationen | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| | | | | | | | | | | |
| ☐ | **Zugriffskontrolle (A.9)** | | | | | | | | | |
| | ▪ Definition von Zugriffsrechten und -rollen<br>▪ Einführung von starken Authentifizierungsmechanismen<br>▪ Sicherstellung des Prinzips der geringsten Privilegien (Least Privilege) | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Kryptographie (A.10)** | | | | | | | | | |
| x | ▪ Anwendung von verschlüsselten Verfahren für Datenübertragung und -speicherung<br>▪ Management von Schlüsseln für Kryptografie | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Physische und umgebungsbezogene Sicherheit (A.11)** | | | | | | | | | |
| | ▪ Schutz von Rechenzentren und Bürogebäuden<br>▪ Zutrittskontrollen für sensible Bereiche<br>▪ Sicherstellung der Verfügbarkeit kritischer IT-Systeme | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Betriebssicherheit (A.12)** | | | | | | | | | |
| xxx | ▪ Implementierung von Schutzmaßnahmen gegen Schadsoftware<br>▪ Sicherstellung regelmäßiger Datensicherungen (Backups)<br>▪ Überwachung und Protokollierung sicherheitsrelevanter Ereignisse | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Kommunikationssicherheit (A.13)** | | | | | | | | | |
| | ▪ Schutz der Vertraulichkeit und Integrität von Netzwerken und Kommunikationskanälen<br>▪ Sichere Datenübertragung innerhalb und außerhalb der Organisation | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Systemerwerb, -entwicklung und -wartung (A.14)** | | | | | | | | | |
| x | ▪ Einbindung von Sicherheitsanforderungen in Entwicklungsprozesse<br>▪ Sichere Software- und Systementwicklung<br>▪ Schwachstellenmanagement und regelmäßige Sicherheitsupdates | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | **Lieferantenbeziehungen (A.15)** | | | | | | | | | |
| | ▪ Bewertung und Steuerung von Sicherheitsrisiken durch Dritte<br>▪ Festlegung vertraglicher Anforderungen für Lieferanten und Dienstleister | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Management von Sicherheitsvorfällen (A.16)** | | | | | | | | | |
| | ▪ Prozesse zur Erkennung, Meldung und Reaktion auf Sicherheitsvorfälle<br>▪ Dokumentation und Lernen aus Sicherheitsvorfällen | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Notfallmanagement (A.17)** | | | | | | | | | |
| | ▪ Entwicklung von Plänen zur Aufrechterhaltung der Geschäftskontinuität<br>▪ Durchführung von Tests und Übungen zur Notfallbewältigung | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |
| ☐ | **Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen (A.18)** | | | | | | | | | |
| | ▪ Überwachung von rechtlichen Verpflichtungen<br>▪ Sicherstellung der Einhaltung von Datenschutzgesetzen<br>▪ Regelmäßige Compliance-Prüfungen und interne Audits | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | |

**Einhaltung von NIS-G**

6. Vor welchen Herausforderungen stand Ihr Unternehmen bei der Erfüllung der gesetzlichen Anforderungen von NIS-G?
7. Wie wirksam waren die Prozesse zur Meldung und Prüfung von Vorfällen bei der Verbesserung der Cybersicherheitslage Ihres Unternehmens?

**Wirksamkeit des ISMS**

8. Was waren Ihrer Erfahrung nach den bedeutendsten Vorteilen der Implementierung eines ISMS im Rahmen des NIS-G-Rahmenwerks?
9. Gibt es Bereiche, in denen das ISMS verbessert werden könnte, um den Anforderungen Ihrer Organisation besser gerecht zu werden?

**Abschließende Fragen**

10. Was sind Ihrer Meinung nach die zukünftigen Herausforderungen und Chancen für die Cybersicherheit in Ihrem Sektor?

11. Haben Sie Empfehlungen für Organisationen oder politische Entscheidungsträger, um die Implementierung und Wirksamkeit von ISMS zu verbessern?

## 3.4 Durchführung und Dokumentation der Befragungen

Jedes Interview wurde anhand des in Abschnitt 3.3 entwickelten Interviewleitfadens strukturiert. Die Teilnehmer wurden ermutigt, detaillierte und reflektierte Antworten auf die offenen Fragen zu geben. Der Ansatz eines aktiven Zuhöransatzes wurde verfolgt, um sicherzustellen, dass sich die Teilnehmer gehört und wertgeschätzt fühlten. Diese Technik beinhaltete, ihre Antworten zu bestätigen, bei Bedarf um Klarstellungen zu bitten und Folgefragen zu stellen, um tiefer in bestimmte Themen einzutauchen (Lüdders, 2017, S. 22-24).

## 3.5 Inhaltsanalyse nach Mayring

Die Analyse der Interviewdaten wurde mithilfe der Inhaltsanalysemethode nach Philipp Mayring (Pelka, 2018, S. 52-54) durchgeführt, die sich durch einen systematischen und transparenten Ansatz zur qualitativen Dateninterpretation auszeichnet. Diese Methode wurde gewählt, da sie eine strukturierte Kategorisierung (Form der Inhaltsanalyse) und Organisation komplexer Textdaten ermöglicht und sich besonders für explorative Forschung zur ISMS-Implementierung eignet.

Der erste Schritt umfasste die Formulierung von Fragen für die Erhebung der Ausprägung in den jeweiligen Kategorien (Kategorienbildung). Diese basieren auf dem theoretischen Rahmen und dem Anhang von ISO 27001:2022 Anhang A.

Die vordefinierten Kategorien umfassten Themen:

- "A.5 Informationssicherheitsrichtlinien",
- "A.6 Organisation der Informationssicherheit",
- "A.7 Personalsicherheit",
- "A.8 Asset-Management",
- "A.9 Zugriffskontrolle",
- "A.10 Kryptographie",
- "A.11 Physische und umgebungsbezogene Sicherheit",
- "A.12 Betriebssicherheit",
- "A.13 Kommunikationssicherheit",
- "A.14 Systemerwerb, -entwicklung und -wartung",
- "A.15 Lieferantenbeziehungen",
- "A.16 Management von Sicherheitsvorfällen",
- "A.17 Notfallmanagement",
- "A.18 Einhaltung gesetzlicher Anforderungen"

Im zweiten Schritt wurde für jede definierte Kategorie eine Kodierungsskala festgelegt, die den Bedeutungsgrad und die Priorität der jeweiligen Maßnahme innerhalb der Implementierung widerspiegelt. Die Skala erstreckt sich von 1 (geringe Relevanz) bis 10 (höchste Priorität), wodurch eine differenzierte Bewertung der Wichtigkeit einzelner Aspekte im Kontext der ISMS-Implementierung gemäß den Anforderungen des NIS-G ermöglicht wird. Diese quantifizierte Bewertung erlaubt eine strukturierte Vergleichbarkeit zwischen den Kategorien und trägt zur Identifikation von Schwerpunktbereichen und potenziellen Optimierungsfeldern bei.

Nach der Definition der Kategorien und der zugehörigen Kodierungsskala wurden die Interviewtranskripte nach Abschluss der Befragungen einer systematischen qualitativen Analyse unterzogen.

# 4. Herausforderungen und Chancen durch das NIS-G

## 4.1 Identifikation der größten Herausforderungen

Wie in der Hypothese dieser Arbeit ausgeführt, werden im Folgenden fünf sicherheitsrelevante Themenfelder als die zentralen Herausforderungen im Kontext der Umsetzung des Netz- und Informationssystemsicherheitsgesetzes (NIS-G) identifiziert. Damit lässt sich eine Wichtigkeit für die Umsetzung ableiten. Diese Themen decken sowohl technische, organisatorische als auch finanzielle Aspekte ab und korrespondieren direkt mit wesentlichen Maßnahmen aus Anhang A der ISO/IEC 27001:2022.

Die nachstehende Tabelle stellt die Zuordnung dieser Herausforderungen zu den entsprechenden Kontrollen der ISO/IEC 27001:2022 dar und beleuchtet typische Umsetzungsprobleme in der Praxis:

| **Nr.** | **Herausforderung** | **ISO/IEC 27001:2022 – Anhang A Control** | **Beschreibung der Maßnahme (Control)** | **Typische Umsetzungsprobleme / Herausforderungen** |
|---|---|---|---|---|
| 1 | Kryptographische Maßnahmen | A.8.24 – Kryptographie | Festlegung und Anwendung geeigneter kryptographischer Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen | Veraltete Algorithmen, unsicheres Schlüsselmanagement, fehlende Verschlüsselung bei ruhenden Daten |
| 2 | Handhabung technischer Schwachstellen | A.8.8 – Management von technischen Schwachstellen | Identifikation, Bewertung und Behandlung technischer Schwachstellen durch geeignete Prozesse | Fehlendes Patch-Management, keine Risikobewertung, unerkannte Sicherheitslücken |
| 3 | Datensicherung | A.8.13 – Sicherung von Informationen | Sicherstellung der Wiederherstell-barkeit von | Unzureichende Wiederherstellungstests, unverschlüsselte |

| | | | | |
|---|---|---|---|---|
| | | | Informationen durch regelmäßige Backups und Tests | Backups, fehlende RTO-/RPO-Konzepte |
| 4 | Schutz vor Schadsoftware | A.8.7 – Schutz vor Schadsoftware | Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Erkennung und Verhinderung von Malware | Veraltete AntiViren-Software, keine Mitarbeiterschulung, unzureichende Erkennung und Reaktion |
| 5 | Steuerung von Software im Betrieb | A.8.19 – Installation von Software | Kontrolle über die Installation von Software zur Vermeidung unerlaubter oder schädlicher Programme | Nutzer mit Adminrechten, fehlendes Whitelisting, keine Software-Inventarisierung |

## 4.2 Erfahrungsberichte der Betreiber (Ergebnisse der Befragungen)

Zur Analyse der praktischen Umsetzung der Anforderungen des Netz- und Informationssystemsicherheitsgesetzes (NIS-G) wurden im Rahmen dieser Arbeit 29 qualitative Befragungen unter Betreibern wesentlicher Dienste in Österreich durchgeführt. Die Teilnehmer setzten sich aus unterschiedlichen Branchen zusammen, darunter Energieversorgung, Gesundheitswesen, Finanzdienstleistungen sowie Transport und Verkehr. Ziel war es, ein möglichst breites Spektrum an Erfahrungen und Umsetzungsständen abzubilden.

Laut Angaben des Bundesministeriums für Inneres (BMI) gibt es aktuell 99 in Österreich gelistete Betreiber wesentlicher Dienste. Damit deckt diese Untersuchung etwa 29 % der Gesamtpopulation ab und bietet eine fundierte Grundlage, um zentrale Herausforderungen, Erfolgsfaktoren sowie Diskrepanzen bei der Umsetzung von Sicherheitsmaßnahmen gemäß ISO/IEC 27001:2022 zu identifizieren und zu bewerten. Die Ergebnisse sind somit als indikativ für bestehende Trends und Problemlagen im Bereich der nationalen Cybersicherheit zu verstehen.

Es wurde die Häufigkeit und Verteilung der Kategorien ausgewertet. Bzgl. der Häufigkeit wurden für alle Kategorien eine Aussage getroffen und es kann bei der weiteren Betrachtung immer von der Anzahl von 29 ausgegangen werden.

Die Tabelle zeigt die jeweiligen Kategorien mit der Anzahl und den kodierten Durchschnittswerten pro Kategorie. Die in der Hypothese angeführten fünf wichtigsten Sicherheitsmaßnahmen wurden in den jeweiligen Kategorien zugeordnet.

| **Kategorie (A.XX)** | **Anzahl** | **Durchschnitt (kodiert)** |
|---|---|---|
| A.5 Informationssicherheitsrichtlinien | 29 | 6,41379 |
| A.6 Organisation der Informationssicherheit | 29 | 5,89655 |
| A.7 Personalsicherheit | 29 | 6,03448 |
| A.8 Asset-Management | 29 | 6,20690 |
| A.9 Zugriffskontrolle | 29 | 5,58621 |
| A.10 Kryptographie | 29 | 6,82759 |
| 8.24 Verwendung von Kryptographie | | |
| A.11 Physische und umgebungsbezogene Sicherheit | 29 | 6,62069 |
| A.12 Betriebssicherheit | 29 | 5,68966 |
| 8.7 – Schutz vor Schadsoftware | | |
| 8.8 – Management von technischen Schwachstellen | | |
| 8.13 – Sicherung von Informationen | | |
| 8.19 – Installation von Software | | |
| A.13 Kommunikationssicherheit | 29 | 4,75862 |
| A.14 Systemerwerb, -entwicklung und -wartung | 29 | 5,20690 |
| A.15 Lieferantenbeziehungen | 29 | 4,82759 |
| A.16 Management von Sicherheitsvorfällen | 29 | 5,75862 |
| A.17 Notfallmanagement | 29 | 6,17241 |
| A.18 Einhaltung gesetzlicher Anforderungen | 29 | 5,93103 |

Basierend auf den kodierten Daten und unter Berücksichtigung des methodischen Rahmens der qualitativen Inhaltsanalyse nach Mayring lassen sich zu den einzelnen

Kategorien folgende wissenschaftlich-qualitative Aussagen treffen. Dabei werden sowohl die Kodierhäufigkeit (Anzahl der Nennungen) als auch die Durchschnittswerte der Kodierung berücksichtigt. Die Bewertungsskala reflektiert die Wichtigkeit der Kategorien für die Befragten.

Die Tabelle (wie oben) ist nach den Durchschnittswerten absteigend sortiert. Dies ergibt eine Reihenfolge, welche hier mit Rang bezeichnet wird:

| **Rang** | **Kategorie (A.XX)** | **Anzahl** | **Durchschnitt (kodiert)** |
|---|---|---|---|
| 1 | A.10 Kryptographie | 29 | 6,82759 |
| | 8.24 Verwendung von Kryptographie | | |
| 2 | A.11 Physische und umgebungsbezogene Sicherheit | 29 | 6,62069 |
| 3 | A.5 Informationssicherheitsrichtlinien | 29 | 6,41379 |
| 4 | A.8 Asset-Management | 29 | 6,2069 |
| 5 | A.17 Notfallmanagement | 29 | 6,17241 |
| 6 | A.7 Personalsicherheit | 29 | 6,03448 |
| 7 | A.18 Einhaltung gesetzlicher Anforderungen | 29 | 5,93103 |
| 8 | A.6 Organisation der Informationssicherheit | 29 | 5,89655 |
| 9 | A.16 Management von Sicherheitsvorfällen | 29 | 5,75862 |
| 10 | A.12 Betriebssicherheit | 29 | 5,68966 |
| | 8.7 – Schutz vor Schadsoftware | | |
| | 8.8 – Management von technischen Schwachstellen | | |
| | 8.13 – Sicherung von Informationen | | |
| | 8.19 – Installation von Software | | |
| 11 | A.9 Zugriffskontrolle | 29 | 5,58621 |

| | | | |
|---|---|---|---|
| 12 | A.14 Systemerwerb, -entwicklung und -wartung | 29 | 5,2069 |
| 13 | A.15 Lieferantenbeziehungen | 29 | 4,82759 |
| 14 | A.13 Kommunikationssicherheit | 29 | 4,75862 |

### 4.2.1 A.10 Kryptographie

Durchschnittswert: 6.83 (höchster Mittelwert aller Kategorien)

Die Kategorie „Kryptographie“ wurde besonders häufig und mit hoher Intensität thematisiert. Dies lässt auf eine ausgeprägte Wahrnehmung der Relevanz kryptographischer Verfahren schließen. In der Praxis bedeutet dies, dass Maßnahmen zur Datenverschlüsselung, Schutz sensibler Informationen und Schlüsselmanagement als zentrale Sicherheitsmaßnahmen wahrgenommen werden. Die hohe Bewertung weist auf eine starke Akzeptanz oder dringenden Handlungsbedarf hin.

### 4.2.2 A.11 Physische und umgebungsbezogene Sicherheit

Durchschnittswert: 6,62

Physische Sicherheitsmaßnahmen – wie Zugangskontrollen, Schutz vor Umweltgefahren (z. B. Feuer, Wasser) oder sichere Gebäudestrukturen – haben laut Aussage der Befragten eine bedeutende Rolle. Die hohe Bewertung kann darauf hinweisen, dass entsprechende Maßnahmen als etabliert, besonders wichtig oder verbesserungswürdig wahrgenommen werden. Diese Kategorie wird als grundlegende Voraussetzung für Gesamtsicherheit im Informationskontext verstanden.

### 4.2.3 A.5 Informationssicherheitsrichtlinien

Durchschnittswert: 6,41

Die Informationssicherheitsrichtlinien wurden in der Befragung als durchaus bedeutsam eingestuft. Der hohe Mittelwert weist darauf hin, dass in vielen Organisationen bereits verbindliche Regelungen zum Umgang mit Informationen etabliert wurden. Dies deutet auf ein breites Bewusstsein für die Notwendigkeit klarer Vorgaben hin, die Mitarbeitenden Orientierung bieten und sicherheitsrelevantes Verhalten steuern. Gleichzeitig lässt sich vermuten, dass in der Praxis regelmäßig an der Weiterentwicklung und Aktualisierung dieser Richtlinien gearbeitet wird. Themen wie Passwortmanagement, Rollen- und Berechtigungskonzepte oder Regelungen zum mobilen Arbeiten spielen dabei vermutlich eine zentrale Rolle.

### 4.2.4 A.12 Betriebssicherheit

Durchschnittswert: 5,69

Die Betriebssicherheit – also die Gewährleistung stabiler und verlässlicher IT-Dienste – wurde, wurde von den abgefragten auf Rang 10 thematisiert. Der niedrigere Mittelwert im Vergleich zu den anderen Kategorien deutet darauf hin, dass es hier Diskussions- oder Verbesserungsbedarf gibt. Eine Kluft zwischen Erwartung und Umsetzungsstand wird hier offenkundig. Aspekte wie Backup-Verfahren, Notfallplanung oder Systemverfügbarkeit dürften besonders relevant sein.

# 5. Diskussion

## 5.1 Synthese der Erfahrungen und Ergebnisse

### 5.1.1 Ziel der Analyse

Die durchgeführte qualitative Inhaltsanalyse nach Mayring diente der systematischen Auswertung von Experteninterviews mit Cybersicherheitsverantwortlichen aus Organisationen, die dem Netz- und Informationssystemsicherheitsgesetz (NISG) unterliegen. Ziel war es, die in der Hypothese definierten fünf prioritären Sicherheitsmaßnahmen gemäß EN ISO/IEC 27001 hinsichtlich ihrer praktischen Relevanz, Wirksamkeit und Umsetzungshürden zu untersuchen.

### 5.1.2 Bewertung der Sicherheitsmaßnahmen im Einzelnen

A. Kryptographie (A.10) – Durchschnitt: 6,83
   - Stellt zentrale technische Maßnahme zum Schutz von Vertraulichkeit, Integrität und Authentizität dar.
   - In vielen Organisationen durch Standardtechnologien (z. B. TLS, E-Mail-Verschlüsselung) bereits etabliert.
   - Von der ISO/IEC 27001 als kontrollierter Bereich gefordert, basierend auf einer Risikobewertung.
   - Hohe Bewertung resultiert aus technischer Verfügbarkeit, regulatorischer Notwendigkeit (z. B. DSGVO, NIS2) und praktischer Umsetzbarkeit.

B. Physische und umgebungsbezogene Sicherheit (A.11) – Durchschnitt: 6,62
   - Schutz vor unbefugtem physischem Zugriff, Diebstahl oder Umwelteinflüssen.
   - Umsetzung erfolgt häufig durch Zugangssysteme, Brandschutz, Videoüberwachung oder Klimasteuerung.
   - Nach ISO/IEC 27001 essenziell, da physische Schwachstellen andere Maßnahmen untergraben können.
   - Die hohe Bewertung weist auf breit akzeptierte und standardisierte Schutzmaßnahmen hin.

C. Informationssicherheitsrichtlinien (A.5) – Durchschnitt: 6,41
   - Bilden das strategische Fundament eines ISMS und sind explizit in der ISO/IEC 27001 gefordert.
   - Regeln verantwortliches Verhalten durch z. B. Passwortrichtlinien, IT-Nutzungsrichtlinien oder Datenschutzleitlinien.
   - Tragen zur Etablierung einer Sicherheitskultur und zur erfolgreichen Auditierung bei.
   - Die Bewertung spiegelt das Bewusstsein für Governance und interne Steuerung wider.

D. Asset-Management (A.08) – Durchschnitt 6,21
   - Grundlage für Risikomanagement: Asset-Management stellt sicher, dass alle relevanten Informationswerte identifiziert und klassifiziert werden – eine notwendige Voraussetzung für eine wirksame Risikoanalyse im ISMS.
   - Zuweisung von Verantwortlichkeiten: Durch die eindeutige Zuordnung von Eigentümern zu Assets wird Verantwortung geschaffen, was die Umsetzung von Schutzmaßnahmen unterstützt.
   - Transparenz über Schutzbedarf: Die strukturierte Erfassung und Bewertung von Informationswerten ermöglicht die Ableitung geeigneter Sicherheitsmaßnahmen entsprechend ihrer Kritikalität.
   - Integration in Sicherheitsprozesse: Asset-Management schafft die organisatorische und technische Basis, um weitere Anforderungen der ISO/IEC 27001 wie Zugriffskontrolle, Incident Management oder Business Continuity umzusetzen.

E. Notfallmanagement (A.17) – Durchschnitt 6,17
   - Aufrechterhaltung der Geschäftskontinuität: Notfallmanagement sorgt dafür, dass kritische Geschäftsprozesse auch bei Störungen oder Ausfällen fortgeführt oder schnell wiederhergestellt werden können.
   - Minimierung von Schäden: Durch vorbereitete Notfallpläne und Wiederanlaufstrategien können Auswirkungen auf Informationssicherheit, Verfügbarkeit und Integrität gezielt begrenzt werden.
   - Verankerung von Verantwortlichkeiten und Prozessen: Klare Zuständigkeiten, strukturierte Abläufe und regelmäßige Tests stärken die Reaktionsfähigkeit im Krisenfall.
   - Pflichtbestandteil des ISMS: Notfallmanagement ist in der ISO/IEC 27001 (insbesondere Anhang A.5.29, A.17) ein verpflichtender Bestandteil und trägt wesentlich zur Resilienz des Unternehmens bei.

### 5.1.3 Einflussfaktoren auf die Umsetzung

Die qualitative Analyse macht deutlich, dass neben der rein technischen Dimension auch andere Faktoren eine zentrale Rolle spielen:

| **Einflussfaktor** | **Beschreibung** |
|---|---|
| Wirtschaftlich | Investitionen in Sicherheitslösungen oft budgetabhängig |
| Regulatorisch | Unsicherheit durch komplexe Vorgaben und uneinheitliche Auslegung des NISG |
| Betrieblich-organisatorisch | Hürden in der Abstimmung zwischen IT, OT und Management |

### 5.1.4 Gesamteinschätzung

Die Ergebnisse bestätigen die Hypothese nicht: Kryptographische Maßnahmen zählen zu den am stärksten priorisierten Sicherheitsmaßnahmen. Bei der Handhabung technischer Schwachstellen, Datensicherung und Schutz vor Schadsoftware und der Steuerung von Software im Betrieb zeigen sich hingegen deutliche Umsetzungsdefizite und strukturelle Hürden. Auffällig ist, dass Maßnahmen mit klar erkennbarem Nutzen und direkter technischer Wirkung bevorzugt werden, während prozessuale Aspekte tendenziell weniger konsequent berücksichtigt werden.

Die Analyse macht deutlich, dass eine wirkungsvolle Umsetzung der NISG-Anforderungen nicht nur technisches Know-how, sondern auch klare organisatorische Zuständigkeiten, Ressourcen und eine strategische Sicherheitskultur voraussetzt. Damit liefern die Interviews nicht nur ein realistisches Bild aktueller Sicherheitspraktiken, sondern auch konkrete Hinweise auf Verbesserungsmöglichkeiten und Entwicklungsbedarf im Hinblick auf die Umsetzung des NISG und der kommenden NIS2-Anforderungen.

# 6. Fazit und Ausblick

## 6.1 Zusammenfassung der zentralen Erkenntnisse

Die Umsetzung des NIS-G zeigt, dass sich Betreiber wesentlicher Dienste stark an den Anforderungen der EN ISO/IEC 27001 orientieren, um ihre Sicherheitsmaßnahmen zu strukturieren. Die Sicherheitsmaßnahme – Kryptographische Maßnahmen (A.10) spielen ein zentrale Rolle. Die restlichen, in der Hypothese formulierten vier Sicherheitsmaßnahmen - Handhabung technischer Schwachstellen, Datensicherung, Schutz vor Schadsoftware und Steuerung von Software im Betrieb – spielen eine untergeordnete Rolle in den Sicherheitsstrategien der Unternehmen. Die Einführung von Informationssicherheits-Managementsystemen (ISMS) hat dazu beigetragen, dass Maßnahmen systematisch umgesetzt wurden und kontinuierlich verbessert werden. Dazu zählen Maßnahmen zur Physische und umgebungsbezogene Sicherheit (A.11).

Ein methodischer Zugang lässt sich daraus ableiten, dass die Unternehmen mit der Erstellung von Informationssicherheitsrichtlinien (A.5) begonnen haben. Diese stellen ein strategisches Fundament eines ISMS dar.

Die Integration der in der Hypothese angeführten fünf Sicherheitsmaßnahmen variieren zwar je nach Sektor und technologischem Reifegrad der Organisationen. Kryptographische Maßnahmen wurden insbesondere im Gesundheits- und Finanzsektor intensiv umgesetzt, um sensible Daten vor unbefugtem Zugriff zu schützen.

## 6.2 Beantwortung der Forschungsfrage

Die Auswertung der Befragungsergebnisse im Rahmen dieser Arbeit zeigt, dass bei Betreibern wesentlicher Dienste insbesondere solche Sicherheitsmaßnahmen bevorzugt zur Anwendung kommen, die technisch greifbar, normativ klar definiert und in der Praxis gut umsetzbar sind. Unter Berücksichtigung der Anforderungen der EN ISO/IEC 27001 konnten folgende fünf Maßnahmen als besonders relevant identifiziert werden:

1. Kryptographie (A.10)

Kryptographische Verfahren wurden mit Abstand am höchsten bewertet. Sie dienen dem Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen und sind in vielen Organisationen bereits technisch etabliert – etwa durch Verschlüsselung von Datenübertragungen und Speichermedien. Die ISO/IEC 27001 fordert explizit die risikobasierte Anwendung kryptographischer Kontrollen.

2. Physische und umgebungsbezogene Sicherheit (A.11)

Maßnahmen wie Zutrittskontrollen, Klimatisierung oder Brandschutz tragen wesentlich zum Schutz von Informationswerten bei. Sie gelten als Grundvoraussetzung für die Effektivität weiterer Kontrollen und sind aufgrund ihrer Standardisierbarkeit gut implementierbar.

3. Informationssicherheitsrichtlinien (A.5)

Die Erstellung und Pflege formalisierter Richtlinien stellt eine zentrale Anforderung der ISO/IEC 27001 dar. In der Praxis haben viele Betreiber bereits entsprechende Regelwerke etabliert, die Verhaltensvorgaben, Verantwortlichkeiten und Sicherheitsziele definieren.

4. Asset-Management (A.08)

Das Asset-Management (A.8) ist eine grundlegende Maßnahme im Rahmen der ISO/IEC 27001 und dient der strukturierten Erfassung, Klassifikation und Verwaltung von Informationswerten. Die Befragung zeigt, dass diese Maßnahme in der Praxis gut umgesetzt wird und eine wichtige Basis für andere Sicherheitsprozesse bildet. Durch die Zuweisung von Verantwortlichkeiten und die Schaffung von Transparenz ermöglicht Asset-Management eine gezielte Risikobewertung und effektive Schutzmaßnahmen.

5. Notfallmanagement (A.17)

Die Fähigkeit, bei sicherheitsrelevanten Vorfällen oder Betriebsunterbrechungen handlungsfähig zu bleiben, wird zunehmend als kritischer Erfolgsfaktor gesehen. Maßnahmen wie Wiederanlaufpläne oder Notfallhandbücher sind daher in vielen Organisationen bereits Bestandteil des ISMS

Es lässt sich feststellen, dass sich die bevorzugt eingesetzten Maßnahmen stark an der technischen und organisatorischen Umsetzbarkeit sowie an der normativen Klarheit der ISO/IEC 27001 orientieren. Während Kryptographie als klar dominierende Maßnahme hervorsticht, zeigt sich bei anderen Bereichen ein mittlerer Reifegrad mit erkennbarem Verbesserungspotenzial – insbesondere im Hinblick auf prozessuale und strategische Maßnahmen, wie etwa dem Lieferantenmanagement und der Kommunikations-sicherheit.

## 6.3 Ausblick auf zukünftige Entwicklungen in der Netz- und Informationssicherheit

Die im Rahmen dieser Arbeit gewonnenen Erkenntnisse zeigen deutlich, dass von den abgefragten Sicherheitsmaßnahmen lediglich Kryptographie als durchgehend anerkannte und in der Praxis umgesetzte Maßnahme bewertet wurde. Mit einem signifikant höheren Durchschnittswert im Vergleich zu allen anderen Kategorien stellt sie die einzige Schutzmaßnahme dar, deren Relevanz und Implementierungsgrad im Rahmen der Befragung konsistent bestätigt wurden.

Demgegenüber erhielten andere Sicherheitsmaßnahmen – etwa organisatorische Prozesse – niedrigere Bewertungen. Dies lässt darauf schließen, dass deren praktische Umsetzung derzeit entweder noch im Aufbau ist oder ihnen in der betrieblichen Praxis bislang eine nachgeordnete Bedeutung beigemessen wird. Insbesondere prozessuale und strukturell komplexere Anforderungen, wie Schwachstellenmanagement oder Softwaresteuerung, scheinen mit organisatorischen Hürden verbunden zu sein.

Vor dem Hintergrund der bevorstehenden gesetzlichen Verschärfungen – insbesondere durch die NIS2-Richtlinie und deren nationale Umsetzung im Rahmen des novellierten Netz- und Informationssystemsicherheitsgesetzes (NISG) – wird es für Betreiber wesentlicher Dienste künftig jedoch unumgänglich sein, auch diese bislang unterbewerteten Maßnahmen systematisch zu integrieren. Die Verpflichtung zum Betrieb eines vollständigen Informationssicherheitsmanagementsystems sowie die Anforderungen an kontinuierliche Überwachung, Wirksamkeitsprüfung und Dokumentation werden zentrale Stellschrauben der regulatorischen Weiterentwicklung sein. Künftig wird verstärkt auf Nachweispflichten, erweiterte Meldepflichten und die persönliche Verantwortung von Führungskräften abzustellen sein – ein klarer Hinweis darauf, dass Informationssicherheit nicht mehr punktuell, sondern ganzheitlich und strategisch betrachtet werden muss.

In diesem Zusammenhang gewinnt auch die Rolle des Chief Information Security Officer (CISO) zunehmend an Bedeutung. Als zentrale Ansprechperson für alle Belange der Informationssicherheit ist der CISO maßgeblich dafür verantwortlich, die Umsetzung regulatorischer Anforderungen zu steuern, Sicherheitsprozesse unternehmensweit zu verankern und das Bewusstsein für Informationssicherheit auf Managementebene zu stärken. Der CISO wird damit zu einer Schlüsselrolle im Spannungsfeld zwischen operativer Umsetzung, strategischer Ausrichtung und gesetzlicher Compliance.

# Literaturverzeichnis


Blauensteiner, P. (2022), Präsentation: Rückblick NIS1 - Ausblick NIS2, Bundesministerium für Inneres (BMI)

Böhm, F. (2014). Kritische Infrastrukturen: Risiko-, Krisen- und Notfallmanagement. Springer Vieweg.

Brenner, M., gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., & Schaaf, T. (2024). Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung. Springer.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023) *Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheits-Managementsysteme.* Verfügbar unter: https://netzwerke.bam.de/Netzwerke/Content/DE/Downloads/qi-fokus-studie-zur-iso-iec-27001.pdf (Zugriff am: 24.02.2025)

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2021): Die Themen des 17. Deutschen IT-Sicherheitskongresses. BSI, Bonn. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Konferenzen/ITSicherheitskongress/17/17-deutscher-it-sicherheitskongress.html (Zugriff am: 24.02.2025)

Europäische Union, Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz des Finanzsektors, ABl. L 333/1 vom 27.12.2022.

Fischer, T. (2015). IT-Sicherheit kompakt: Grundlagen und Praxiswissen. Hanser.

Hasan, K., Hossain, F., Amin, A., Sutradhar, Y., Jeny, I. J., & Mahmud, S. (2025). Enhancing proactive cyber defense: A theoretical framework for AI-driven predictive cyber threat intelligence. Journal of Technologies Information and Communication, 5(1), 33122.

Hämmerli, B. (2015). Schutz Kritischer Infrastrukturen: Herausforderungen und Strategien. Springer.

INDUSTRIE.DE, (2024), https://industrie.de/cybersecurity/die-effektivitaet-von-cybersicherheitstrainings/ (Zugriff am: 03.04.2025)

ISO/IEC (2022): ISO/IEC 27001:2022, Anhang A – Information security controls. International Organization for Standardization, Genf.

Kersten, H., & Schröder, K. W. (2023). ISO 27001: 2022/2023. Springer.

Kleinhans, D. (2016). Resilienz Kritischer Infrastrukturen: Konzepte und Anwendungen. Springer Vieweg.

National Institute of Standards and Technology (NIST) (2018): Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, Gaithersburg, MD.
Verfügbar unter: https://doi.org/10.6028/NIST.CSWP.04162018 [Zugriff am: 24.02.2025]

National Institute of Standards and Technology (NIST) (2021) *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, Special Publication 800-183.

Pohlmann, N. (2014). Cyber-Sicherheit: Aktuelle Bedrohungen und Trends. Springer Vieweg.

Rudolph, J. (2013). Stand der Forschung zur Informationssicherheit in Kritischen Infrastrukturen. Springer Vieweg.

Schneider, J. (2017). Grundlagen der Informationssicherheit: Eine praxisorientierte Einführung. Springer Vieweg.

Schryen, G. (2013). Informationssicherheit: Ökonomische Aspekte und Implikationen. Springer.

Schulze, A., & Wollinger, G. R. (2020). Handbuch Cybersecurity für die öffentliche Verwaltung. Kommunal- und Schul-Verlag.

Steiger, S. (2022). Cybersicherheit in Innen- und Außenpolitik: Deutsche und britische Policies im Vergleich. transcript Verlag.

Tjader & Thomas (2021): Best Practices zur Einführung eines ISMS nach ISO/IEC 27001: Erfolgsfaktoren und Herausforderungen in der Praxis. IT-Governance Journal, 14(2), 45-63.

Voigt, P., & Bussche, A. (2024). EU-Datenschutz-Grundverordnung (DSGVO). Springer Berlin Heidelberg.

Weber, R. H. (2014). Internet of Things: Neue Herausforderungen für die Informationssicherheit. Springer.

Wegener & Mikos, 2017, S. 63-65 Qualitative Medienforschung. utb GmbH.