FERDINAND PORSCHE
FERN FH

Auswirkungen der „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ auf die Betreiber wesentlicher Dienste in Österreich

Masterarbeit

eingereicht von: **Walter Müllner, BA MSc**
Matrikelnummer: 1510471034

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH Gesellschaft zur Erhaltung und Durchführung von Fachhochschul-Studiengängen

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Dipl.-Betrw. (FH) Marcus Römer, MSc

Zweitgutachten: Dipl.-Ing. Thomas Gyoergyfalvay, BA MBA

Wiener Neustadt, Mai 2018

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit 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 Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, Juni 2018 _____

Unterschrift

Kurzzusammenfassung: Auswirkungen der „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ auf die Betreiber wesentlicher Dienste in Österreich

Die heutige Gesellschaft ist zunehmend von speziellen Infrastrukturen und Services abhängig. Um den digitalen Fortschritt auch weiterhin gewährleisten zu können, ist der Schutz dieser kritischen Infrastrukturen, die stark von Informations- und Kommunikationstechnologien abhängig sind, von zentraler Bedeutung. Um den rasanten Anstieg von Cybervorfällen entgegenzuwirken und Schaden einzudämmen, wurde 2016 die „EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-Richtlinie) beschlossen. Was für technische und organisatorische Maßnahmen sich als Auswirkungen für betroffene Unternehmen in Österreich ergeben und welche Steuerungsmöglichkeiten zu schaffen sind, wird in dieser Masterarbeit erarbeitet.

Um diese Maßnahmen zu identifizieren wird a) eine Literaturrecherche durchgeführt, in der auf bestehende (inter-)nationale Vorschriften, Normen und Standards referenziert wird. b) Damit Unternehmen eine Steuerung ermöglicht wird, ist zu diesem Zweck als Prototyp ein „Self Assessment für NIS-Readiness“ entwickelt worden. c) Dieser Prototyp wird sechs ExpertInnen vorgestellt und einer kritischen Betrachtung, mit folgender Befragung, unterzogen. d) Im Rahmen zweier Feldexperimente (mit zwei österreichischen, (in-)direkt betroffenen Unternehmen) wird die Anwendbarkeit des Prototyps verprobt.

Als Ergebnis der Forschungen sind 26 spezifische Themen aus 11 Bereichen abgeleitet, die als Auswirkungen zu berücksichtigen sind. Weiters ist der Prototyp eines bewerteten und auf Praxistauglichkeit verprobten „Self Assessment für NIS-Readiness“ vorhanden, auf dessen Basis Unternehmen in Österreich die Auswirkungen der NIS-Richtlinie identifizieren, sowie daraus entstehende Maßnahmen etablieren und steuern können.

Schlagwörter: NIS-Richtlinie, Cybersicherheit, Self Assessment für NIS-Readiness, Netz- und Informationssysteme, Kritische Infrastruktur, Betreiber wesentlicher Dienste, IT-Service Provider

Abstract: Impact of the „Directive concerning measures for a high common level of security of network and information systems across the Union“ on operators of essential services in Austria

Today's society is increasingly dependent on special infrastructures and services. The protection of these critical infrastructures, which depend heavily on information and communication technologies, is essential to ensure that digital progress continues. In order to counteract the rapid increase in cyber incidents and contain damage, the "EU Directive concerning measures for a high common level of security of network and information systems across the Union" (NIS Directive) was adopted in 2016. The technical and organizational measures that will have an impact on the companies concerned in Austria and the control options to be created will be developed in this master thesis.

In order to identify these measures, a) a literature research will be carried out in which references are made to existing (inter-)national regulations, norms and standards. b) A "Self assessment for NIS Readiness" will be developed for this purpose as a prototype to enable companies to control the process. c) This prototype will be presented to six experts and subjected to a critical examination, with the following survey. d) The applicability of the prototype will be tested in two field experiments (with two Austrian (in-)directly affected companies).

As a result of the research 26 specific topics from 11 areas are derived, which are to be considered as effects. Furthermore, the prototype of an evaluated "Self Assessment for NIS Readiness", which has been tested in practice, is available on the basis of which companies in Austria can identify the effects of the NIS Directive and establish and control the resulting measures.

Keywords: NIS Directive, cybersecurity, Self Assessment for NIS-Readiness, network and information systems, critical infrastructure, operators of essential services, IT-service provider

Danksagung

Die Strapazen dieses Studium zu absolvieren haben sich auf jeden Fall gelohnt und sind ein weiterer Meilenstein auf dem persönlichen Lebensweg, der hoffentlich noch viele Überraschungen bereithalten wird. Die folgenden Worte sollen Ausdruck meines zutiefst empfunden Danks an meine verständnisvolle Ehefrau, wie auch meine Verwandten und Freunde sein.

Mein großer Dank gilt vor allem meiner Ehefrau Chantal für die moralische wie auch fachliche Unterstützung in den fordernden Monaten dieses Studiums. Sie diente mir als Inspiration und Stütze in den jeweiligen schwierigen Momenten. Durch Ihr stets optimistisches Naturell und die Ausdauer konnten unüberwindlich wirkende Hürden spielerisch genommen werden.

Meinem Vater Herbert kann ich hier leider nur mehr im Nachhinein Dank sagen und die vollste Bewunderung aussprechen, für alles was er mir gemeinsam mit meiner Mutter ermöglichte und mit auf den Lebensweg gegeben hat. In Erinnerung bleiben all die unauslöschlichen Momente, die wir gemeinsam erleben durften. Aus tiefstem Herzen bedanke ich mich bei meiner Mutter Marianne für die Geduld und das Verständnis, wenn es in manchen Zeiten auch schwieriger war.

Meinen Betreuern Marcus Römer und Thomas Gyoergyfalvay möchte ich ebenfalls besonderen Dank ausdrücken, da Ihre eingebrachten Expertisen und Ratschläge einen großen Beitrag zum Gelingen lieferten. Ich rechne vor allem Marcus Römer die Bereitschaft hoch an, sich der Betreuung neben Job und Privatleben anzunehmen.

Last but not least, möchte ich allen mitwirkenden ExpertInnen der Befragungen meinen Dank aussprechen. Die persönliche Fachkenntnis zu teilen und eigene Freizeit zu opfern, haben einen wesentlichen Beitrag zur inhaltlichen Qualität der Masterarbeit beigetragen. Ich war beeindruckt von dem außergewöhnlich hohen Wissen zu diesem Thema und der entgegengebrachten Offenheit meinen Anliegen gegenüber.

„*Keine Zukunft vermag gutzumachen, was du in der Gegenwart versäumst.*“
(Albert Schweitzer, 1875 - 1965)

Inhaltsverzeichnis

1. Einleitung

Um die Bedeutung und den nunmehr langen Weg des Themas zu verdeutlichen, sind folgend zwei Zitate hochrangiger politischer VertreterInnen festgehalten. Die für Inneres zuständige Kommissarin Cecilia Malmström sagte dazu:

> *„Das Verbrechen geht neue Wege. Mithilfe von Schadsoftware ist es möglich, die Kontrolle über eine große Zahl von Computern zu gewinnen und Kreditkartennummern zu stehlen, sensible Informationen ausfindig zu machen und Großangriffe zu starten.[...] Die Vorschläge, die wir heute vorlegen, sind ein wichtiger Schritt [...].“*[1]

Zur gleichen Zeit gab die für die digitale Agenda zuständige Vizepräsidentin der Kommission, Neelie Kroes, folgendes Statement ab:

> *„Online-Bedrohungen kennen keine Grenzen. [...] Unsere EU-Organe und Regierungen müssen sehr eng zusammenarbeiten, damit wir die Art und das Ausmaß der neuen Online-Bedrohungen verstehen lernen.“*[2]

Die folgenden Unterkapitel geben Einblicke in die Zielsetzung der Masterarbeit, wie methodisch diese Arbeit umgesetzt wurde und welche speziellen Rahmenbedingungen zu berücksichtigen waren.

1.1 Hintergrund der Arbeit

Durch den rasanten digitalen Fortschritt ist die heutige Gesellschaft zunehmend von speziellen Technologien, Infrastrukturen und Services abhängig. Dabei ist es nahezu nebensächlich, ob es sich beispielsweise um die Versorgung mit Wasser, Energie, Telekommunikation oder Finanzdienstleistungen handelt. Diese und weitere Bereiche, sind in Fachkreisen als „kritische Infrastrukturen“ (KI) bekannt. Eine Störung kann sich bereits schwerwiegend und direkt auf viele Menschen, bzw. die Gesellschaft auswirken. Zahllose Dienste sind heutzutage hochgradig abhängig von „Informations- und Kommunikationstechnologien“ (IKT). Die Informationstechnologie (IT) mit den vielen (un-)sichtbaren Systemen wurde zu einem zentralen Kernelement der globalisierten Welt.

Doch wo Licht ist, ist auch Schatten: Die Gefahr von Cyberattacken und daraus resultierender Schaden haben in den letzten Jahren zugenommen. Es ist vorhersehbar, dass Cyberangriffe auch weiterhin eines der großen Risiken für Bevölkerung, Wirtschaft und Ökonomie darstellen wird. Belegt werden kann dies mittels dem jährlichen „Allianz Risk Barometer“. Diesem zufolge landen 2017 „Cybervorfälle“ auf Platz 3 der globalen

---

[1] (TeleTrusT – Bundesverband IT-Sicherheit e.V., 2010, online)

[2] (TeleTrusT – Bundesverband IT-Sicherheit e.V., 2010, online)

Geschäftsrisiken. Dabei bestätigten 30% der befragten Personen, dass Cyberangriffe ein ernsthaftes Risiko darstellen und diese eine steigende Tendenz aufweisen.[3]

Zur Verdeutlichung der erwarteten Schadenssummen. Im „Official 2017 Annual Cybercrime Report" des US-Analystenhauses „Cybersecurity Ventures" werden global für 2021 bereits sechs Billionen US-Dollar an Schaden durch Cybercrime prognostiziert. Das sind fast 10% der weltweiten Wirtschaftsleistung des Jahres 2017.[4] Auf die Europäische Union (EU) umgelegt, erklärte Matti Maasikas, estnischer stellvertretender Minister für Europaangelegenheiten, folgendes.

> "*Cyberkriminalität und staatlich unterstützte böswillige Cyberaktivitäten zählen zu den größten globalen Bedrohungen für unsere Gesellschaften und Volkswirtschaften. Weltweit verlieren wir bereits rund 400 Mrd. EUR jährlich aufgrund von Cyberangriffen.* [...] *Die EU muss ihren Angreifern immer einen Schritt voraus sein*"[5]

Um dieser Situation entgegenwirken zu können, ist es von Seiten des Staats bzw. der Gemeinschaft erforderlich entsprechende Aktionen zu setzen und sich der Verantwortung zu stellen. Als entsprechende Maßnahme wurde die „Richtlinie (EU) 2016/1148 des Europäischen Parlaments (EP) und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (in Folge NIS-Richtlinie) gemäß dem ordentlichen Gesetzgebungsverfahren am 6. Juli 2016 beschlossen.[6] Diese NIS-Richtlinie ist ein wichtiger Schritt, um für die EU eine Steigerung des allgemeinen Niveaus der Netz- und Informationssicherheit zu forcieren und das weitere Funktionieren des Binnenmarktes zu unterstützen.

1.2 Ausgangslage

Cyberaktivitäten mit kriminellem oder bösartigem Hintergrund stellen nicht nur eine Bedrohung für die einzelnen Staaten und die Bestrebungen zum Aufbau des digitalen Binnenmarktes dar, sondern können auch als Gefahr für das Funktionieren der Demokratien, der Freiheiten und der Werte angesehen werden. Eine künftige Sicherheit ist stark davon abhängig, inwieweit es den Gesetzgebern gelingt, die EU bzw. die einzelnen Mitglieder vor Cyberbedrohungen zu schützen:[7]

Studien zeigen, dass die Risiken in Bezug auf Cyberbedrohungen exponentiell anwachsen. Dabei hat die Verbreitung von Ransomware stark zugenommen, was der Anstieg an Angriffen 2017 (z.B. WannaCry, Petya) dramatisch symbolisiert.[8] Wobei Ransomware bei Weitem nicht die einzige und auch nicht größte Bedrohung darstellt (vgl. Abbildung 1).

---

[3] Vgl. (Allianz Global Corporate & Specialty SE 2017, S. 2)

[4] Vgl. (Cybersecurity Ventures 2017, S. 3)

[5] (Council of the EU 2017, S. 1)

[6] Vgl. (Amtsblatt der Europäischen Union 2016, S. 1)

[7] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 2)

[8] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 2)

Gemäß dem „Threat Landscape Report 2017" der "European Union Agency for Network and Information Security" (ENISA) ist die Bedrohung durch „Malware" weiterhin an erster Stelle, gefolgt von „Web based attacks" (vgl. Abbildung 1).

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware		→
2. Web based attacks	↑	2. Web based attacks		→
3. Web application attacks	↑	3. Web application attacks		→
4. Denial of service	↑	4. Phishing		↑
5. Botnets	↑	5. Spam		↑
6. Phishing	⊃	6. Denial of service		↓
7. Spam	↓	7. Ransomware		↑
8. Ransomware	⊃	8. Botnets		↓
9. Insider threat	⊃	9. Insider threat		→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss		→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Abbildung 1: Top 10 und Vergleich der IT-Bedrohungslandkarte 2017 vs. 2016[9]

All diese Bedrohungen können sowohl von privaten, kommerziellen wie auch staatlichen AkteurInnen ausgehen. Zwischen „traditioneller" Kriminalität und Cybercrime findet zunehmend ein fließender Übergang statt. Diese kriminelle Bedrohung wird zusätzlich verstärkt, da das Internet als Medium zur Ausweitung der Aktivitäten als auch für die Suche nach neuen kriminellen Methoden eingesetzt werden kann. Staatliche Akteure verfolgen eigene geopolitische Ziele immer öfter nicht nur mittels „klassischer Mittel", wie militärischer Gewalt, sondern auch mittels Cyberaktivitäten. Den zunehmenden Desinformationskampagnen, gezielten Falschmeldungen und auf KI´s ausgerichteten Cyberangriffen ist entsprechend zu begegnen. Sollte es der EU bzw. den Mitgliedern nicht gelingen, die Cybersicherheit zu steigern, wird die Bedrohungslage noch mehr anwachsen.[10]

Gemäß einer im Auftrag der Europäischen Kommission durchgeführten Studie, könnten bereits im Jahr 2020 Milliarden Geräte in das „Internet of Things" integriert sein. Dabei nimmt Cybersicherheit keine besondere Priorität ein.[11] Dabei handelt es sich bei den Geräten unter anderem um jene, die z.B. (Ab-)Wassernetze, Stromnetze, Finanzsysteme, Wohnungen und Spitäler steuern. Wenn diese nicht adäquat geschützt werden können, so kann das drastische Folgen haben und das Anwendervertrauen massiv beeinflussen. Die

[9] (ENISA 2018, S. 9)

[10] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 2f)

[11] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 3)

aktuelle, über viele Jahre entwickelte Strategie der EU soll dazu einen Beitrag in folgenden Bereichen liefern:

- Erhöhung der Abwehrfähigkeit und der strategischen Autonomie,
- Steigerung technologischer Kapazitäten und Kompetenzen,
- Förderung des Aufbaus eines soliden Binnenmarktes.[12]

Dafür ist, unter Einbindung aller wichtigen Akteure, ein hohes Maß an Cybersicherheit zu schaffen, damit im Bedarfsfall wirksam reagiert werden kann. Die NIS-Richtlinie ist hierbei ein zentrales Element um Lösungen zu vielen der Fragen oder Ideen zu liefern. Es handelt sich um die erste unionsweite Rechtsvorschrift zur Cybersicherheit. Sie dient dem Aufbau von Abwehrfähigkeiten, indem etwa:

- nationale Cybersicherheitskapazitäten gestärkt werden,
- eine bessere Zusammenarbeit zwischen Mitgliedstaaten gefördert wird,
- Unternehmen wichtiger Wirtschaftssektoren wirksame Risikomanagement Verfahren einzuführen haben,
- schwere Sicherheitsvorfälle den nationalen Behörden zu melden sind.[13]

Die Mitgliedstaaten sollen dabei weiterhin für die eigene nationale Sicherheit verantwortlich bleiben. Jedoch sprechen der grenzüberschreitende Bedrohungscharakter und die Komplexität dafür, dass die EU tätig werden muss und im Bedarfsfall Unterstützung bieten sollte, sowie relevante Kompetenzen auf EU-Ebene aufbaut. Schlussendlich setzt sich die EU durch die Bekämpfung aktueller und künftiger Cyberbedrohungen proaktiv für die Sicherung des Wohlstands, der Gesellschaft und der Werte sowie der Grundrechte und -freiheiten in Europa ein, anstatt nur rückwirkend auf Vorfälle zu reagieren.[14]

Um diese Aufgaben und Anforderungen auf nationaler Ebene umsetzen zu können, bedarf es einer nationalen Strategie für die Sicherheit von „Netz- und Informationssystemen" (NIS), die jeder Mitgliedsstaat für sich festzulegen hat. Das österreichische Gesetz, welches auf Basis der NIS-Richtlinie noch zu erarbeiten ist, hatte dazu in den letzten Jahren eine Vielzahl an Arbeitstiteln. Nachfolgend eine Auswahl der Bezeichnungen, die als synonym zu verstehen sind:

- Cyber Sicherheitsgesetz[15] (in diversen Schreibweisen)
- IT-Sicherheitsgesetz[16]
- Netz- und Informationssystemsicherheitsgesetz[17]

Ein Arbeitsentwurfsauszug vom 17.10.2017 zum österreichischen Bundesgesetz deutet darauf hin, dass ein zukünftiges Gesetz als „Netz- und Informationssystemsicherheits-

[12] (EUROPÄISCHE KOMMISSION 2017, S. 3)

[13] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 8)

[14] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 2ff)

[15] Vgl. (CERT.at 2017, S. 6)

[16] Vgl. (Cyber Security Austria 2012, online)

[17] Vgl. (A-SIT Plus GmbH 2017, S. 22)

gesetz“ (NISG) erlassen wird. Somit wird im Rahmen der Masterarbeit die Abkürzung NISG für das österreichische Gesetz zur NIS-Richtlinie verwendet.

1.3 Aufbau der Arbeit

Die Masterarbeit besteht aus 4 Kapiteln. Das Kapitel 1 gibt einen Einblick in die Relevanz des Themas, erläutert die Forschungsfragen und zeigt die methodische Herangehensweise zur Beantwortung auf.

In Kapitel 2 werden Definitionen und Erklärungen aus den Bereichen wie z.B. IKT, Informationssicherheit, (inter-)nationale Standards gegeben. Zudem wird der Status Quo zur Umsetzung der NIS-Richtlinie beschrieben. Es wird ein kurz- bis mittelfristiger Ausblick gegeben, sowie ein spezifischer Vergleich der beiden Länder Österreich und Deutschland hinsichtlich dieser Materie durchgeführt.

Das Kapitel 3 stellt mit dem selbstentwickelten Prototyp des „Self Assessment für NIS-Readiness“, den ExpertInnenbefragungen und durchgeführten Feldexperimenten (als empirischen Teil und dem persönlichen wissenschaftlichen Beitrag) das Herzstück der Masterarbeit dar. Zu diesem Zweck wird auf die angewendete Methodik eingegangen, ein Einblick in die Entwicklung und Struktur des Self Assessments gegeben und die Durchführung der Befragungen und Feldexperimente erläutert. Zudem wird die Auswertung, Analyse und Interpretation der Resultate aus ExpertInnenbefragungen bzw. Feldexperimenten vorgenommen. Es werden entsprechenden Erkenntnisse gewonnen und ein aussagekräftiger Bezug zu den Forschungsfragen bzw. Hypothesen hergestellt.

Im finalen Kapitel 4 werden gewonnene Erkenntnisse aus Theorie und Empirie zusammengefasst, die in Kapitel 1.4 gestellten Forschungsfragen und die Hypothesen aus Kapitel 1.5 beantwortet, sowie Empfehlungen für weiterführende Studien festgehalten. Ein Ausblick auf die zukünftige Entwicklung schließt dieses Kapitel und Masterarbeit ab.

Der Anhang A enthält den vollumfänglichen Prototyp des „Self Assessment für NIS-Readiness“. Der Anhang B enthält den Fragebogen und die Detailantworten der sechs ExpertInnenbefragungen. Der Anhang C enthält die Resultate der beiden, auf Basis des Prototyps, durchgeführten Feldexperimente.

1.4 Forschungsfragen

Obwohl die NIS-Richtlinie, verglichen mit beispielsweise der EU- „Datenschutz-Grundverordnung“ (DSGVO), nicht so intensiv in der Öffentlichkeit diskutiert wird, sollen in der Masterarbeit die Auswirkungen auf betroffene Unternehmen untersucht werden.

Forschungsfrage:

F 1. Welche technischen und organisatorischen Auswirkungen werden sich durch das Inkrafttreten der NIS-Richtlinie auf die betroffenen IT-Service Provider in Österreich sowie „Betreiber wesentlicher Dienste“ ergeben?

Um diese Forschungsfrage gründlich zu beantworten, ist es zielführend folgende einzelne Zusatzfragen in den Fokus zu rücken und Antworten dafür zu erarbeiten.

Z 1. Sind aus dem bestehenden deutschen IT-Sicherheitsgesetz Erkenntnisse für das noch ausstehende österreichische NISG zu gewinnen?
Z 2. Welche Steuerungsmaßnahmen sind in Unternehmen zu etablieren, damit entsprechende Verantwortlichkeiten auch an externe IT-Service Provider in Österreich übertragen werden können?
Z 3. Wie können IT-Service Provider und „Betreiber wesentlicher Dienste“ in Österreich die aus der NIS-Richtlinie entstehenden, relevanten Themen ableiten und sicherstellen, dass NIS-Vorgaben auch eingehalten werden?

Diese Fragen sind als Basis der Masterarbeit und der erstellten ExpertInnenbefragungen bzw. Feldexperimente mit Bezug zum „Self Assessment für NIS-Readiness“ anzusehen.

1.5 Hypothesen

Nach intensiver Literaturrecherche sind folgende Hypothesen aufgestellt worden, die im Zuge der Masterarbeit verifiziert oder gegebenenfalls falsifiziert wurden.

H 1. Die „Betreiber wesentlicher Dienste“ haben die Möglichkeit die Verantwortung auch an externe IT-Service Provider zu übertragen.
H 2. Es ist für Österreich ratsam, sich bei ausgewählten Fragestellungen (z.B. sektorale Schwellenwerte, Sanktionen, Meldestruktur) zum NISG an bereits bestehenden Gesetzestexten aus Deutschland zu orientieren.
H 3. „Betreiber wesentlicher Dienste“ und IT-Service Provider, die schon auf Basis der ISO 27001 zertifiziert sind, haben bezüglich der Anforderungen aus der NIS-Richtlinie bereits viel Vorarbeit geleistet.
H 4. Ein „Self Assessment für NIS-Readiness” wird von potenziell betroffenen Unternehmen zur Bewertung und Einschätzung als positiv angesehen.
H 5. Im Zuge eines strukturierten „Self Assessment für NIS-Readiness“ können technische und organisatorische Aspekte, die sich aus der NIS-Richtlinie ergeben, aufgezeigt und so einer möglichen Behandlung zugeführt werden.
H 6. Eine Bewertung der NIS-Readiness anhand eines Reifegradmodells wird hinsichtlich einer objektiven Bewertung als zweckmäßig angesehen.

1.6 Methodenauswahl

Das Ziel ist es, im Kapitel 3.3 die obigen Forschungsfragen und Hypothesen mittels folgender verschiedener Methoden beantworten zu können.

- Literaturrecherche,
- Prototyp („Self Assessment für NIS-Readiness“),
- Feldexperimente (Verifikation),
- Qualitative Analysen mit ExpertInnenbefragung zum Prototyp des Self Assessments und dem Feldexperiment.

Nähere Details und Erläuterungen werden dazu in Kapitel 3.1 beschrieben.

1.7 Abgrenzungen des Untersuchungsbereiches

Zum Zeitpunkt der Verfassung dieser Masterarbeit war in Österreich noch kein nationales Gesetz zur Umsetzung der NIS-Richtlinie existent. Dennoch ist der Fokus dieser Arbeit primär auf den Standort Österreich gerichtet. Anlassbezogen wird auf die deutsche Gesetzgebung referenziert und einer vergleichenden Analyse unterzogen.

Im Rahmen der Masterarbeit sind ExpertInnenbefragungen aus verschiedenen (in-)direkt betroffenen Sektoren Österreichs geführt worden. Da diese Sektoren jedoch einer sehr breiten Streuung unterliegen, ist aus Effektivitätsgründen ein möglichst repräsentativer Querschnitt an ExpertInnen ausgewählt worden. Diese wurden so gewählt, dass sowohl die Sichtweisen der betroffenen Unternehmen wie auch der zuständigen IT-SP in die Analyse einfließen konnten.

Die NIS-Richtlinie adressiert in der aktuellen Fassung grundsätzlich unterschiedliche Betreibergruppen. In der Masterarbeit wird der Fokus hauptsächlich auf die „Betreiber wesentlicher Dienste“ (BwD) gelegt, da diese standardmäßig strengeren Vorgaben unterliegen. Die hier vorgenommene Betrachtung gilt ausschließlich für die Länder Österreich und Deutschland und kann somit nicht verallgemeinert werden.

Die nationale Gesetzgebung zur NIS-Richtlinie wird in den analysierten Ländern - Österreich und Deutschland -vielfältige Auswirkungen auf existierende Gesetze haben. In dieser Masterarbeit wird jedoch nicht im Detail bewertet, ob betroffene nationale Gesetze zueinander in Widerspruch stehen oder Lücken haben. Zudem wird keine rechtliche Analyse durchgeführt, wie weitere Rechtsakte aussehen könnten, um eine Erhöhung des Sicherheitsniveaus von NIS zu gewährleisten.

Eine Betrachtung organisatorischer und technischer Aspekte, die sich im Rahmen der NIS-Richtlinie ergeben können, wird nur für schon vorhandene Systeme und Prozesse durchgeführt.

2. Theoretische Betrachtung

Um eine angemessene und wirksame Abwehr vor Cyberbedrohungen zu gewährleisten, ist ein umfassender gemeinschaftlicher Ansatz anzustreben. Dafür erforderlich sind ausgereifte Strukturen zur Steigerung bzw. Förderung der Cybersicherheit. Dies nicht nur in den jeweiligen EU-Mitgliedstaaten sondern auch in den Institutionen der EU. Zudem wird folgendes gebraucht:

- ein ressortübergreifender Ansatz zur Verbesserung der Cyberabwehrfähigkeit sowie der strategischen Autonomie,
- Weiterentwicklungen bei der technologischen Kompetenz,
- deutlich mehr qualifizierte ExpertInnen.[18]

Um diese angestrebten Fortschritte zu erreichen, muss die Erkenntnis da sein, dass Cybersicherheit eine Herausforderung für die ganze Gesellschaft ist. Um diese zu bewältigen, sind verschiedene Ebenen wie Regierungen, Wirtschaft und die Zivilgesellschaft zu involvieren.[19] Dieser Ansatz wird ansatzweise bereits auf nationaler Ebene in Form von „Public-Private-Partnership" (PPP)-Modellen[20] gelebt. Bereits mehr als 70 Staaten (EU - dazu zählen auch Österreich und Deutschland - und Nicht EU) haben entsprechende Cyberstrategien entwickelt.[21]

Ein Anspruch auf Vollständigkeit bzgl. Literatur wird in dieser Masterarbeit nicht erhoben, da sich die bearbeitete Thematik bzgl. der NIS-Richtlinie (inter-)national noch in Umsetzung befindet und eine hohe Volatilität aufweist. Deshalb werden europäische und nationale Gesetze, Verordnungen oder Mitteilungen als Basis zum Erkenntnisgewinn und zur Beantwortung der Forschungsfragen herangezogen.

Um den Stand der Entwicklungen bestmöglich widerzugeben wird der Hauptfokus auf themenbezogene Fachliteratur, wie auch auf Berichte und Studien von fach-einschlägigen (inter-)nationalen Beratungs- und Forschungsunternehmen gelegt. Die Literaturrecherche und -auswertung zielt vornehmlich auf Dokumente mit Bezug zur NIS-Richtlinie für den europäischen Binnenmarkt ab. Hier werden speziell die zwei Länder Österreich und Deutschland einem Vergleich unterzogen.

„*Eine wirklich gute Idee erkennt man daran, dass ihre Verwirklichung von vorne herein ausgeschlossen erscheint.*"
(Albert Einstein, 1879 - 1955)

[18] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 4)

[19] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 4ff)

[20] Vertraglich geregelte Zusammenarbeit zwischen öffentlicher Hand und privatwirtschaftlichen Unternehmen in einer Zweckgesellschaft.

[21] Vgl. (Bartsch und Frey 2017, S. 60)

2.1 Definition und Grundlagen

Wie so oft in der IT werden auch im Zusammenhang mit der NIS-Richtlinie viele Fachbezeichnungen und Abkürzungen verwendet. Um in dieser Masterarbeit ein gemeinsames Verständnis und Wissen sicherzustellen, werden folgend die wesentlichen relevanten Begriffe und Methoden detaillierter beschrieben.

2.1.1 „Kritische Infrastruktur" (KI)

Sogenannte KI können als wesentlicher Grundpfeiler zur gesellschaftlichen Grundversorgung mit Gütern und Services des täglichen Lebens angesehen werden. Das österreichische „Bundeskanzleramt" (BKA) definiert KI wie folgt:

> „[...] jene Infrastrukturen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon), die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde."[22]

Diese Definition stimmt im Wesentlichen mit jener überein, die Seitens der EU in der Richtlinie zu „europäischen kritischen Infrastrukturen" (EKI)[23] formuliert wurde.

2.1.2 „Computer Emergency Response Team" (CERT)

Aufgrund der deutlich zugenommenen Bedrohungslage durch Angriffe auf die IKT-Infrastrukturen und die KI´s ist auch die Bedeutung des CERT / CSIRT („Computer Emergency Response Team" / „Computer Security Incident Response Team") immer mehr angewachsen. Dabei können diese in diversen Ausprägungen auftreten, bzw. etabliert werden. Als nationale CERT´s können sie zuständig sein für z.B.:

- ein ganzes Land
- einen kompletten Wirtschaftssektor bzw. eine Branche
- für spezielle KI´s
- ein eigenes Unternehmen bzw. einen Konzern[24]

Ursprünglich wurden CERT´s als Einrichtungen zur praktischen Unterstützung bei IT-Sicherheitsvorfällen ins Leben gerufen. So gab es in der Anfangszeit auch keinen Rechtsrahmen dafür, bzw. war und ist er in vielerlei Hinsicht nicht exakt.[25] Bei der

---

[22] (Bundeskanzleramt Österreich 2015, S. 6)

[23] Vgl. (Amtsblatt der Europäischen Union 2008, S. 3)

[24] Vgl. (Tschohl et al. 2017, S. 1)

[25] Vgl. (Tschohl et al. 2017, S. 1)

Bezeichnung CERT handelt es sich um eine eingetragene Marke der Carnegie Mellon University.[26] Sofern ein CSIRT nach gegebenen Guidelines agiert, kann es bei der Carnegie Mellon University einen Antrag stellen, den Begriff CERT im Namen führen zu dürfen, um darauffolgend in einer öffentlichen Liste genannt zu werden. In der NIS-Richtlinie wird den Empfehlungen der Carnegie Mellon University folgend der Begriff CSIRT - als generische Bezeichnung - verwendet.[27] Die Begriffe CERT und CSIRT werden in dieser Masterarbeit synonym verwendet.

Die Abbildung 2 gibt einen grundlegenden Überblick von potenziellen Services, die sich, laut einer ENISA-Studie, ein Unternehmen von einem CSIRT erwarten kann.

REACTIVE SERVICES	PROACTIVE SERVICES	SECURITY QUALITY MANAGEMENT SERVICES
Alerts and Warnings Incident Handling ▪ *Incident analysis* ▪ *Incident response on site* ▪ *Incident response support* ▪ *Incident response coordination* Vulnerability Handling ▪ *Vulnerability analysis* ▪ *Vulnerability response* ▪ *Vulnerability response coordination* Artefact Handling ▪ *Artefact analysis* ▪ *Artefact response* ▪ *Artefact response coordination*	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Abbildung 2: Liste der CSIRT Services[28]

Grundlegend kann zwischen reaktiven, proaktiven und qualitätssteigernden Services unterschieden werden. Die tatsächlichen Leistungsausprägungen des jeweiligen CSIRT werden in der Praxis oftmals deutliche Unterschiede aufweisen, da es je nach konkretem Fall unterschiedlichste Anforderungen geben kann.

2.1.3 "Chief Information Security Officer" (CISO)

In der NIS-Richtlinie wird nicht konkret ausformuliert welche Rolle / Person / Gruppe auf Seiten der BwD die Meldung relevanter Sicherheitsvorfälle vorzunehmen hat. In themenspezifischen Dokumenten wird jedoch oftmals ein „Chief Information Security Officer" (CISO) als Instanz genannt, der/die eine themenspezifische zentrale Anlaufstelle inner- und außerhalb des Unternehmens darstellen soll. Auch wenn ein CISO, in Österreich auch

[26] Vgl. http://www.cert.org/incident-management/csirt-development/cert-authorized.cfm?

[27] Vgl. (Tschohl et al. 2017, S. 1)

[28] (ENISA 2016b, S. 11)

IT-Sicherheitsbeauftragte/r genannt wird, ist er/sie in diesem Sinne nicht als operative Instanz zu sehen, sondern soll in seiner/ihrer Funktion die entsprechenden Verantwortungen bündeln.

Speziell im Ereignisfall ist es meistens zeitkritisch und von hoher Relevanz, dass die unternehmensinternen Zuständigkeiten und Verantwortlichkeiten bekannt sind. In Österreich wird deshalb im fachspezifischen Whitepaper des „Kuratorium Sicheres Österreich“ (KSÖ) vorgeschlagen, dass im NISG die Funktion des CISO (oder StellvertreterIn) definiert wird, sowie ausdrücklich die Rolle im Zuge der Bewältigung des Cyberereignisses beschrieben wird. Folgend ein Auszug dazu:

> *„Der/Die IT-Sicherheitsbeauftragte ist die zentrale Ansprechperson für alle Informations- und IT-Sicherheitsfragen innerhalb einer Organisation und trägt die fachliche Verantwortung für diesen Bereich. Zu den Pflichten des/der IT-Sicherheitsbeauftragten gehören (1) die verantwortliche Mitwirkung an der Erstellung des Informationssicherheitskonzepts, (2) die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen, (3) die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen, (4) die Gewährleistung der Informationssicherheit im laufenden Betrieb sowie (5) die Verwaltung der für die Informationssicherheit zur Verfügung stehenden Ressourcen.“*[29]

2.1.4 “Capability Maturity Model Integration” (CMMI)

Das „Capability Maturity Model Integration“ (CMMI) ist in den 1980er Jahren am Software Engineering Institute der Carnegie Mellon University entwickelt worden. Ausgangsbasis war ein Auftrag des amerikanischen Verteidigungsministeriums ein Werkzeug zur Beurteilung von Softwarelieferanten bereitzustellen.[30] Das CMMI ist grundsätzlich ein Reifegradmodell, dass auf drei wichtigen Dimensionen aufsetzt (vgl. Abbildung 3).

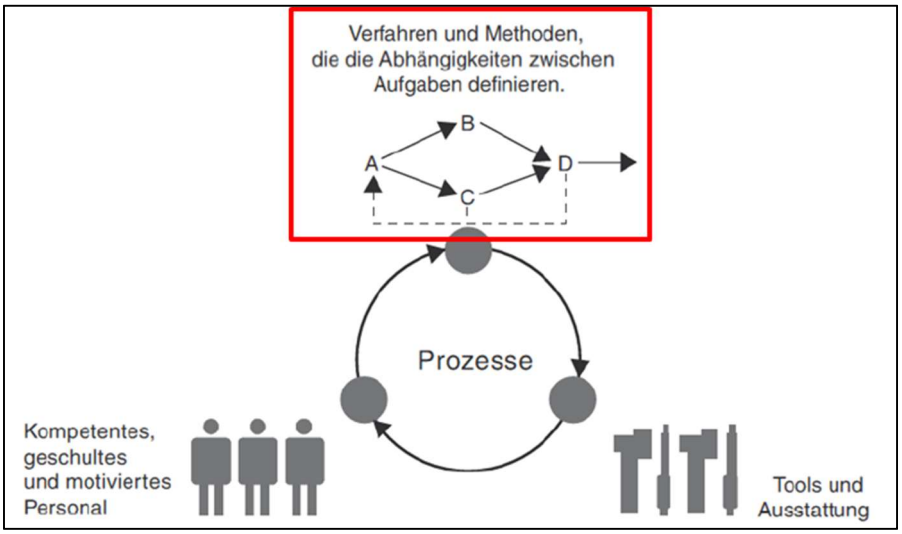


Abbildung 3: Die bedeutenden drei Dimensionen für Arbeitsabläufe[31]

[29] (KSÖ – Kuratorium Sicheres Österreich 2016, S. 13)

[30] Vgl. (CMMI Product Team 2011, S. 17)

[31] (CMMI Product Team 2011, S. 16)

Als Kernaussage ist festzuhalten, dass vor allem mittels der Arbeitsabläufe (rot umrahmt) die diversen Geschäftsaktivitäten der Organisation besser aufeinander abgestimmt werden können. Durch diese Abläufe kann eine bessere Skalierbarkeit, sowie Integration von verbesserungswürdigem Wissen ermöglicht werden und es ermöglicht Ressourcen wirksam einzusetzen und Geschäftstrends zu analysieren. Unbestritten bleibt jedoch, dass auch Mensch und Technologie wichtig sind.[32]

In der aktuellen Version 1.3 ist prinzipiell noch zwischen den drei folgenden spezifischen CMMI zu unterscheiden:

- CMMI for Development (CMMI-DEV)
  Ist im Speziellen auf die Bereiche rund um die Entwicklung von Produkten und Dienstleistungen ausgerichtet.
- CMMI for Services (CMMI-SVC)
  Fokussiert auf die Bereiche rund um die Erbringung und Verbesserung von Dienstleistungen.
- CMMI for Acquisition (CMMI-ACQ)
  Ist im Speziellen auf die Bereiche rund um die Beschaffung von Produkten und Dienstleistungen, aus Sicht einkaufender Organisation, ausgerichtet.

Auch wenn CMMI-DEV einer umfänglichen Weiterentwicklung unterzogen wurde und 2018 als „CMMI Development V2.0“ erschien, so bezieht sich die Masterarbeit ausschließlich auf die CMMI Version 1.3. Deren drei spezifischen CMMI-Modelle bestehen im Kern aus 16 Prozessgebieten (die für alle CMMI-Modelle gelten) und sind nach der gleichen Struktur aufgebaut. Jedes der einzelnen Modelle weist darüber hinaus noch folgende entsprechende Prozessgebiete (siehe Kapitel 2.1.4.1 bis 2.1.4.3) auf.

Alle drei der nachfolgenden CMMI-Modelle sind für das „Self Assessments für NIS-Readiness“ (vgl. Kapitel 3.2.2) als zentrale Elemente anzusehen, da spezifische Inhalte als Basis zur Modellbildung und Bewertung herangezogen wurden.

2.1.4.1 CMMI for Development / CMMI für Entwicklung

Im Rahmen des CMMI-DEV sind 22 Prozessgebiete enthalten (inkl. der 16 Kernprozess-gebiete). Von den restlichen sechs spezifischen wird eines gemeinsam mit CMMI-SVC (Zulieferungsmanagement) genutzt und folgende fünf sind spezifisch für die Entwicklung:

1. Produktintegration
2. Anforderungsentwicklung
3. technische Umsetzung
4. Verifizierung
5. Validierung[33]

[32] Vgl. (CMMI Product Team 2011, S. 16)

[33] Vgl. (CMMI Product Team 2011, S. 15f)

2.1.4.2 CMMI for Services / CMMI für Dienstleistungen

Das CMMI-SVC enthält 24 Prozessgebiete (inkl. der für alle drei CMMI´s geltenden 16 Kernprozessgebiete). Von den restlichen acht spezifischen wird eines gemeinsam mit CMMI-DEV (Zulieferungsmanagement) genutzt und sieben sind spezifisch für Services:

1. Kapazitäts- und Verfügbarkeitsmanagement
2. Störungsbehebung und -vermeidung
3. Kontinuitätsmanagement
4. Erbringung von Dienstleistungen
5. Entwicklung von Dienstleistungssystemen
6. Betriebsüberführung von Dienstleistungssystemen
7. Strategisches Dienstleistungsmanagement[34]

2.1.4.3 CMMI for Acquisition / CMMI für Beschaffung

Das CMMI-ACQ sind 22 Prozessgebiete enthalten (inkl. der 16 Kernprozessgebiete) wobei die restlichen sechs als spezifisch für die Beschaffung anzusehen sind:

1. Management der Vereinbarungen
2. Anforderungsmanagement
3. Verfolgen des Arbeitsfortschritts auf technischer Ebene
4. Validierung der Ergebnisse des Lieferanten
5. Verifikation der Ergebnisse des Lieferanten
6. Lieferantenauswahl und Entwicklung der Lieferantenvereinbarung[35]

2.1.5 Cybersicherheit

Der Begriff „Cybersicherheit“ wird je nach Land, Branche oder IT-Framework in unterschiedlichster Schreibweise angewendet. Doch unabhängig davon ob nun

- Cybersicherheit bzw. Cyber Sicherheit bzw. Cyber-Sicherheit oder
- Cybersecurity bzw. Cyber Security bzw. Cyber-Security

geschrieben wird, so können alle diese Begriffe als synonym angesehen werden. Abbildung 4 zeigt die einzelnen Domänen, welche in den Überbegriff Cybersicherheit eingehen.

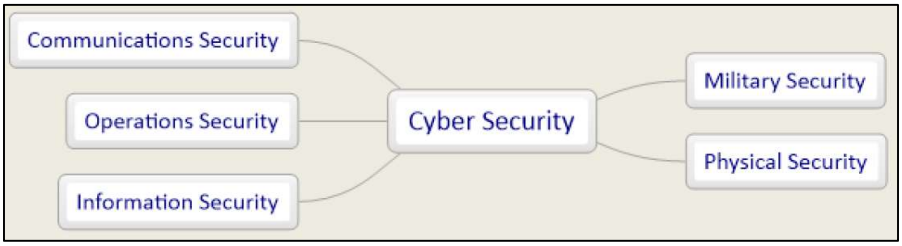


Abbildung 4: Verschiedene Domänen der Cybersicherheit[36]

[34] Vgl. (CMMI Product Team 2010b, S. 3)

[35] Vgl. (CMMI Product Team 2010a, S. 4)

[36] (ENISA 2015, S. 11)

Je nach betrachtetem IT-Standard oder Framework wie etwa

- ISO 27001 oder ISO 27032
- NIST SP 800-39
- CNSSI 4009

sind die Definitionen in ihren Teilaspekten doch verschieden. Gemäß des ENISA-Berichts „Definition of Cybersecurity" ist eine eindeutige Definition von Cybersicherheit nicht möglich, bzw. wird nicht als erforderlich angesehen. Als Problem wird beschrieben, dass es sich um einen Hüllenbegriff handelt, der nicht all die relevanten Themen umfassen kann. Stattdessen soll für den spezifischen Fall eine entsprechende Definition getroffen werden die auch dazu passt.[37] In Österreich wird etwa im fachspezifischen Dokument „KSÖ Rechts- und Technologiedialog Whitepaper" (in Folge KSÖ-Whitepaper genannt) vorgeschlagen, Cybersicherheit im entsprechenden NISG wie folgt zu definieren:

> „*Cybersicherheit beschreibt den Schutz eines zentralen Rechtsgutes mit rechtsstaatlichen Mitteln vor akteursbezogenen, technischen, organisations- und naturbedingten Gefahren, die die Sicherheit des Cyberspace (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyberspace gefährden. Cybersicherheit trägt dazu bei, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen sowie die Fähigkeit zu stärken, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.*"[38]

Der Umfang von Cybersicherheit ist also entsprechend groß und hat Relevanz für viele geschäftskritische Bereiche. Die EU war und ist somit gefordert und reagiert nun verstärkt auf die rasant ansteigende Gefahr der Cyberbedrohungen. Sie setzt mit der NIS-Richtlinie erste wichtige Schritte zur Förderung der Cybersicherheit.

2.1.6 ISO 27000-Normenreihe

Die ISO 27000-Reihe behandelt Themen, die im Zusammenhang mit dem „Information Security Management System" (ISMS) stehen. Die zwei nachfolgenden Normen sind dabei vor allem für das Kapitel 3.2.2 von zentraler Bedeutung, da wesentliche Inhalte in das „Self Assessments für NIS-Readiness" eingeflossen sind.

2.1.6.1 ISO 27001 und Anhang A

Bei dieser Norm werden im Speziellen die Anforderungen an ein ISMS beschrieben. Wie alle neu überarbeiteten ISO-Normen weisen die ersten 4 Kapitel (0 - 3) vornehmlich allgemeinen Charakter auf. In den Kapiteln 4 - 10 wird konkret auf die Anforderungen bzgl. festlegen, umsetzen, betreiben, überwachen, überprüfen, instandhalten und verbessern eines dokumentierten ISMS im Kontext zu den allgemeinen Geschäftsrisiken

[37] Vgl. (ENISA 2015, S. 28)

[38] (KSÖ – Kuratorium Sicheres Österreich 2016, S. 12)

einer Organisation eingegangen.[39] Dies sind im Besonderen nachfolgende Elemente:

- Kontext der Organisation (Kapitel 4))
  Verstehen der Organisation und der Stakeholder und des Anwendungsbereiches
- Führung (Kapitel 5)
  Managementverantwortung, Informationssicherheitspolitik sowie organisatorische Rollen, Zuständigkeiten und Verantwortungen
- Planung (Kapitel 6)
  Risikomanagement-Kriterien und Informationssicherheitsziele
- Unterstützung (Kapitel 7)
  Ressourcenverfügbarkeit, Kompetenzen, Awareness, Kommunikation und Dokumentation
- Betrieb (Kapitel 8)
  Betriebliche Planung und Steuerung, Risikomanagement Prozesse (Informationssicherheitsrisikobeurteilung und -behandlung)
- Bewertung der Leistung (Kapitel 9)
  Prüfungsmaßnahmen (Überwachung, Messung, Analyse und Bewertung), Audits und Managementbewertung
- Verbesserung (Kapitel 10)
  Abweichungen, Korrekturmaßnahmen und kontinuierliche Verbesserung[40]

Der zugehörige Anhang A (abgeleitet aus ISO 27002) enthält konkrete Maßnahmen und Maßnahmenziele welche im Kontext mit Inhalten des Kapitels 6 anzuwenden sind. Diese Maßnahmen und -ziele gliedern sich in folgende Bereiche:

A.5 Informationssicherheitsrichtlinien
A.6 Organisation der Informationssicherheit
A.7 Personalsicherheit
A.8 Verwaltung der Werte
A.9 Zugangssteuerung
A.10 Kryptographie
A.11 Physische und umgebungsbezogene Sicherheit
A.12 Betriebssicherheit
A.13 Kommunikationssicherheit
A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
A.15 Lieferantenbeziehungen
A.16 Handhabung von Informationssicherheitsvorfällen
A.17 Informationssicherheitsaspekte beim Business Continuity Management
A.18 Compliance[41]

In Summe lassen sich die beschriebenen Anforderungen wie folgt unterteilen:

- 14 Abschnitte (Sections) splitten sich in

[39] Vgl. (A-SIT Zentrum für sichere Informationstechnologie – Austria 2017, online)

[40] Vgl. (DIN-Normenausschuss Informationstechnik und Anwendungen 2015, S. 2ff)

[41] Vgl. (DIN-Normenausschuss Informationstechnik und Anwendungen 2015, S. 16ff)

- 35 Maßnahmenziele (Control Objectives) woraus
- 114 Maßnahmen (Controls) abgeleitet werden.

Die ISO 27001 wird zudem auf branchenspezifische Standards einen wesentlichen Einfluss haben. (vgl. 2.4.4 oder 2.5.3) und für BwD sowie IT-SP von Bedeutung sein.

2.1.6.2 ISO 27017

Die Norm ist, gemäß deutscher Übersetzung, als „Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste" zu verstehen. Sie kann somit grundsätzlich als Ergänzung zur ISO 27001 angesehen werden und bietet einen Leitfaden für die Aspekte der Informationssicherheit im Bereich der Cloud Services.

Die Norm ist so gestaltet, dass sie als Implementierungsleitfaden für ein Cloud-ISMS (mit Referenz zur ISO 27002) und Cloud-Maßnahmen sowie allgemein anerkannter Schutzkontrollen verwendet werden kann. Die Norm-Anforderungen sind konkret auf IT-SP aus dem Bereich des Cloud-Computing zugeschnitten und beziehen sich auf die ISO 27002. Insbesondere werden in der ISO 27017 Anleitungen zu 37 Maßnahmen bereitgestellt. Zusätzlich werden noch folgende sieben cloudspezifischen Maßnahmen beschrieben:

1. Gemeinsame Rollen sowie Pflichten innerhalb einer Cloud-Umgebung
2. Regelung zur Retournierung und Entfernung von Kundenressourcen in Cloud Services nach dem Vertragsende
3. Schutz und Trennung virtueller Umgebungen zwischen den Kunden
4. Erfordernisse bzgl. „Härtung" virtueller Maschinen damit die jeweiligen Geschäftsanforderungen erfüllt werden
5. Verfahren (für Definition, Dokumentation, Monitoring) für administrative Abläufe einer Cloud-Umgebung
6. Kundenseitige Überwachung von entsprechenden Aktivitäten innerhalb einer Cloud-Umgebung
7. Abstimmung der Informationssicherheit Policy hinsichtlich virtueller und physischer Netzwerke[42]

Die ISO 27017 hat dabei nicht nur Auswirkung auf den IT-SP von Cloud-Services selbst, sondern insgesamt auf die Sicherheit der Cloud. Sie stellt den nutzenden Organisationen der Cloud Services praktische Informationen, bzgl. der Erwartungen an den IT-SP der Cloud Services, bereit.

2.1.7 Stand der Technik

Laut BSI kann der Begriff „Stand der Technik" zwar interpretiert, aber keine allgemeingültige Definition gegeben werden. Es handelt sich dabei formell um einen gängigen juristischen Begriff. Es hat sich in der heutigen Zeit praktisch bewährt, den Begriff auch in Gesetzen oder Verordnungen zu verwenden, anstatt konkrete technische

[42] Vgl. (BSI Group s.a., S. 2)

Anforderungen zu definieren. Generell schreitet die technische Entwicklung schneller voran als die Gesetzgebung nachziehen könnte.

Der Begriff „Stand der Technik“ ist somit unbestimmt. Er kann zwischen die Generalklauseln „allgemein anerkannten Regeln der Technik“ und „Stand der Wissenschaft und Technik“ eingereiht werden (vgl. Abbildung 5, rot umrahmt). Je nachdem wie hoch / gering der jeweilige Grad der „Allgemeinen Anerkennung“ und die „Bewährung und Erprobung in der Praxis“ ist, kann der Übergang zwischen den einzelnen Begriffen erfahrungsgemäß fließend sein und als gewisser Unsicherheitsfaktor angesehen werden.[43]

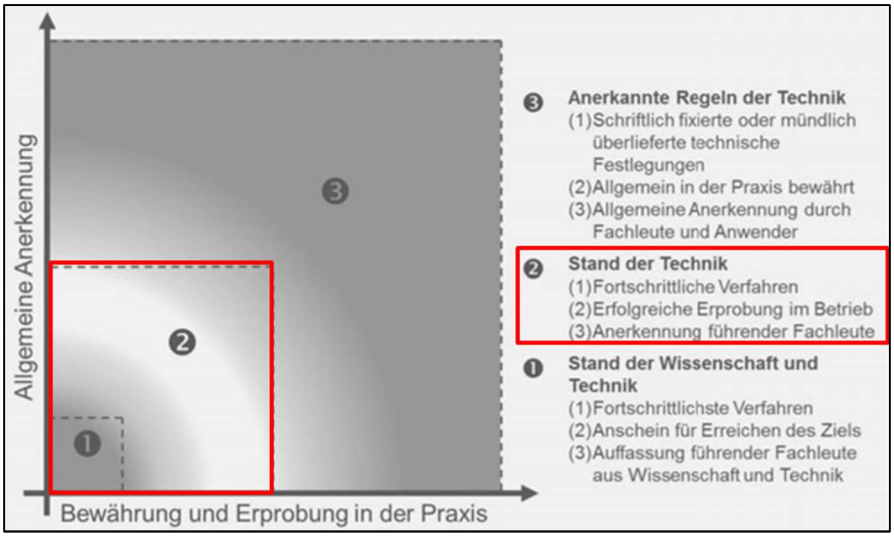


Abbildung 5:Schema zur Zuweisung der Generalklauseln[44]

Von Bedeutung ist in diesem Sinne, was zu einem bestimmten Zeitpunkt als „Stand der Technik“ anzusehen ist. Dies kann beispielsweise auf Basis bestehender (inter-)nationaler Standards, Frameworks oder anerkannten Best Practices ermittelt werden.[45]

2.2 NIS-Richtlinie

Auch wenn die EU-Mitgliedsstaaten bereits auf einem guten Weg sind Cybersicherheitsbedrohungen zu erkennen und zu bekämpfen, so ist sich die EU dennoch darüber im Klaren, dass es von Bedeutung sein wird, noch höhere Standards zu etablieren. Durch die kontinuierlich voranschreitende Globalisierung, Vernetzung und Digitalisierung von relevanten Schlüsselindustrien /-sektoren, wie etwa Energie, Verkehr oder Gesundheit, haben massive Sicherheitsvorfälle im Cyberraum nur mehr in den seltensten Fällen Auswirkung auf ausschließlich einen Staat.

2.2.1 Chronologische Entwicklung Cybersicherheit in der EU

Um geeignete Maßnahmen ergreifen zu können, wurden bereits ab 2001 wesentliche Entwicklungen auf europäischer und ebenso nationaler Ebene in die Wege geleitet. Die

[43] Vgl. (Michaelis 2016, S. 458)

[44] (Michaelis 2016, S. 458)

[45] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2016, online)

nachfolgende Aufstellung gibt einen grundlegenden Überblick über die Entwicklungen auf EU-Ebene, welcher aber als nicht taxativ zu verstehen ist:

- Bereits 2001 wies die Europäische Kommission in der Mitteilung „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“ auf die steigende Bedeutung der Netz- und Informationssicherheit hin.
- Per Verordnung (EG) Nr. 460/2004 wurde 2004 die ENISA, zur Entwicklung einer Kultur der Netz- und Informationssicherheit, errichtet.
- Darauf folgte 2006 die Annahme einer „Strategie für eine sichere Informationsgesellschaft“ (KOM(2006) 251), welche bei der Entwicklung der Kultur der Netz- und Informationssicherheit in Europa unterstützen sollte.
- Der Rat der EU beschloss am 8.12.2008 die „Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern“.
- Der Europäische Rat hat im März 2010 die „Strategie für die innere Sicherheit der Europäischen Union“ angenommen und darin Cyberkriminalität als entsprechende Herausforderung anerkannt.[46]
- Mit Februar 2013 wurde durch die Europäische Kommission ein Vorschlag zur „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“ eingereicht.
- Den EU-Mitgliedstaaten wird seit Anfang 2013 das „Critical Infrastructure Warning and Information Network“ (CIWIN) als technische Plattform zwecks Informationsaustausch zur Verfügung gestellt.
- Mit Mai 2013 erging die Verordnung (EU) Nr. 526/2013, dass die ENISA in erneuerter Form errichtet wird, um mit den neuen Aufgaben zur Schaffung und zum ordnungsgemäßen Funktionieren des Binnenmarktes beizutragen.
- Seitens der EU ist 2013 auch eine Cybersicherheitsstrategie verabschiedet worden, in der vielfältige Maßnahmen zur Stärkung der Abwehrfähigkeit gegenüber Cyberattacken festgehalten sind. Die hier formulierten Hauptziele und Grundsätze gelten nach wie vor. Diese Ziele gingen in einem Vorschlag für eine „Richtlinie über die Netz- und Informationssicherheit“ auf.[47]
- Nach ausgiebiger Diskussion und mehreren Studien zur Weiterentwicklung von „European Program for Critical Infrastructure Protection“ (EPCIP) wurden 2013 entsprechende Arbeitsdokumente vorgelegt.[48]
- Mit 2015 wurde „Die Europäische Sicherheitsagenda“ verabschiedet. Darin ist Cyberkriminalität eine der drei Kernprioritäten bei denen unmittelbarer Handlungsbedarf gesehen wird. Es wird zudem die rasche Annahme des Vorschlags zur NIS-Richtlinie als eine wichtige Voraussetzung festgehalten.[49]

---

[46] Vgl. (Amt für Veröffentlichungen der Europäischen Union 2010, S. 14)

[47] Vgl. (EUROPÄISCHE KOMMISSION 2013, S. 14)

[48] Vgl. (Bundeskanzleramt Österreich 2015, S. 4f)

[49] Vgl. (EUROPÄISCHE KOMMISSION 2015c, S. 15)

- Das Dokument „Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union“ (2016) adressiert prominent die Cybersicherheit und nimmt darin auch die Mitgliedsstaaten in die Pflicht.[50]
- Die aktuelle NIS-Richtlinie ist mit August 2016 in Kraft getreten und wurde zur fristgerechten Umsetzung an alle EU-Mitgliedsstaaten gerichtet.
- Der Europäische Rat rief, auf Basis des Vorschlags eines Reformpakets, im Oktober 2017 zur Annahme eines gemeinsamen Konzepts für die Cybersicherheit in der EU auf. Wesentliche Initiativen im Vorschlag sind etwa:
  - eine schlagkräftigere EU-Agentur für Cybersicherheit soll geschaffen werden,
  - ein EU-weites Cybersicherheit Zertifizierungssystems soll eingeführt werden,
  - die NIS-Richtlinie soll zügig umgesetzt werden.[51]

Im folgenden Kapitel werden die speziellen Inhalte, Fristen und Maßnahmen dieser NIS-Richtlinie, welche das zentrale Thema dieser Masterarbeit ist, konsolidiert. Die jüngere Vergangenheit zeigte, dass es nicht unüblich ist, dass eine Richtlinie vage bzw. allgemein gehalten wird und damit mehr als Handlungsrahmen für die nationalen Gesetzgeber zu verstehen ist. Während der Recherche wurde dieser Umstand auch öfters in verschiedenen Quellen beschrieben und teils kritisch betrachtet.

2.2.2 Zentrale Inhalte der NIS-Richtlinie

Die folgenden Inhalte wurden aus der NIS-Richtlinie extrahiert und sind von essentieller Bedeutung für die EU bzw. ihren Mitgliedsstaaten:

- Es wird darin eine nationale Strategie der Mitgliedsstaaten zur „Sicherheit von NIS“ gefordert, in der strategischere Ziele sowie konkrete politische Maßnahmen vorzusehen sind.
- Es ist eine „Kooperationsgruppe“ (KG) - Vertreter sind Mitgliedsstaaten, Europäische Kommission und ENISA - zur strategischen Zusammenarbeit und dem internationalen Informationsaustausch einzurichten.
- Aufbau eines (inter-)nationalen CSIRT-Netzwerks zur operativen Zusammenarbeit sowie die Verpflichtung, dass von Seiten der Mitgliedsstaaten nationale CSIRTs (laut NIS-Vorgabe) benannt und etabliert werden.
- Die Mitgliedsstaaten haben nationale zuständige Behörden, zentrale Anlaufstellen und CSIRTs zu benennen und so auszustatten, dass sie übertragene Aufgaben wirksam und effizient wahrnehmen können und die Ziele der NIS-Richtlinie erreicht werden. Dafür sollen sie mit angemessenen
  - technischen,
  - finanziellen und
  - personellen Ressourcen ausgestattet sein.[52]
- Die NIS-Richtlinie zielt auf spezifische Wirtschaftssektoren ab - somit auf hinzurechenbare relevante Unternehmen - welche für die Aufrechterhaltung

[50] Vgl. (European Union 2016, S. 7)

[51] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 4ff)

[52] Vgl. (Amtsblatt der Europäischen Union 2016, S. 5)

kritischer wirtschaftlicher und / oder gesellschaftlicher Tätigkeiten unerlässlich sind. Dabei wird zwischen folgenden zwei Typen unterschieden:[53]

1. „Betreiber wesentlicher Dienste“ (Operators of Essential Services)
   Dabei handelt es sich um eine öffentliche oder private Einrichtung einer speziellen Art ausgewählter Sektoren (Details im Anhang II der NIS-Richtlinie[54]), welche zudem definierten Kriterien entspricht. In Abbildung 6 (in blau) sind die sieben definierten Sektoren dargestellt, welche nach der NIS-Richtlinie relevant sind.
2. „Anbieter digitaler Dienste“ (Digital Service Provider)
   Dieser Typus ist eine juristische Person, welche einen digitalen Dienst anbietet. Als Dienst ist dabei - allgemein formuliert - eine Dienstleistung der Informationsgesellschaft einer speziellen Art (Details im Anhang III der NIS-Richtlinie[55]) zu verstehen. In Abbildung 6 (in rot) sind die drei definierten digitalen Dienste dargestellt, welche von der NIS-Richtlinie erfasst sind.

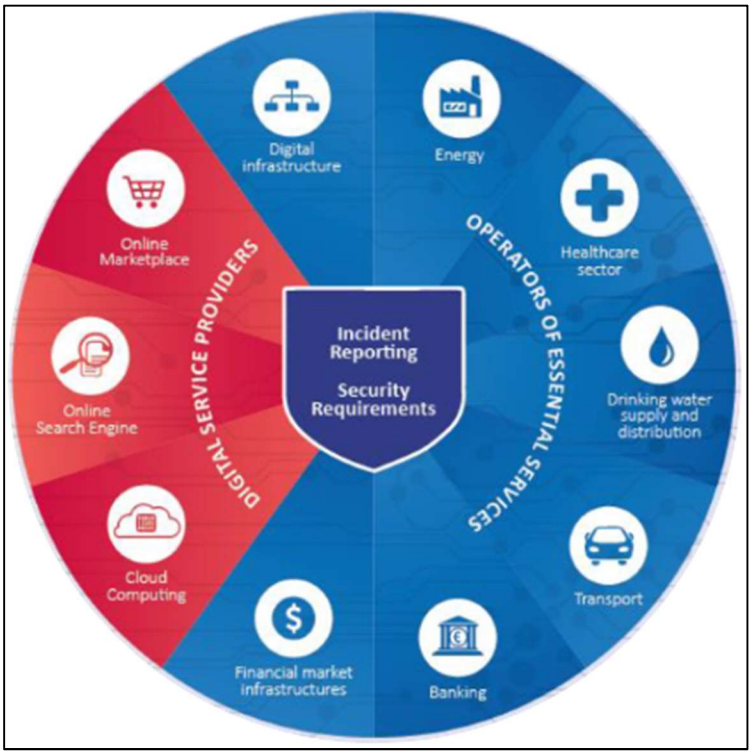


Abbildung 6: Relevante Sektoren laut NIS-Richtlinie[56]

- Als zentrale Kriterien zur Ermittlung der BwD sind die folgenden definiert:
  - Der erbrachte Dienst ist für die Aufrechterhaltung kritischer gesellschaftlicher und / oder wirtschaftlicher Tätigkeiten unerlässlich.
  - Die Bereitstellung dieses Dienstes ist abhängig von NIS.
  - Durch einen auftretenden Sicherheitsvorfall käme es zu einer erheblichen Störung beim Bereitstellen dieses Dienstes.[57]

[53] Vgl. (Amtsblatt der Europäischen Union 2016, S. 12ff)

[54] Vgl. (Amtsblatt der Europäischen Union 2016, S. 27ff)

[55] Vgl. (Amtsblatt der Europäischen Union 2016, S. 30)

[56] (ENISA 2017a, S. 9)

[57] Vgl. (Amtsblatt der Europäischen Union 2016, S. 14)

- Es gibt grundlegende Unterschiede zwischen BwD (wegen unmittelbarer Verbindung mit physischer Infrastruktur) und „Anbieter digitaler Dienste“ (AdD) (wegen deren grenzüberschreitender Art). Die NIS-Richtlinie verfolgt deshalb bei diesen beiden Gruppen jeweils einen unterschiedlichen Ansatz:
  - Bei BwD sollten Mitgliedstaaten in der Lage sein, die Betreiber zu bestimmen und strengere Anforderungen zu stellen als in dieser Richtlinie festgelegt. Als BwD ausgenommen sind z.B. die öffentliche Verwaltung und der Telekommunikationssektor, da sie eigenen europäischen Richtlinien bzw. nationalen Gesetzen unterliegen. [58]
  - AdD sollten nicht durch Mitgliedstaaten bestimmt werden, um so eine einheitliche Behandlung in der EU zu etablieren. Die NIS-Richtlinie, und anknüpfende Rechtsakte, sollten ein hohes Harmonisierungsmaß betreffend Sicherheitsanforderungen und Meldepflichten aufweisen. So sind z.B. KMU (kleiner 50 Mitarbeiter) als AdD ausgenommen.[59]
- Üblicherweise ist das Risiko für den BwD höher einzustufen, als jenes für den AdD. Deshalb sollten die Sicherheitsanforderungen für AdD geringer ausfallen und es sollte ihnen freigestellt sein, jene Maßnahmen zu ergreifen, die sie für die Bewältigung für angemessen erachten.
- Es sind auf EU-Ebene Mindestanforderungen für Kapazitätsaufbau und -planung, Zusammenarbeit, Informationsaustausch sowie Sicherheit zu beschreiben.
  - Sicherheitsanforderungen:
    Die Mitgliedstaaten haben sicherzustellen, dass BwD geeignete und verhältnismäßige „technische und organisatorische Maßnahmen“ (TOM) ergreifen, um Risiken für die Sicherheit der NIS (die für ihre Tätigkeiten genutzt werden) zu bewältigen. Die Maßnahmen müssen nach „Stand der Technik“ ein Sicherheitsniveau der NIS gewährleisten, welches dem Risiko angemessen ist.[60]
  - Meldepflichten:
    Es obliegt den Mitgliedsstaaten sicherzustellen, dass bei relevanten Sicherheitsvorfällen - mit Auswirkung auf die Verfügbarkeit der wesentlichen Dienste - eine unverzügliche Meldung durch die BwD erfolgt. Es müssen in der Meldung entsprechende Informationen enthalten sein, dass die zuständige Behörde oder das CSIRT bestimmen kann, ob der Vorfall grenzüberschreitende Folgen hat.[61] Ein mögliches „Tripple-Layer-Framework“ für den Krisenfall könnte, wie nach Empfehlung der ENISA aufgebaut sein (siehe Abbildung 7).

[58] Vgl. (Amtsblatt der Europäischen Union 2016, S. 2)

[59] Vgl. (Amtsblatt der Europäischen Union 2016, S. 8)

[60] Vgl. (Amtsblatt der Europäischen Union 2016, S. 20)

[61] Vgl. (Amtsblatt der Europäischen Union 2016, S. 20)

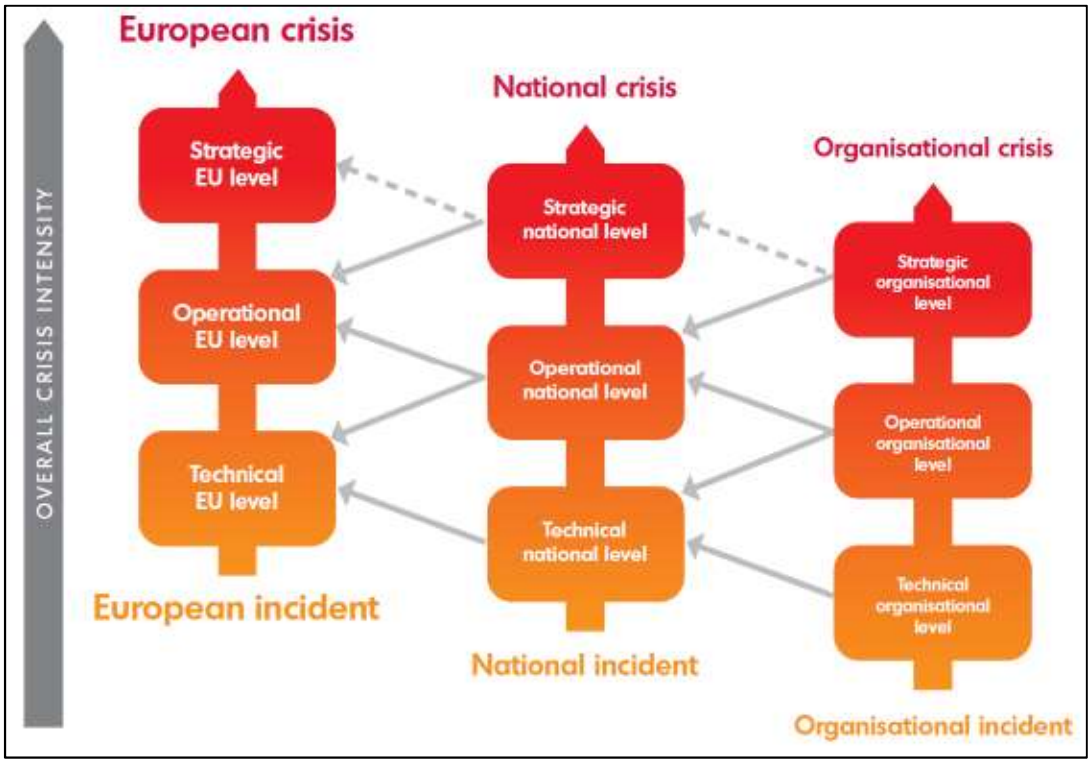


Abbildung 7: Krisen-Eskalationsmodell innerhalb der EU[62]

- Mitgliedstaaten können, gemäß NIS-Richtlinie, Bestimmungen erlassen oder aufrechterhalten, mit denen ein höheres Sicherheitsniveau zu erreichen ist.
- Zur Bestimmung des Störungsausmaßes hat der Mitgliedstaat zumindest die folgenden sechs sektorübergreifenden Faktoren zu berücksichtigen und gegebenenfalls auch weitere sektorspezifische Faktoren einfließen zu lassen:
  1. Zahl der Nutzer, die den angebotenen Dienst in Anspruch nehmen.
  2. Abhängigkeit anderer NIS-Sektoren von diesem angebotenen Dienst.
  3. Mögliche Auswirkung von Sicherheitsvorfällen (bzgl. Ausmaß und Dauer) auf wirtschaftliche und gesellschaftliche Tätigkeiten oder öffentliche Sicherheit.
  4. Marktanteil der Einrichtung des BwD.
  5. Geografische Ausbreitung des Gebiets, welches vom Sicherheitsvorfall betroffen sein könnte.
  6. Bedeutung der Einrichtung für die ausreichende Aufrechterhaltung des Dienstes, unter Berücksichtigung alternativer verfügbarer Mittel für die Bereitstellung des jeweiligen Dienstes.[63]
- Ausgewählte Sektoren unterliegen bereits sektorspezifischen EU-Rechtsakten, welche Vorschriften hinsichtlich Sicherheit von NIS beinhalten. In diesem Falle sollten die sektorspezifischen Bestimmungen gelten, wenn sie Anforderungen vorsehen, die hinsichtlich ihrer Wirkung den in der NIS-Richtlinie enthaltenen Verpflichtungen mindestens gleichwertig sind.[64]

[62] (ENISA 2016b, S. 23)

[63] Vgl. (Amtsblatt der Europäischen Union 2016, S. 15)

[64] Vgl. (Amtsblatt der Europäischen Union 2016, S. 2)

2.2.3 Zeitrahmen laut Definition der NIS-Richtlinie

Dass die NIS-Richtlinie durch alle Adressaten bis Mai 2018 vollständig umgesetzt wird, ist für die Cyberabwehrfähigkeit von zentraler Bedeutung. Die NIS-Richtlinie sieht einen relativ konkreten zeitlichen Fahrplan vor und definiert welche Leistungsinhalte durch welche Parteien (Mitgliedsstaat oder EU) zu liefern sind.[65]

- Mitgliedstaaten sollten bis Herbst 2017 Leitlinien erarbeitet und publiziert haben, um die Umsetzung, vor allem bzgl. BwD, stärker zu harmonisieren.
- Von Seiten der Europäischen Kommission werden als Teil des Cybersicherheitspakets entsprechende Verfahren vorgestellt, welche durch Mitgliedstaaten verprobt werden sollen und sich bei der Umsetzung bewähren,[66]
- Bis spätestens 9.2.2018 ist ein Arbeitsprogramm von der KG zu erstellen. Dieses befasst sich mit Maßnahmen, die zur Umsetzung ihrer Ziele und Aufgaben im Einklang mit den Zielen der NIS-Richtlinie zu ergreifen sind. Danach ist das Arbeitsprogramm alle zwei Jahre zu erstellen.
- Die KG beschreibt zwischen 9.2.2017 und 9.11.2018 Verfahren, Inhalt und Art nationaler Maßnahmen, zwecks Ermittlung der BwD in einem spezifischen Sektor
- Die Mitgliedstaaten erlassen Vorschriften über Sanktionen für Verstöße und informieren darüber die Europäische Kommission bis zum 9.5.2018. Ebenso melden sie sich unverzüglich bei der Europäischen Kommission, sollten sich etwaige spätere Änderungen abzeichnen.
- Eine Umsetzung der NIS-Richtlinie in nationales Recht hat bis 9.5.2018 zu erfolgen. Ab 10.5.2018 wenden die Mitgliedstaaten diese Maßnahmen an.
- Die zentrale Anlaufstelle der KG legt bis zum 9.8.2018 einen Bericht über die eingegangenen Meldungen, inkl. folgender Inhalte vor:
  - Meldungsanzahl
  - Art der gemeldeten Sicherheitsvorfälle
  - ergriffene Maßnahmen

  Dieser zusammenfassende Bericht ist danach jährlich zu erstellen.
- Die KG erstellt bis zum 9.8.2018 einen Bericht, in welchem die gewonnenen Erfahrungen bezüglich der strategischen Zusammenarbeit bewertet werden. Der Bericht ist zukünftig alle eineinhalb Jahre zu erstellen.
- Die BwD-Ermittlung muss bis 9.11.2018 durch die Mitgliedsstaaten erfolgen. Dabei sollte mit geeigneten Maßnahmen sichergestellt werden, dass die Bestimmungen der NIS-Richtlinie auf EU-Ebene bestmöglich geeignet sind, damit ein hohes gemeinsames NIS-Sicherheitsniveau erreichbar ist.[67]
- Die Liste der ermittelten BwD ist regelmäßig von den Mitgliedsstaaten zu überprüfen und im Bedarfsfall zu aktualisieren. Nach dem 9.5.2018 hat dies mindestens alle zwei Jahre zu erfolgen.
- Es ist bis zum 9.5.2019 ein Bericht vorzulegen, in dem die Nachvollziehbarkeit der Ansätze für die Ermittlung der BwD durch die Mitgliedstaaten bewertet wird.

---

65 Vgl. (Amtsblatt der Europäischen Union 2016, S. 11ff)

66 Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 8)

67 Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 7)

- Die Europäische Kommission überprüft regelmäßig die Anwendung der NIS-Richtlinie und erstattet Bericht. Dazu berücksichtigt sie Berichte der KG und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Der erste Bericht ist bis zum 9.5.2021 vorzulegen.

2.2.4 Status Quo Umsetzung der nationalen NIS-Richtlinie

Im Forschungsbericht „The Cyber Threat In Europe" von „Black Hat"[68] werden Umfrageergebnisse von 127 IT- und SicherheitsexpertInnen aus mehr als 15 Ländern Europas und den USA veröffentlicht. Viele der TeilnehmerInnen kommen aus hohen Positionen und stammen aus mehr als 20 verschiedenen Sektoren wie z.B. Gesundheitswesen, Energieversorger, Finanzdienstleister oder Regierungen. Im Bericht werden unter anderem folgende Themen der Informationssicherheit betrachtet:

- Die Sicherheit von KI´s und Angriffe auf Nationalstaaten
- Sicherheitsrisiken für Unternehmen und Auswirkungen der NIS-Richtlinie
- Die Anforderungen der DSGVO[69]

Als zentrale Erkenntnisse - für diese Masterarbeit - können folgende Aussagen bzgl. der aktuell eingeschätzten Chancen, Risiken sowie Status Quo hervorgehoben werden.

- 11% der TeilnehmerInnen glauben, dass durch eine Umsetzung der NIS-Richtlinie die KI in Europa besser geschützt sein wird.
- Es erwarten 77% der Befragten, dass in den nächsten 2 Jahren eine länderübergreifende Cyberattacke die KI´s in Europa treffen wird.
- 70% meinen, dass in den kommenden 2 Jahren die KI´s des eigenen Landes von einer Cyberattacke betroffen sein werden.
- Fast zwei Drittel glauben, dass sie auf einen gravierenden Sicherheitsvorfall in ihrem Unternehmen (in den nächsten 12 Monaten) reagieren werden müssen.
- Die Anpassung europäischer Gesetze wäre nach Ansicht von 42% nötig, damit Unternehmen aktiv gegen AngreiferInnen vorgehen können.
- 39% der Befragten sind der Meinung, dass fehlende relevante Kompetenzen und Fähigkeiten die Hauptgründe für das Scheitern von Sicherheitsstrategien sind.
- 38% meinen, dass sie ausreichend qualifiziertes Sicherheitspersonal haben, um das Unternehmen gegen Cyberbedrohungen zu verteidigen.[70]

Europa und besonders die EU stehen nicht nur vor der großen Herausforderung, ein faktisch ungleiches IT-Sicherheitsniveau der Mitgliedsstaaten durch eine Richtlinie anzugleichen, sondern noch viel mehr den transnationalen Informationsaustausch und das dafür nötige Vertrauen in die Zusammenarbeit zu stärken. Um das zu schaffen ist es wichtiger als bisher, dass sich Gesetzgeber und Verwaltung, sowie Wissenschaft und

---

[68] Black Hat ist die wichtigste fachliche Veranstaltungsreihe für Informationssicherheit, deren Teilnehmer sich aus den erfahrensten und hochqualifizierten Fachkräften weltweit zusammensetzen.

[69] Vgl. (Black Hat 2017, S. 2)

[70] Vgl. (Black Hat 2017, S. 4ff)

Unternehmen bestmöglich aufeinander abstimmen.[71]

Einer ENISA-Studie zufolge, existieren noch relativ große nationale Unterschiede bei der Entwicklung und Implementierung einer Cybersicherheitsstrategie. Im Dokument „National Cyber Security Strategies (NCSS) Good Practice Guide" wurden, auf Basis von Daten aus insgesamt 17 Staaten (inkl. Österreich) und Interviews, entsprechende Herausforderungen und Lücken identifiziert und ein Überblick hinsichtlich der existierenden NCSS gegeben.[72] Es wurden 15 umfangreiche NCSS-Ziele (mit detaillierten Aufgaben) definiert, die zur erfolgreichen Umsetzung erreicht sein sollen. Aufgrund der damals durchgeführten Analyse, konnte eine Bandbreite von fünf bis 14 bearbeiteten oder erreichten Zielen des jeweiligen Staats festgestellt werden.[73] Der daraus abgeleitete Guide kann den Mitgliedsstaaten inhaltlich eine entsprechende Hilfestellung zur Entwicklung und Etablierung einer Cybersicherheitsstrategie bieten. Vor allem unter dem Aspekt, dass Referenzbeispiele aus einzelnen Ländern beschrieben werden.

Auf Basis einer Erhebung aus dem Jahr 2017 ist die NIS-Richtlinie in den nachfolgenden Mitgliedstaaten bereits umgesetzt worden:

- Deutschland per 29.06 2017 (vgl. Kapitel 2.4.1)
- Tschechische Republik per 01.08.2017

Hinsichtlich der gegebenen Aktualität bzgl. Inkrafttretens des nationalen Gesetzes, ist auch in ausgewählten Medien abermals auf die Umsetzung der NIS-Richtlinie bzw. das NISG hingewiesen worden.[74] Im Rahmen dieser Masterarbeit wurde mit Umsetzungsstichtag 10.5.2018 eine finale Erhebung durchgeführt, die zu folgendem Ergebnis führte:

- Finnland → nationales Gesetz umgesetzt
- Großbritannien → nationales Gesetz umgesetzt
- Kroatien → nationales Gesetz umgesetzt
- Slowakei → nationales Gesetz umgesetzt
- Zypern → nationales Gesetz umgesetzt[75]

Das soll nicht bedeuten, dass in den anderen Mitgliedstaaten noch keine Anstrengungen hinsichtlich einer Umsetzung unternommen wurden. Die NIS-Richtlinie wurde bis dato noch nicht in das jeweilige nationale Recht überführt bzw. es erfolgte keine laufende Informationsweitergabe hinsichtlich des jeweiligen Status. Es liegt jedoch die Vermutung nahe, dass sich die jeweiligen nationalen Umsetzungsmaßnahmen in verschieden weit fortgeschrittenen Phasen bewegen.[76]

---

[71] Vgl. (Kipker 017, S. 147)

[72] Vgl. (ENISA 2016c, S. 11)

[73] Vgl. (ENISA 2016c, S. 51)

[74] Vgl. (Schmid 2018, online)

[75] Vgl. (EUROPÄISCHE KOMMISSION, s.a., online)

[76] Vgl. (Schnider 2017, online)

2.3 NISG in Österreich

Österreich stehen leistungsfähige Infrastrukturen zur Verfügung und es hat ein hohes Niveau der Versorgungsicherheit erreicht. Die Funktionsfähigkeit von Infrastrukturen ist jedoch durch Einflüsse wie z.B. Cyberbedrohungen, Klimawandel, technische Unfälle, Kriminalität / Terrorismus und menschliches Versagen zunehmend gefährdet. Der Schutz solcher KI hat deshalb auch in der Republik Österreich in den letzten Jahren an Bedeutung gewonnen. Trotzdem ist zum Zeitpunkt der Erstellung dieser Masterarbeit noch kein NISG verabschiedet worden, bzw. auch kein Entwurf dazu öffentlich verfügbar gewesen. Aus diesem Grund wird der Fokus in diesem Kapitel stark auf Österreichs „Austrian Program for Critical Infrastructure Protection" (APCIP) gelegt.

Einleitend ist zu sagen, dass Österreich bei Gesetzgebung und Strukturen im Bereich des Schutzes von KI´s bevorzugt einen stark dezentralen Ansatz verfolgt. Dadurch verbleibt ein wesentlicher Anteil der Verantwortung im spezifischen Sektor bzw. beim Betreiber und eine gewisse Flexibilität bleibt erhalten. Wie in Abbildung 8 zu sehen ist, können dadurch aber verhältnismäßig komplexe Verbindungen zwischen relevanten Interessensvertretern und betroffenen Betreibern entstehen.[77]

2.3.1 Chronologische Entwicklung der Cybersicherheit in Österreich

Die Vorstellung des EPCIP im Jahr 2006 durch die Europäische Kommission und die darauffolgende Entwicklung, sind als initialer Impuls zum Aufbau des APCIP anzusehen. Am 2.4.2008 beschloss die österreichische Bundesregierung das APCIP, woraus der „Masterplan APCIP 2008" entstand. Der derzeit aktuelle „Masterplan APCIP 2014" stammt vom 4.11.2014. Darin werden bereits erledigte Arbeiten dokumentiert und der Masterplan auf Basis neuer Erkenntnisse weiterentwickelt.

Der Masterplan wurde damals gemeinsam vom österreichischen BKA und dem „Bundesministerium für Inneres" (BMI) erarbeitet und mit relevanten staatlichen Interessenvertretungen und ausgewählten, strategischen Unternehmen akkordiert. Der Plan ist auf den folgenden Prinzipien aufgebaut:

- Kooperation,
- Subsidiarität,
- Komplementarität,
- Vertraulichkeit,
- Verhältnismäßigkeit

und basiert auf einem „betreiberzentrierten Arbeitsprogramm" sowie dem „All-Hazards-Ansatz"[78].[79] Zentral ist dabei die Unterstützung von strategisch wichtigen österreichischen Firmen bei der Etablierung ausgereifter Sicherheitsarchitekturen

[77] Vgl. (ENISA 2016a, S. 28f)

[78] Ansatz der im Rahmen der Sicherheitsvorsorge das gesamte Spektrum der potenziellen Bedrohungen umfasst.

[79] Vgl. (Bundeskanzleramt Österreich 2015, S. 8)

(Risiko- / Sicherheitsmanagement und „Business Continuity Management“ (BCM)).

Der Schutz von KI´s kann, aus Sicht der österreichischen Regierung, nur in Form eines vertrauensvollen PPP-Modells erfolgreich gelingen. Für das APCIP wurde folgende Leitlinie definiert:

> „*Staat und Wirtschaft leisten gemeinsam einen wesentlichen Beitrag zur Steigerung der Resilienz und Sicherheit Österreichs.*“[80]

Seit April 2008 hat es wesentliche Entwicklungen auf österreichischer Ebene gegeben, die auch durch europäische Aktivitäten gefördert und gefordert wurden:

- Bereits mit der Mitteilung über EPCIP (EU COM(2006) 786) vom 12.12.2006 wurde auf europäischer Ebene ein bedeutender Schritt zum Schutz von europäischer kritischer Infrastrukturen gesetzt.
- Mit 2008 wurde vom Rat der EU die Richtlinie 2008/114/EG zur „Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern“ beschlossen.
- Cybersicherheit beschäftigte Österreichs BMI und das KSÖ seit Herbst 2011 außerordentlich, woraus sich die „Cyber Security Initiative“ entwickelte.[81]
- Österreich hat mit der Meldung an die Europäische Kommission (15.2.2011) EPCIP umgesetzt, auch wenn dies bis 12.1.2011 erforderlich gewesen wäre.
- Die Identifikation der Unternehmen und Organisationen - mit strategischer Bedeutung für Österreich - wurde in Abstimmung mit relevanten Ministerien und Interessenvertretungen per Anfang 2012 abgeschlossen.
- Die „Österreichische Strategie für Cyber Sicherheit" (ÖSCS) wurde im März 2013 von der Regierung beschlossen und sieht weitreichende Maßnahmen zum Schutz von KI´s (Handlungsfeld 4) bzgl. Risiken und Bedrohungen im Cyberspace vor. Im Handlungsfeld 7 (internationale Zusammenarbeit) wird bereits auf die NIS-Richtlinie verwiesen. Es gibt eine Vielzahl an Strukturen und Interessensvertreter, die individuell am Thema Cybersicherheit arbeiten, weshalb Handlungsfeld 1 (Strukturen und Prozesse) einige organisatorische Maßnahmen vorsieht.
- Am 8.5.2013 wurde der Leitfaden „Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich“ der Öffentlichkeit präsentiert und in Folge an alle identifizierten Unternehmen und Organisationen verteilt.
- In der „Österreichischen Sicherheitsstrategie“ (ÖSS) vom 3.7.2013 wird die Regierung aufgefordert, ein gesamtstaatliches Konzept zur Steigerung der Resilienz Österreichs (Wiederherstellung von Staat und Gesellschaft nach Krisen) und zum Schutz von KI´s zu erarbeiten. [82]

---

[80] (Bundeskanzleramt Österreich 2015, S. 4)

[81] Vgl. (KSÖ – Kuratorium Sicheres Österreich, s.a., online)

[82] Vgl. (Bundeskanzleramt Österreich 2015, S. 5)

- Das Arbeitsprogramm der Bundesregierung von Ende 2013 widmet sich im Kapitel „Sicherheit und Rechtsstaat“ dezidiert der Thematik und hält fest:

  > *„Der Schutz kritischer Infrastrukturen (SKI) und die Gewährleistung von »Cyber Sicherheit« sind von besonderer Bedeutung [...].“*[83]

- Mit 2015 wollte sich, laut eigenen Angaben, das BKA auf die Fertigstellung des Entwurfs für ein NISG konzentrieren.[84]
- Die im März 2017 publizierte „Sicherheitsdoktrin des BMI für Österreich 2017 - 2020“ sieht im Handlungsfeld 1 (Steigerung der Resilienz Österreichs) einige strukturell wichtige Maßnahmen vor, die hinsichtlich Cybersicherheit, dem NISG und der NIS-Richtlinie von wesentlicher Bedeutung sind.[85]

Im Sicherheitsprogramm zum Schutz von KI´s gibt es durchaus Interessensgruppen (z.B. CERT, „Staatliche Krisen- und Katastrophenschutzmanagement“ (SKKM)) die ebenso für die Strukturen laut NIS-Richtlinie von Relevanz sein werden. Anhand der folgenden Abbildung 8 ist ersichtlich, dass für das zukünftige NISG spezielle Strukturen nötig sein werden, um eine EU-spezifische Kommunikationsstruktur etablieren zu können. Es ist dabei eine zentrale Herausforderung für die beteiligten Ressorts, die NIS-Richtlinie auf nationaler Ebene umzusetzen und in bestehenden Strukturen (z.B. APCIP) abzubilden.[86]

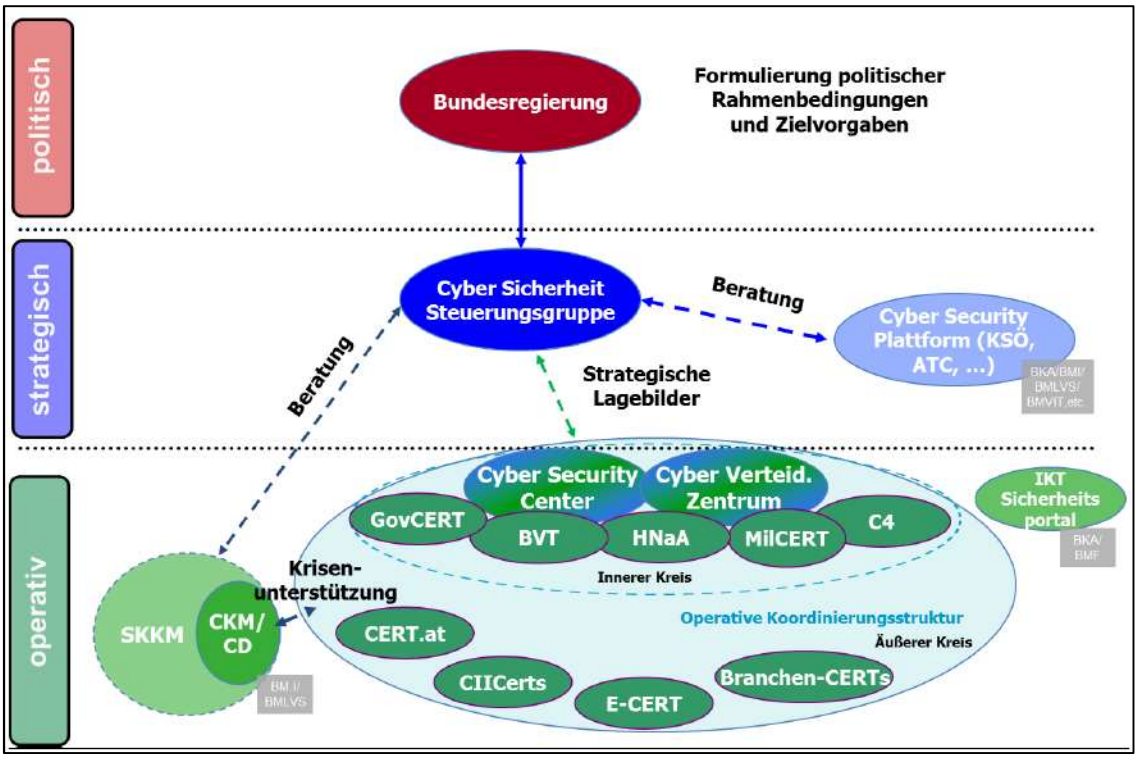


Abbildung 8: Einordnung der »Operativen Koordinierungsstruktur«[87]

[83] (Bundeskanzleramt Österreich 2015, S. 4)

[84] Vgl. (Bundeskanzleramt Österreich s.a., S. 11)

[85] Vgl. (Bundesministerium für Inneres 2017, S. 21ff)

[86] Vgl. (CERT.at 2017, S. 35)

[87] (CERT.at 2017, S. 40)

Der „Innere Kreis Der Operativen Koordinierungsstrukturen“ (IKDOK) hat 2016 den Regelbetrieb aufgenommen. Dieser bildet im Krisenfall, unterstützt durch den „äußeren Kreis“, die direkte Schnittstelle zum „Cyber Krisen Management“ (CKM). Die Mechanismen des CKM orientieren sich an den bereits erprobten Abläufen des SKKM. Dem IKDOK gehören, neben den Vorsitz führenden Stellen Cyber Security Center und Cyber Defense Center, diverse andere staatliche Interessensvertreter an.[88]

Im Zuge der europäischen Übung „Cyber Europe 2016“ wurde vom Veranstalter und Übungsbeobachter festgestellt, dass der IKDOK die ihm übertragenen Aufgaben sowohl inhaltlich, wie auch organisatorisch einwandfrei umgesetzt hat.[89]

Die Vielfalt an Akteuren und Programmen verdeutlicht die Komplexität der Problematik und zeigt zudem auch mögliche Unklarheiten bzgl. der Zuständigkeiten auf. Dabei handelt es sich um eine abstrakte Darstellung, welche die Komplexität in den Verbindungen zwischen den einzelnen Bereichen nur ansatzweise wiedergibt.

Die folgende Abbildung 9 stellt (aus Sicht 2017) einen weitgehend aktuellen zeitlichen Fahrplan zur Umsetzung der NIS-Richtlinie dar. Rot umrahmt die beiden kritischen Zeitpunkte, bei denen es nach aktueller Kenntnis bereits zu Verzögerungen gekommen ist, bzw. noch keine Ergebnisse vorliegen. Diesem Umstand geschuldet, werden auch andere Meilensteine problematisch zu betrachten sein.

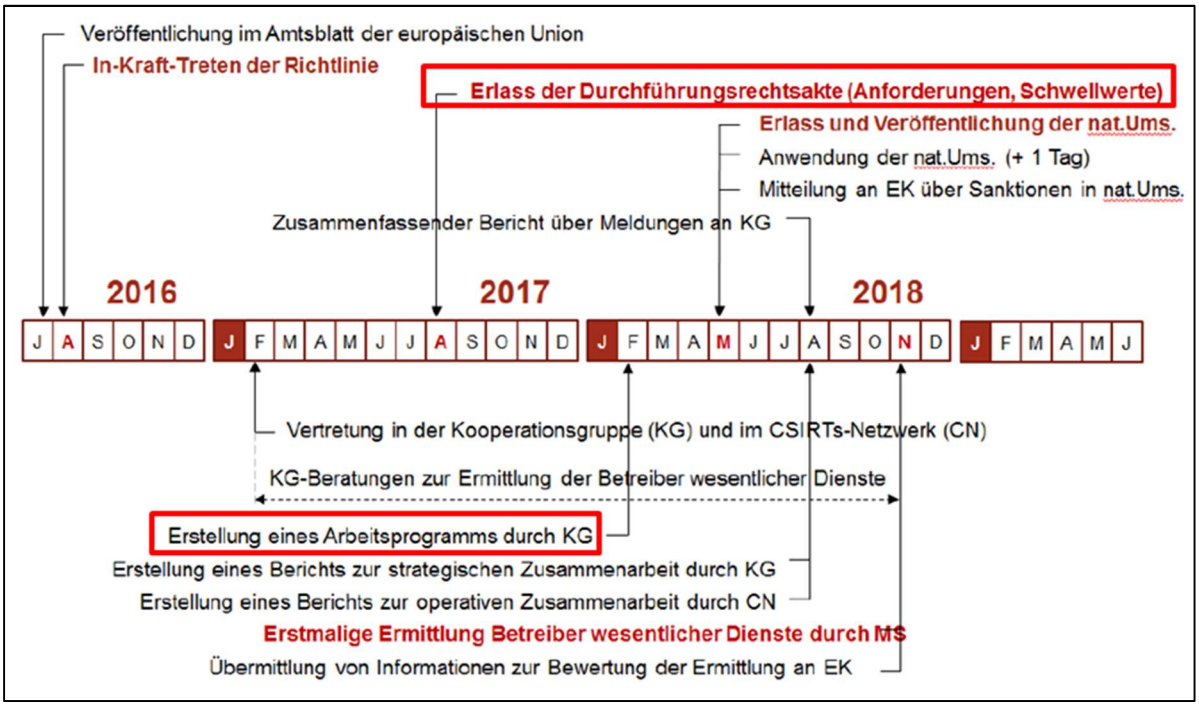


Abbildung 9: Nationale Zeitleiste für NIS-Umsetzung[90]

[88] Vgl. (CERT.at 2017, S. 36)

[89] Vgl. (CERT.at 2017, S. 36)

[90] (Mayer und Schmied 2017, S. 19)

Der Gesetzgebungsprozess in Österreich kann komplex und langwierig sein. Im Rahmen des Gesetzgebungsverfahrens sind sowohl der National- wie auch der Bundesrat einzubinden. Es werden z.B. Beratungen, Berichterstattungen, Debatten und Abstimmungen durchlaufen. Der Bundesrat hat dabei in den meisten Anlassfällen ein Mitwirkungsrecht in Form eines Einspruchs oder Zustimmungsrechts.[91]

Nach aktuellem Kenntnisstand (9.5.2018) liegt noch kein endgültiger Gesetzesentwurf zur Begutachtung oder zum Beschluss vor, weshalb somit klar ist, dass Österreich bis zur Frist 9.5.2018 kein NISG verabschiedet hat. Weitere Verzögerungen auf nationaler Ebene können in diesem Kontext auch nicht ausgeschlossen werden. Mit entsprechenden Strafen oder zumindest Strafandrohungen von Seiten der EU sollte diesbezüglich gerechnet werden, wenngleich diese vornehmlich symbolischen Charakter haben werden.

2.3.2 Schutz kritischer Infrastrukturen in Österreich

Einen tiefergehenden Einblick in die Prinzipien und strategische Zielsetzungen des APCIP sollen die nachfolgenden Erklärungen vermitteln, um daraus gegebenenfalls Erkenntnisse im Bezug zum zukünftigen NISG zu gewinnen:

- Operator based Approach (betreiberbasierter Ansatz)
  Österreich verzichtet bewusst auf eine Aufzählung der kritischen Sektoren, da die Meinung vertreten wird, dass die Wechselwirkungen einer komplexen Wirtschaft nicht ausreichend abbildbar seien. KI´s werden deshalb auf Basis eines betreiberorientierten Zugangs identifiziert. Die strategischen Unternehmen, welche KI´s betreiben, werden nach definierten Kriterien erfasst und in einer Liste für „Austrian Critical Infrastructure“ (ACI) erfasst.
- Subsidiarität und Selbstverpflichtung der Unternehmen
  Eigentümer und Betreiber der strategischen Unternehmen sind primär selbst verantwortlich für die Aufrechterhaltung der Leistungen und den Schutz der Anlagen. An deren Versorgungsfunktion besteht ein nationales Interesse, weshalb sich diese Unternehmen in einer (freiwilligen) Selbstverpflichtung zu erhöhter Resilienz und damit zu Schutzstandards bekennen. Diese Standards wären für die jeweilige Branche gemeinsam zu definieren. Für die Festlegung der Rahmenbedingungen muss sich die Politik verantwortlich zeigen, damit ein vorgegebenes Schutzniveau der jeweiligen Branche erreicht wird.
- Komplementarität
  Bestehende Maßnahmen und Pläne für Österreich sollen weiter genutzt und neuen - sich kontinuierlich ändernden - Bedrohungen angepasst werden.
- Vertraulichkeit
  Informationen sollen vertraulich ausgetauscht werden und das auch nur in einer Informationstiefe, welche die spezielle Aufgabenstellung erfordert.
- Kooperation
  Die Zusammenarbeit aller relevanten Interessensvertreter soll einen angemessenen Beitrag zur Umsetzung und Weiterentwicklung von APCIP liefern.

[91] Vgl. (Republik Österreich - Parlamentsdirektion, s.a., online)

- Verhältnismäßigkeit
  Maßnahmen und resultierende Kosten müssen in einem ausgeglichenen Verhältnis zu Risiko und den Möglichkeiten zur Gefahrenmitigation stehen.
- „All-Hazards-Ansatz“
  KI´s sollen vor einem möglichst breiten Spektrum möglicher Risiken abgesichert werden. Diese Maßnahmen sind aus einem umfassenden Sicherheitsverständnis abzuleiten und sollten alle relevanten Risiken adressieren.[92]

Von zentralem Interesse ist gegenwärtig, auf Basis welcher Faktoren in Österreich die betroffenen Unternehmen ausgewählt wurden, die in APCIP zu berücksichtigen sind. Aufgrund folgender Rahmenbedingungen wurde die ACI-Bundesliste erstellt, bzw. ist die Identifikation der Unternehmen erfolgt:

- Ist es ein österreichweit agierendes Unternehmen oder Organisation?
- Ist die Gütergruppeneinteilung nach NACE System?[93]
- Gibt es ein Vergleich Statistik Austria zu Marketing Daten?
- Ausgenommen sind Bau, Beherbergungswesen, Bildungseinrichtungen und internationale Organisationen
- Es ist kein regionaler und lokaler Versorger
- Es ist ein „lebendes Dokument“ und unterliegt laufenden Änderungen
- Die konsolidierte Liste ist „Eingeschränkt“ bzw. „Unter Verschluss“[94]

Folgende Auswahlkriterien sind zur ACI Identifizierung festgelegt worden:

- Daseinsvorsorge
- Wirtschaftsstandort
- EKI
- Spezialisierte Leistungen und Exporte (Weltmarktführer)
- Faktor zeitliche Dimension
- Operative Unternehmen und keine Holdings
- Diversifizierte Unternehmen in der „vorgelagerten“ Wirtschaftsstufe[95]

Exemplarisch sind folgende Methoden zur ACI Identifizierung angewendet worden:

- ÖNACE[93]-Klassifikation
- KRITIS Methode mit Redundanz, Umsatz und Mitarbeiter
- Gegencheck mit sektoralen Fachlisten
- Gegencheck mit „Firmen ABC“ und Ranking der „Top 1000 Unternehmen“
- Gegencheck mit Studie „Internationale Leitbetriebe in Österreich“
- Akkordierung mit Fachministerien und Interessenvertretungen[96]

---

[92] Vgl. (Bundeskanzleramt Österreich 2015, S. 8)

[93] „NACE“ steht für „Nomenclature générale des activités économiques dans les communautés européennes“. ÖNACE ist die österreichische Version der europäischen Wirtschaftstätigkeitenklassifikation NACE Rev.2.

[94] Vgl. (Bundeskanzleramt Österreich 2016, S. 6)

[95] Vgl. (Bundeskanzleramt Österreich 2016, S. 7)

[96] Vgl. (Bundeskanzleramt Österreich 2016, S. 8)

Aus der Erhebungsphase ist die ACI-Liste gemäß Abbildung 10 hervorgegangen.

	APCIP		L.APCIP
A: Land- und Forstwirtschaft, Fischerei	☑	(5)	
B: Bergbau und Gewinnung von Steinen und Erden	☑	(5)	
C: Herstellung von Waren	☑	(170)	☑
D: Energieversorgung	☑	(20)	☑
E: Wasserversorgung, Abwasser- und Abfallentsorgung	☑	(2)	☑
G: Handel, Instandhaltung und Reparatur von Kraftfahrzeugen	☑	(46)	
H: Verkehr und Lagerei	☑	(28)	☑
J: Information und Kommunikation	☑	(27)	☑
K: Erbringung von Finanz- und Versicherungsdienstleistungen	☑	(17)	☑
M: Erbringung von wissenschaftlichen Dienstleistungen	☑	(6)	
N: Erbringung von sonstigen wirtschaftlichen Dienstleistungen	☑	(4)	
O: Öffentliche Verwaltung, Verteidigung, Sozialversicherung	☑	(30)	☑
Q: Gesundheits- und Sozialwesen	☑	(39)	☑

Abbildung 10: ACI Branchenübersicht nach ÖNACE unterteilt[97]

Eine Summe von 399 Unternehmen (Abbildung 10 - Rot umrahmt) für den Standort Österreich ist ein realitätsnaher Indikator, um abzuschätzen wie viele Unternehmen eventuell von der NIS-Richtlinie direkt betroffen sein könnten. Es muss jedoch klar festgehalten werden, dass APCIP nicht mit der NIS-Richtlinie gleichzusetzen ist.

2.3.3 Relevante Gesetze in Österreich

Folgende in Österreich existierende Gesetze / Verordnungen könnten von der NIS-Richtlinie betroffen sein, wobei diese Aufzählung als nicht taxativ zu verstehen ist:

- Datenschutzgesetz DSG bzw. Datenschutz-Anpassungsgesetz 2018
- E-Government - Gesetz - E-GovG
- Energieversorgungssicherheitsgesetz
- Gesundheitstelematikgesetz - GTelG
- Informationssicherheitsgesetz – InfoSiG
- Informationssicherheitsverordnung - InfoSiV
- Signatur- und Vertrauensdienstegesetz - SVG
- Telekommunikationsgesetz - TKG
- IKT-Konsolidierungsgesetz – IKTKonG[98]

Es liegt der Schluss nahe, dass es im Zuge einer nationalen Gesetzgebung durchaus zu Überschneidungen jeglicher Art mit anderen Gesetzen kommen kann und daraus verschiedenste Probleme erwachsen werden.

[97] (Bundeskanzleramt Österreich 2016, S. 9)

[98] Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 48f)

2.3.4 Initiativen in Österreich zur NIS-Richtlinie

Der Wirtschaftssektor „Elektrizitätswirtschaft“ hat sich in Österreich als einer der Ersten strukturiert an den Analyse- und Bewertungsprozess herangewagt und diesen auch durchlaufen. Dieser Prozess durchleuchtet im Detail die Risiken für die nationale Versorgungssicherheit mit Strom, in Zusammenhang mit der Nutzung von IKT-Infrastrukturen. Durch die diversen, nationalen, interagierenden Sicherheitsstrategien wie z.B. APCIP, ÖSCS wurde die obige Initiative von einigen Ministerien und bedeutenden Branchenvertretern durchgeführt. Diese Initiative zur Risikoanalyse erfolgte im Herbst 2012 wobei die Durchführung im Jahr 2013 erfolgte. Diese Risikoanalyse war ein erster Schritt zur Umsetzung von vorgeschlagenen Maßnahmen aus den Sicherheitsprogrammen. Hinsichtlich Qualität und Quantität kann dieses Dokument durchaus für andere Sektoren als strukturelles Vorbild dienen. Entsprechende Erkenntnisse, wie die Verwundbarkeit der IKT und die Gefahren rund um den Datenschutz führten zu der Einsicht, dass es neuer Sicherheitsarchitekturen bedarf.[99] Beispielsweise war die Schaffung eines brancheneigenen CSIRT – zur Früherkennung und Bearbeitung von Cyberattacken - eine der vielen Maßnahmen. Das „Austrian Energy CERT“ ist ebenso Teil jener Maßnahmen, die bzgl. NIS-Richtlinie auch von der ENISA empfohlen wurde.[100]

Auch wenn KMU von der NIS-Richtlinie nicht direkt bzw. nur in geringem Ausmaß betroffen sind, so hat das „Österreichische Sicherheitsforschungsförderprogramm“ (KIRAS[101]) das Projekt „GENESIS Guideline für Behörden und KMU-Anbieter strategischer Services zur risikoorientierten Implementierung der NIS-Richtlinie“ initiiert. Ziel von GENESIS ist es:

> *„Das Vorhaben hat zum Ziel, ein Risikomanagement-Framework für die von der NIS-Richtlinie betroffenen KMUs zu konzipieren. Dieses Framework soll sowohl den in der Richtlinie formulierten Anforderungen als auch dem Ergebnis des aktuell laufenden nationalen Gesetzwerdungsprozesses genügen.*“[102]

Mit diesem Projekt bzw. der darin zu erarbeitenden Studie werden sowohl die Betreiber von KI´s wie auch Behörden adressiert. Auf der einen Seite soll dadurch eine kosteneffiziente, modulare und individuelle Umsetzung der NIS-Richtlinie für die KMUs ermöglicht werden und andererseits eindeutige, inhaltliche Mindestanforderungen als Orientierungshilfe für KMU und Behörden geschaffen werden.

Da in Österreich auch eine Vielzahl an IT-SP, aus dem KMU-Segment, in den relevanten Sektoren aktiv sind, kann dieses Projekt GENESIS auch durchaus wertvolle Hilfestellung für die IT-SP leisten. Eventuell kann dieses Framework Anregungen für IT-SP liefern, wie die eigenen Strukturen bzw. Prozesse „NIS-Ready“ gemacht werden könnten. Es ist ebenso vorstellbar, dass es IT-SP auf Basis dieses GENESIS Frameworks erleichtert wird

---

99 Vgl. (E-Control 2014, S. 2)

100 Vgl. (CERT.at 2018, online)

101 KIRAS ist ein nationales Programm zur Förderung der Sicherheitsforschung in Österreich und unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der Sicherheit Österreichs und seiner Bevölkerung.

102 (KIRAS Sicherheitsforschung 2017, online)

nötige Vorhaben zur Erfüllung der NIS-Richtlinie bei den BwD ins Gedächtnis zu rufen bzw. zu initiieren.

2.3.5 Ausstehende Maßnahmen in Österreich für NISG

Wie in Kapitel 2.2.4 festgehalten, gab es in jüngerer Vergangenheit innerhalb der Mitgliedsstaaten hinsichtlich der Entwicklung und Implementierung einer Cybersicherheitsstrategie noch größere Unterschiede. Österreich ist als eines der 17 untersuchten Länder im Mittelfeld zu finden, wenn ein Bezug auf die Quantität der erreichten Empfehlungsziele genommen wird. Von den 15 empfohlenen Zielen der ENISA wurden für Österreich 12 Ziele, als teil oder vollständig erfüllt, angezeigt.[103]

Es soll folgend exemplarisch aufgezeigt werden, welche Maßnahmen von Seiten der österreichischen Regierung nun konkret noch zu ergreifen sind, um das nationale NISG auf Basis der Vorgaben der NIS-Richtlinie fristgerecht umzusetzen:

- Meldewege für verpflichtende und freiwillige Meldungen für die BwD sind zu entwickeln, zu etablieren und relevanten Interessensgruppen zu kommunizieren.
- Es sind nötige NIS-Behörde(n) und ein SPOC als zentrale Ansprechstelle für die anderen Mitgliedstaaten und Vertreter im PPP-Modell einzurichten.
- Es ist zu entscheiden und dann zu definieren, auf Basis welcher Kriterien (z.B. Schwellenwerte je Branche) die Meldeverpflichtungen etabliert werden.
- Betroffene Betreiber sind zu identifizieren und per Bescheid zu informieren.
- Festlegung und gegebenenfalls Definition von Sicherheitsanforderungen bzw. Normierungsmöglichkeiten für BwD.
- Es sind entsprechende Sanktionen gemäß NIS-Richtlinie festzulegen.
- Unterstützung bei der Etablierung von Branchen-CERTs und Integration in das EU-CSIRT-Netzwerk sowie in den österreichischen CERT-Verbund.
- Verbesserung der Kommunikationswege für den Fall eines Ausfalls von Energie (Blackout) oder von Telekommunikationseinrichtungen (Internet).
- Erlassung des nationalen Gesetzes (NISG) zur NIS-Richtlinien Umsetzung.

2.4 IT-Sicherheitsgesetz in Deutschland

Wie in der aktuellen Cyber-Sicherheitsstrategie von Deutschland bereits in den einleitenden Worten festgehalten, ist Sicherheit oftmals mehr als trügerisch.

> *„Die Digitalisierung eröffnet Chancen, birgt Risiken und braucht daher Vertrauen. Eine umfassende Sicherheit ist nicht erreichbar, ein Missbrauchspotenzial wird stets existieren. Aufgabe des Staates und der Wirtschaft ist es, die Grundlagen für dieses Vertrauen zu schaffen. Sicherheit ist hierbei ein wesentlicher Aspekt.“*[104]

Mit den jeweiligen Gesetzen hat Deutschland jedoch bereits einige Schritte unternommen,

---

[103] Vgl. (ENISA 2016c, S. 51)

[104] (Bundesministerium des Innern 2016, S. 4)

um den Worten auch Taten folgen zu lassen.

Deutschland verfolgt (anders als Österreich) bzgl. Gesetzgebung und Strukturen im Bereich des Schutzes von KI´s einen stark zentralisierten Ansatz. Hier sind wesentliche Verantwortungen an zentrale, sektorübergreifende Behörden übertragen worden, was klare und einheitliche Strukturen schafft. Nach ENISA ist dieser Ansatz jedoch in anderen untersuchten EU-Mitgliedsstaaten wie z.B. Tschechische Republik und Frankreich die Ausnahme. Die meisten Länder verfolgen den dezentralen Ansatz.[105] Hervorzuheben ist, dass Deutschland und die Tschechische Republik bereits das nationale NIS-Gesetz verabschiedet haben (vgl. Kapitel 2.2.4).

In den folgenden Unterkapiteln wird deshalb ein Überblick über die Situation in Deutschland gegeben, um nachfolgend einen Vergleich mit der Situation in Österreich durchführen zu können.

2.4.1 Chronologische Entwicklung Cybersicherheit in Deutschland

Anhand der verfügbaren Literatur wurde festgehalten, dass Deutschland in der Vergangenheit beim Umgang mit Informationssicherheitsrisiken oft auf informelle und kooperative Strategien setzte. Inzwischen wird von diesem Prinzip abgegangen, und es hat ein Institutionalisierungs- und Vergesetzlichungsprozess Einzug gehalten. Die folgende Aufzählung gibt einen Überblick, welche Anstrengungen unternommen wurden bzw. werden, um die Cybersicherheit zu gewährleisten:[106]

- Der Staat verabschiedete 1990 das „Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik". Darin wurden dem BSI zur Förderung der Sicherheit in der IT grundlegende, zentrale Aufgaben übertragen.
- Mit Juli 2005 wurde vom Bundesministerium des Innern der „Nationale Plan zum Schutz der Informationsinfrastrukturen" publiziert.
- Im Jahr 2007 wurde der „Umsetzungsplan" (UP) KRITIS, ein PPP-Modell zum Schutz „Kritischer Infrastrukturen" (KRITIS) in Deutschland, mit ca. 30 Organisationen ins Leben gerufen.
- Mit der Überarbeitung des „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes" (BSIG) im Jahr 2009 wurde dem BSI zunehmend eine Schlüsselposition bei der Ausarbeitung und Implementation von rechtlichen Vorgaben zur Informationssicherheit eingeräumt.
- Im Februar 2011 beschloss die deutsche Bundesregierung die „Cyber-Sicherheitsstrategie für Deutschland". Darin wurden wesentliche Weichenstellungen für die zukünftige Cyber-Sicherheitspolitik getroffen.[107]
- Im Juli 2015 sind schließlich mit dem „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-SiG) entsprechende Regelungen erlassen worden, damit im gesellschaftlichen Bereich eine Stärkung des Schutzniveaus für

[105] Vgl. (ENISA 2016a, S. 30f)

[106] Vgl. (Wischmeyer 2016, S. 1f)

[107] Vgl. (Bundesministerium des Innern 2011, S. 6ff)

- IT-Systeme und Netzwerke erreicht wird.
- Im Jahr 2016 wurde die deutsche Cyber-Sicherheitsstrategie überarbeitet.[108]
- Mit Mai 2016 ist der erste Teil (Korb 1) der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-KritisV) in Kraft getreten. Darin wird für die Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation geregelt, welche Anlagen den KRITIS gemäß IT-SiG zuzurechnen sind. Gesamt haben 205 Betreiber im Korb 1 rund 550 Anlagen beim BSI registrieren lassen.
- Mit Juni 2017 ist der zweite Teil (Korb 2) der BSI-KritisV, in dem die noch offenen Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr geregelt werden, in Kraft getreten. Seitens des BSI wurde bis Ablauf der Frist Ende 2017 mit zusätzlichen 800 bis 1.000 zu registrierenden Anlagen gerechnet.[109]
- Mit 30.6.2017 ist zudem das "Gesetz zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (NIS-Richtlinien-UG) in Kraft getreten. Wobei die Umsetzung in deutsches Recht aufgrund der Analogie zum IT-SiG unkompliziert geschehen sollte.

Vor allem mit diesen in Kraft getretenen Gesetzen und Verordnungen sind die zentralen Elemente der NIS-Richtlinie für Deutschland verbindlich geworden. Da in Deutschland, im Gegensatz zu Österreich, bereits relevante Gesetze zur Umsetzung der NIS-Richtlinie existieren, wird in dieser Masterarbeit auf eine eigene tiefergehende Analyse hinsichtlich des Schutzes von KI´s (wie in Kapitel 2.3.2) verzichtet.

2.4.2 Zentrale Inhalte der Gesetze in Deutschland

Das IT-SiG und das NIS-Richtlinien-UG können im Vergleich zu vielen anderen Gesetzen durchaus als unkonventionell bezeichnet werden. Was sie so besonders macht ist, dass es sich um sogenannte „Mantelgesetze“[110] handelt. Diese sind per Definition dafür vorgesehen, dass in einem Rechtsetzungsakt andere existierende Gesetze geändert, neu geschaffen oder gegebenenfalls aufgehoben werden können. Dabei werden über einen Änderungsbefehl einzelne Wörter, Satzteile oder Sätze in den betroffenen Stammgesetzen verändert. Die jeweiligen Auswirkungen des Mantelgesetzes können üblicherweise erst dann verstanden werden, wenn die Änderungen mit dem bisherigen Wortlaut des Stammgesetzes verglichen wird.[111]

Das IT-SiG und NIS-Richtlinien-UG sind in vielen Bereichen sehr übereinstimmend. Mit dem NIS-Richtlinien-UG wird deutlich, dass sich für Deutschland die bisherigen gesetzgeberischen Vorarbeiten im Bereich der IT-Sicherheit ausgezahlt haben. Ob nun das IT-SiG Einfluss auf die NIS-Richtlinie genommen hat oder Deutschland einfach zeitgerecht wesentliche Kernelemente der absehbaren NIS-Richtlinie in das nationale IT-

[108] Vgl. (Bundesministerium für Inneres 2017, S. 10f)

[109] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017b, S. 62f)

[110] Wegen seines artikelorientierten Aufbaus wird das Mantelgesetz auch als Artikelgesetz bezeichnet.

[111] Vgl. (Bundesministerium der Justiz 2008, S. 191)

SiG einfließen hat lassen, sei dahingestellt. Die vom NIS-Richtlinien-UG betroffenen Unternehmen müssen somit keinen doppelten Implementierungsaufwand befürchten. Es können lediglich im Zuge der Konkretisierung der BSI-KritisV Nachschärfungen notwendig werden. Durch den internationalen Bezug können hauptsächlich Aufwände für die beteiligten Behörden entstehen.[112]

Das deutsche IT-SiG umfasst neun Sektoren mit hinterlegten Kriterien, wobei aktuell, gemäß BSI-KritisV, sieben der neun Sektoren (vgl. Abbildung 11) im Fokus sind.[113]

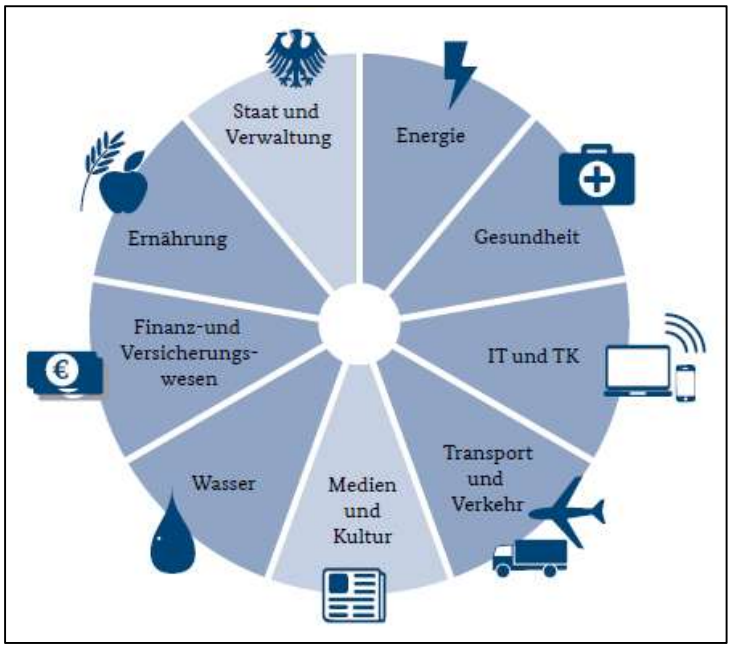


Abbildung 11: KRITIS-Sektoren des IT-Sicherheitsgesetzes[114]

Für Telekom-Provider gelten für gewisse Basisdienste eigene Sonderregelungen, wie auch für Vertreter von Staat und Verwaltung. Für den Sektor „Medien und Kultur" hat der Bund keine Regelungskompetenz, sowie auch für die Landes- und Kommunalbehörden im Sektor „Staat und Verwaltung". Für Bundesbehörden gibt es seit der BSIG-Novellierung 2009 vergleichbare Pflichten.[115]

Diese sieben relevanten KRITIS-Sektoren in obiger Abbildung 11 sind weitgehend auch ident mit den vorgegebenen sieben NIS-Sektoren (vgl. Abbildung 6). Abweichend enthält das IT-SiG den Sektor „Finanz- und Versicherungswesen" der in der NIS-Richtlinie in zwei getrennten Sektoren enthalten ist. Zudem sieht das IT-SiG, anders als die NIS-Richtlinie, den Sektor „Ernährung" auch als relevant an, weshalb in Deutschland somit tendenziell mehr Unternehmen (als von der EU vorgesehen) umfasst werden.

In Deutschland erfolgt die Festlegung nicht durch eine zentrale staatliche Stelle, sondern KRITIS-Unternehmen müssen sich selbst identifizieren und im Anschluss beim BSI melden. Dafür steht ein online „Melde- und Informationsportal" bereit. Dabei wurden in

[112] Vgl. (Kipker 2017, S. 147)

[113] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017b, S. 48)

[114] (Bundesamt für Sicherheit in der Informationstechnik 2017b, S. 48)

[115] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017b, S. 48)

den jeweiligen BSI-KritisV (Korb 1 und 2) entsprechende kritische Dienstleistungen je Sektor definiert (vgl. Abbildung 12). Mittels dieser Abgrenzungen haben die betroffenen Unternehmen die Möglichkeit, sich gezielt auf die relevanten Bereiche zu konzentrieren.

Sektor	Kritische Dienstleistungen
Energie	Stromversorgung, Gasversorgung, Versorgung mit Kraftstoff und Heizöl, Versorgung mit Fernwärme
Wasser	Trinkwasserversorgung, Abwasserbeseitigung
Ernährung	Versorgung mit Lebensmitteln
IKT	Sprach- und Datenübertragung, Datenspeicherung und -verarbeitung
Gesundheit	Medizinische Versorgung, Versorgung mit Arzneimitteln und Medizinprodukten
Finanz- und Versicherungswesen	Zahlungsverkehr und Kartenzahlung, Bargeldversorgung, Kreditvergabe, Geld- und Devisenhandel, Wertpapier- und Derivatehandel, Versicherungsleistungen
Transport und Verkehr	Transport von Gütern, Transport von Personen im Nahbereich, Transport von Personen im Fernbereich

Abbildung 12: Kritische Dienstleistungen der KRITIS-Sektoren[116]

Die vorhin genannten Gesetze ändern und ergänzen in dem Zusammenhang neben dem BSIG auch das Telekommunikationsgesetz und das Telemediengesetz (vgl. Kapitel 2.4.3). Konkret erhält das BSI durch die Änderungen neue Aufgaben und Befugnisse. Vor allem kann es damit auch außerhalb der deutschen Bundesverwaltung etwaigen Defiziten im Bereich der IT-Sicherheit wirksam begegnen.

Die folgenden Inhalte wurden auf Basis IT-SiG und NIS-Richtlinien-UG extrahiert und stellen zentrale Elemente zur nationalen Umsetzung der NIS-Richtlinie dar:

- KMU sind gemäß Gesetzgebung als KRITIS-Betreiber ausgenommen.
- Das NIS-Richtlinien-UG erweitert die Befugnisse des BSI im Hinblick auf die geplanten „Mobile Incident Response Teams“ (MIRT).
- Laut NIS-Richtlinien-UG wird die Nutzung personenbezogener Daten neu geregelt. Das BSI darf bei Maßnahmen personenbezogene Daten erheben und verarbeiten, soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen NIS erforderlich und angemessen ist.
- Die Betreiber von KI´s sind verpflichtet, spätestens zwei Jahre (bis Mai 2018) nach Inkrafttreten des IT-SiG, angemessene organisatorische und technische

[116] (Atug, Mettke-Pick und Pohl 2017, online)

Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Komponenten, -Systeme oder -Prozesse zu treffen, die zur Funktionsfähigkeit der von ihnen betriebenen KI maßgeblich sind. Dabei ist der „Stand der Technik" einzuhalten.[117]

- Eine Definition anwendbarer Sicherheitsstandards („Stand der Technik") kann durch KRITIS-Betreiber oder einem Branchenverband sektorweit vorgeschlagen werden. Das BSI prüft, ob diese branchenspezifischen Sicherheitsstandards (B3S) den gesetzlichen Anforderungen genügen, und entscheidet darauf aufbauend.
- Die KRITIS-Betreiber müssen, gemäß IT-SiG, alle zwei Jahre nachweisen, dass die getroffenen Maßnahmen zum Schutz der KI´s den Gesetzesanforderungen genügen. Es bestehen dafür die folgenden Möglichkeiten:
  - Interne Audits oder Prüfungen durchführen.
  - Prüfung und Zertifizierung durch eine externe unabhängige Stelle.

  Diese internen / externen Aktivitäten sowie eventuelle Sicherheitsmängel sind dem BSI zu melden. Das BSI führt gegebenenfalls Kontrollen durch und kann die Vorlage der Ergebnisse und die Mängelbeseitigung verlangen.
- Gemäß IT-SiG ist der als bedeutend anzusehende Versorgungsgrad anhand branchenspezifischer Schwellenwerte für jede, wegen ihrer Bedeutung als kritisch betrachtete, Dienstleistung im jeweiligen Sektor zu bestimmen.[118]
- Mit der BSI-KritisV sollen Unternehmen anhand messbarer und nachvollziehbarer Kriterien prüfen können, ob sie in den Regelungsbereich des IT-SiG fallen. Der Regelschwellenwert liegt bei 500.000 versorgten Personen, wobei der sektorspezifische Schwellenwert als wesentlich zu sehen ist.
- Auf Basis des IT-SiG kann eine Ordnungswidrigkeit in speziellen Fällen (vorsätzlich oder fahrlässig einer vollziehbaren Anordnung zuwiderhandelnd) mit einer Geldbuße von bis zu 100.000 Euro geahndet werden.[119]
- Das IT-SiG sieht Meldepflichten bei IT-Vorfällen vor. In der Regel erfolgen diese anonym. Im Falle, dass ein vollständiger Systemausfall droht, ist auch der Unternehmensname dem BSI zu melden. Laut Regierungsschätzungen wird nach BSI-KritisV die Meldepflicht ca. 2.000 Unternehmen betreffen.[120]
- Gemäß IT-SiG müssen KRITIS-Betreiber eine Kontaktstelle in ihrem Unternehmen nennen. Diese fungiert als Ansprechpartner für das BSI. Zusätzlich kann innerhalb eines Sektors eine übergeordnete zentrale Kontaktstelle benannt werden, welche den Kontakt zum BSI hält.
- Das NIS-Richtlinien-UG ergänzt das IT-SiG hinsichtlich AdD. In Zukunft unterliegen diese auch Mindestanforderungen und Meldepflichten. Es wird davon ausgegangen, dass in Deutschland 500 bis 1.500 Unternehmen von der Neuregelung hinsichtlich AdD betroffen sein werden.[121]

---

[117] Vgl. (Bundesministerium der Justiz und für Verbraucherschutz 2017, S. 9)

[118] Vgl. (Bundesministerium der Justiz und für Verbraucherschutz 2017, S. 13)

[119] Vgl. (Bundesministerium der Justiz und für Verbraucherschutz 2017, S. 15)

[120] Vgl. (xmera e.K. 2017, S. 7)

[121] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017a, online)

Vor allem im Bereich der Meldepflichten und der Kategorisierung werden in Deutschland konkrete Hilfestellungen gegeben. Wie in Abbildung 13 dargestellt, werden von Seiten des BSI für die Betreiber von KI´s, welche unter die BSI-KritisV fallen, generell drei unterschiedliche Fälle von IT-Störungen beschrieben.

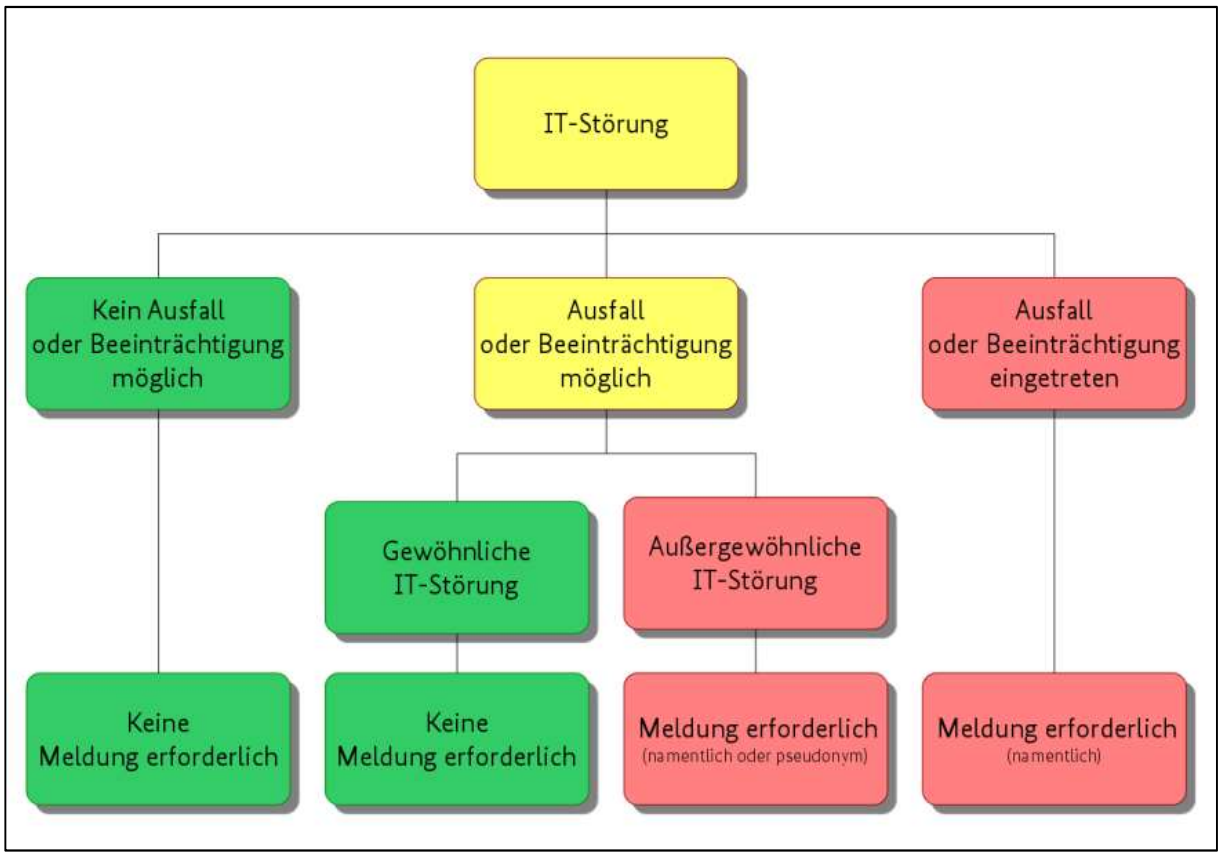


Abbildung 13: Meldekriterien für IT-Störungen gemäß IT-SiG[122]

Tritt eine IT-Störung auf, sind die folgenden drei Fälle zu unterscheiden:

1. Es ist nicht möglich das es zu einem Ausfall oder einer Beeinträchtigung der kritischen Dienstleistung kommt. Somit ist keine Meldung erforderlich.
2. Es besteht die Möglichkeit, dass es zu einem Ausfall oder einer Beeinträchtigung der kritischen Dienstleistung kommt. Eine Meldung ist nur dann erforderlich, wenn es eine außergewöhnliche IT-Störung ist.
3. Die kritische Dienstleistung ist ausgefallen oder beeinträchtigt. Somit ist nun eine namentliche Meldung zwingend erforderlich.[123]

In der nachfolgenden Abbildung 14 ist eine, gemäß BSI, Einteilung auftretender IT-Störungen dargestellt. Auf Basis dieser Kategorisierung, ob nun gewöhnliche oder außergewöhnliche IT-Störung, kann eine grundlegende Entscheidung getroffen werden ob eine entsprechende Meldung an die relevanten Stellen abzusetzen ist.

[122] (Bundesamt für Sicherheit in der Informationstechnik 2016, online)

[123] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2016, online)

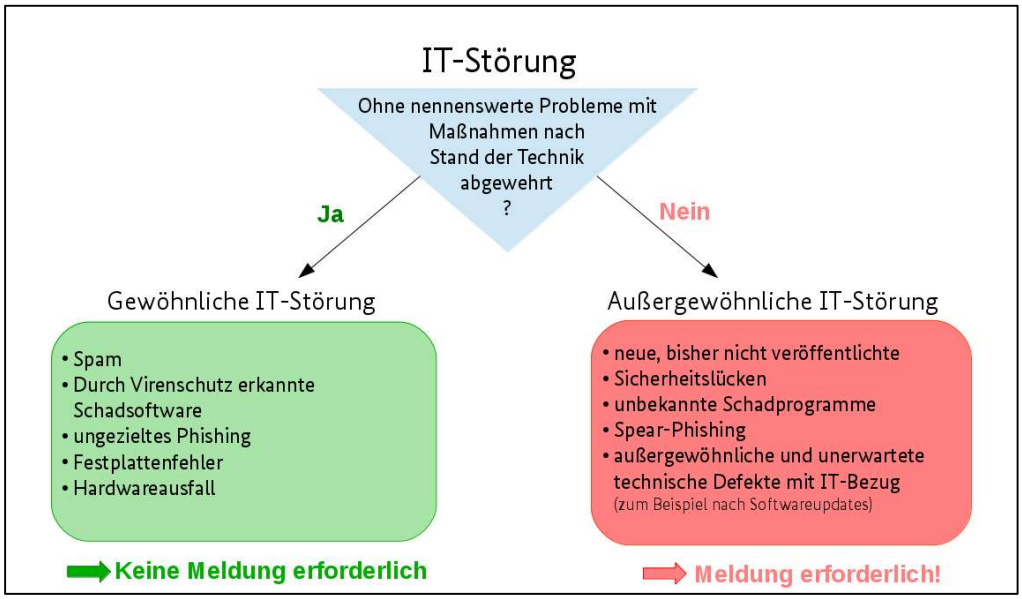


Abbildung 14: Unterschied von gewöhnlicher zu außergewöhnlicher IT-Störung[124]

Anhand der praxisorientieren Ausgestaltung können betroffene Unternehmen schon heute konkrete Richtlinien und Abläufe entwickeln und etablieren.

2.4.3 Relevante Gesetze in Deutschland

In Deutschland gibt es, wie in Österreich, eine Vielzahl an Gesetzen / Verordnungen, die von der NIS-Richtlinie betroffen sind und angepasst wurden. Die Abbildung 15 zeigt, in welche acht deutschen Stammgesetze das IT-SiG (in-)direkt eingegriffen hat. Hier war neben dem BSIG besonders der Energiesektor mit Anpassungen in Atomgesetz (AtG) und dem Energiewirtschaftsgesetz (EnWG) betroffen.

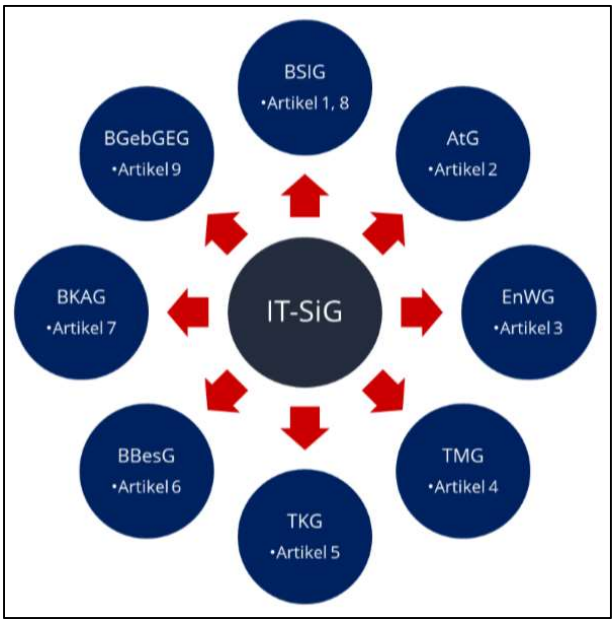


Abbildung 15: Im IT-SiG enthaltene Stammgesetz[125]

[124] (Bundesamt für Sicherheit in der Informationstechnik 2016, online)

[125] (xmera e.K. 2017, S. 4)

Aufgrund der danach veröffentlichten NIS-Richtlinie im Jahr 2016, war es in Deutschland erforderlich, dass nachträgliche NIS-Richtlinien-UG zu verabschieden, welches abermals Auswirkung auf ausgewählte Gesetze hatte (vgl. Abbildung 16).

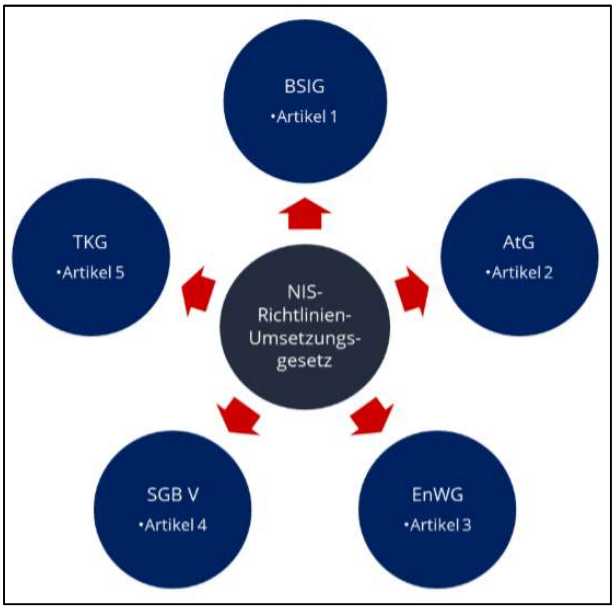


Abbildung 16: Im NIS-Richtlinien-UG enthaltene Stammgesetze[126]

Diese Anpassungen waren, aufgrund der bereits durchgeführten Vorarbeiten, hinsichtlich der Auswirkungen qualitativ und quantitativ überschaubar.

2.4.4 Initiativen in Deutschland zur NIS-Richtlinie

Auch wenn das BSI per Gesetz stärkere Befugnisse erhalten hatte, setzt es sich weiterhin dafür ein, dass die im IT-SiG verankerte, mit dem UP KRITIS seit 2007 gelebte kooperative Zusammenarbeit auch weiterhin verfolgt wird. In Deutschland wurde dazu bzgl. eines nationalen Sicherheitsstandards, bereits ein gemeinsamer Weg beschritten. Als branchenspezifische Sicherheitsstandards sind B3S typischerweise keine durch Normungsinstitut wie ISO oder DIN erstellten, Standards. Ein B3S ist als Konzept anzusehen, dass von Branchenvertretern gemeinsam definiert wird, um geeignete Sicherheitsanforderungen zu erfassen und welches bei der Umsetzung unterstützen soll.

Wie im deutschen IT-SiG definiert, können BwD und ihre Branchenverbände (bevorzugt Branchenarbeitskreise (BAK) des UP KRITIS) entsprechende B3S zur Gewährleistung der Sicherheitsanforderungen erarbeiten und vorschlagen. Die Prüfung kann danach zentral beim BSI beantragt werden. Im Fall der Eignung wird dieser Standard vom BSI, gegebenenfalls unter Mitwirkung anderer zuständiger Aufsichtsbehörden (z.B. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)), anerkannt. In Abbildung 17 ist der grundsätzliche B3S Entstehungsprozess elementar dargestellt.[127]

[126] (xmera e.K. 2017, S. 6)

[127] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2016, online)

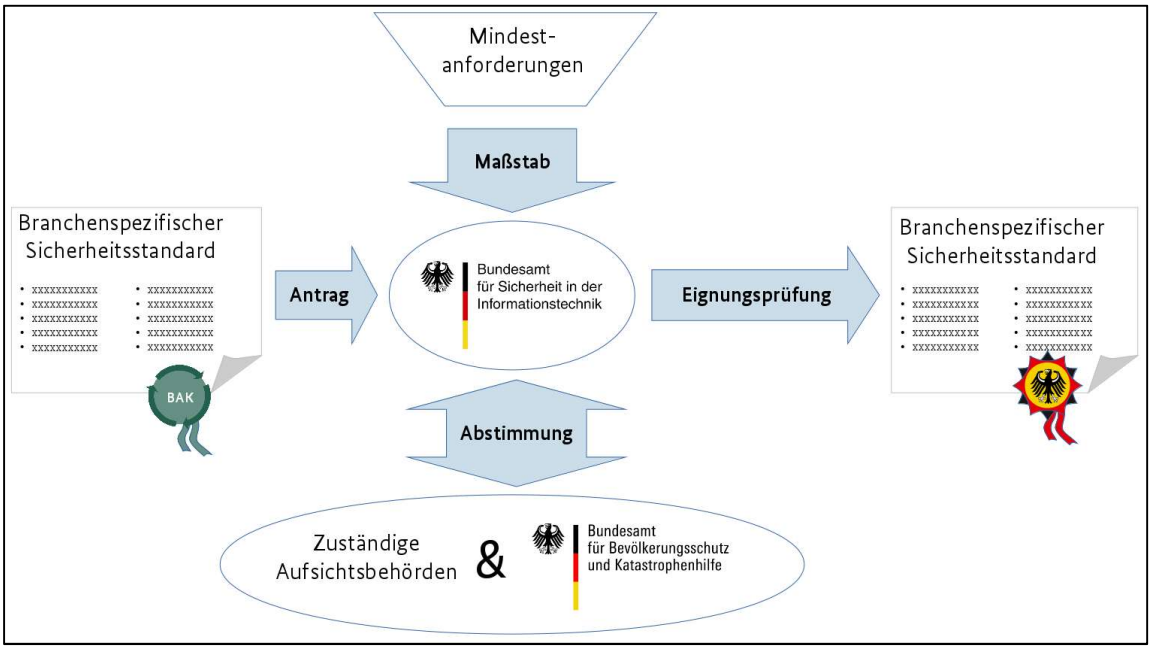


Abbildung 17: Eignungsprüfung für B3S[128]

Es besteht aber keine gesetzliche Verpflichtung zur Erarbeitung eines solchen B3S. Es ist als eine Chance zu sehen, dass sich die Branche durch eigene Fachexpertise (im jeweiligen Sektor) selbst den „Stand der Technik" ausformuliert. Nach der erfolgreich festgestellten Eignung des B3S, können sich die betroffenen KRITIS-Betreiber an diesem ausrichten und implementieren. Die BwD haben im Falle des Audits weitestgehend Rechtssicherheit betreffend dem „Stand der Technik", wenn sie sich nach einem anerkannten B3S prüfen lassen. Spätestens alle zwei Jahre ist jedoch zu überprüfen, ob bzw. in welchem Umfang die im B3S getroffenen Annahmen und Beschreibungen noch dem aktuellen Stand entsprechen.

Als zentrale Stelle kann das BSI dabei eine beratende Rolle bei der Erarbeitung von B3S einnehmen. Dazu kann es, abgestimmt mit dem BBK und anderen relevanten Institutionen, eine Orientierungshilfe bzgl. der Inhalte und Anforderungen herausgeben. Auf Basis dieser Orientierungshilfe können die B3S erarbeitet werden. Die aktuellste Version wurde als Dokument „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG" mit 10.01.2018 in der Version 1.0 veröffentlicht.[129] Da es sich um ein „lebendes" Dokument handelt, werden Änderungen von relevanten Aspekten / Kriterien bei Rückmeldung in zukünftige Versionen eingearbeitet. In der zuletzt erfolgten Überarbeitung der B3S-Orientierungshilfe sind exemplarisch die folgenden wesentlichen Anpassungen vorgenommen worden:

- Aufnahme einer Prozessbeschreibung
  Die detaillierte Beschreibung des Erstellungs-, Einreichungs- und Prüfprozesses sowie der Veröffentlichung eines B3S.
- Deutlichere Trennung der Rollen in der Erstellung von B3S
- Einbeziehung von Standards in der Erstellung von B3S

[128] (Bundesamt für Sicherheit in der Informationstechnik 2016, online)

[129] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017d, online)

Es werden Hilfestellungen zur Einbeziehung bestehender:
  - allgemeiner Standards (z.B. BSI IT-Grundschutz, ISO 27001)
  - branchenspezifischer Standards (z.B. C5-Katalog, ISO 62442)

  als Unterstützung zur B3S-Erstellung geboten.
- Zusammenfassung von "Schutzziele" zu einem gemeinsamen Punkt
  Die verschiedenen KRITIS - branchenrelevanten - und IT-Schutzziele sind verständlicher definiert und im gemeinsamen Kontext erläutert.[130]

Abschließend haben BwD die Erfüllung der Sicherheitsanforderungen mindestens alle zwei Jahre gegenüber dem BSI nachzuweisen, wobei dies als Prüfung oder Sicherheitsaudit möglich ist. Das BSI behält sich das Recht vor, bei aufgedeckten Mängel in Abstimmung mit den zuständigen Aufsichtsbehörden die Beseitigung dieser zu verlangen.

Außerdem wurde in Deutschland dem Umstand Rechnung getragen, dass immer mehr Unternehmen Cloud Services beziehen. Zu diesem Zweck hat das BSI 2016 einen Cloud Computing Anforderungskatalog namens „Cloud Computing Compliance Controls Catalogue“ (C5) erarbeitet, welcher laufend weiterentwickelt wird. Dieser enthält Mindestanforderungen (114 Sicherheitsanforderungen in 17 Bereichen) welche professionelle Cloud Services für geschäftsrelevante Daten und Prozesse erfüllen müssen. Großteils sind die Anforderungen wiederum aus anderen etablierten Standards (z.B. ISO 27000-Reihe, Cloud Controls Matrix) abgeleitet. Eine Prüfung, bzw. der Nachweis, ob die Anforderungen des C5 durch den Cloud Service Provider erfüllt wurde, ist durch einen Wirtschaftsprüfer zu erbringen. Zwecks Prüfungsdurchführung und Berichterstattung werden internationale Prüfungsstandards (z.B. ISAE 3000, ISAE 3402) herangezogen, um Cloud-Kunden für das eigene Risikomanagement einen validen Inhalt zu liefern.[131]

Hinsichtlich Cloud Services in Verbindung mit der BSI-KritisV ist zudem eine differenzierte Betrachtung nötig. Ein Anbieter von Cloud Services kann sowohl:

1. selbst als KRITIS-Betreiber klassifiziert sein, oder
2. als IT-SP für einen KRITIS-Betreiber agieren.

Für Fall 1 gelten die Vorgaben wie im IT-SiG definiert. Im Fall 2 ist der Sachverhalt komplexer. Wenn der IT-SP zentrale Systeme oder Prozesse betreibt, die für kritische Dienstleistungen maßgeblich sind, ist der IT-SP mittelbar (nicht direkt) betroffen. Hier muss der BwD im Zuge des eigenen IT-Risikomanagements eine Bewertung des Outsourcings vornehmen. Die Verantwortung und Pflichten können laut IT-SiG, auch bei einer Auslagerung informationstechnischer Systeme, nicht an Dritte (z.B. IT-SP) überbunden werden und verbleiben beim Betreiber. Dieser muss somit, z.B. über relevante Zertifizierungen (z.B. ISO 27001) oder mittels externen Audits, die Einhaltung der Anforderungen sicherstellen.[132]

---

[130] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2018, online)

[131] Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017c, S. 19)

[132] Vgl. (Adelmeyer, Petrick und Teuteberg, 2017, S. 114f)

Bezugnehmend zur Hypothese H 1 kann in diesem Fall festgehalten werden, dass die Gesetzgebung in Deutschland (vgl. IT-SiG) eine Übertragung der Verantwortung und Pflichten durch den BwD an einen Dritten nicht zulässt.

Hinsichtlich der Zusatzfrage Z 2 ist hier ein wesentlicher Inhalt zur Beantwortung enthalten. Als wirksame Steuerungsmaßnahmen kann sich der BwD nach einem spezifischen Managementsystem ausrichten (z.B. ISO 27001) und gegebenenfalls einer relevanten Zertifizierung unterziehen. Im Rahmen dessen, wird üblicherweise auch relevanten Themen wie z.B. Lieferantenbeziehungen, Handhabung von Informationssicherheitsvorfällen eine zentrale Bedeutung eingeräumt. Alternativ sind Vereinbarungen bezüglich der Durchführung von externen Audits beim leistungserbringenden Dritten (z.B. IT-SP) ein zielführendes Instrument. Jedoch ist auch hier darauf hinzuweisen, dass die letztgültige Verantwortung nur beim BwD verbleiben kann.

2.4.5 Ausstehende Maßnahmen in Deutschland

Auch wenn die europäische NIS-Richtlinie aus Sicht Deutschlands verhältnismäßig umfangreich ausgefallen ist, so wird dennoch nicht erwartet, dass sich im Speziellen für die Betreiber von KI erheblicher Handlungsbedarf ergibt. In folgenden Bereichen sind weitestgehend Überschneidungen bzw. gleichlautende Regelungen erkennbar:

- Für die Sektoren der KI werden in den deutschen Gesetzen keiner Änderung oder Erweiterung notwendig werden.
- Bei TOM haben betroffene Firmen keine wichtigen Änderungen zu erwarten.
- Für die Betreiber halten sich Änderungen bzgl. der Meldepflicht in engen Grenzen.

Deutschland hat mit dem IT-SiG bereits, der NIS-Richtlinie vorauseilend, eine nationale Gesetzgebung gestartet. Die europäische und deutsche Gesetzgebung ist relativ gut aufeinander abgestimmt, weshalb nur Feinjustierungen zu erwarten sind. Die deutschen Betreiber von KI´s werden in diesem Sinne das IT-SiG plangemäß umsetzen, bzw. haben es bereits getan. Daran anknüpfend sind eventuell erforderliche Detailanpassungen, laut NIS-Richtlinien-UG, einfacher vorzunehmen. Der deutsche Gesetzgeber hat jedoch mit einem deutlich höheren Aufwand zu rechnen. Besonders die in der NIS-Richtlinie enthaltene Umsetzung, des erweiterten europäischen Kooperationsrahmens zur Cybersicherheit, wird Behörden und gesetzgebenden Institutionen noch Arbeit bereiten.

Wie auch schon in Kapitel 2.2.4 festgehalten, ist Deutschland eines von sehr wenigen EU-Mitgliedsländern, das bereits ein nationales Gesetz zur Umsetzung der NIS-Richtlinie verabschiedet hat. Durch das vergangene und aktuelle rechtspolitische, organisatorische und technische Handeln, im Bereich der IT- bzw. Cybersicherheit, kann sich Deutschland als gut vorbereitet auf die Herausforderungen im neuen europäischen Cybersicherheits-Bereich betrachten.[133]

[133] Vgl. (Kipker 2016, S. 4)

2.5 Vergleich von Österreich und Deutschland

Auch wenn die beiden Länder auf den ersten Blick sehr ungleich wirken, so sind hinsichtlich IKT-Nutzung - vor allem bei Unternehmen - doch einige Parallelen feststellbar. Wie in Abbildung 18 ersichtlich ist, sind österreichische (rot) wie auch deutsche Unternehmen (grün) mit je 6% bei der Nutzung von Cloud Computing Diensten deutlich unter dem EU-Durchschnitt von 11% (blau). Die Unternehmen beider Länder sind jedoch laut EU-Statistik bzgl. Digitalisierung überdurchschnittlich weit entwickelt.

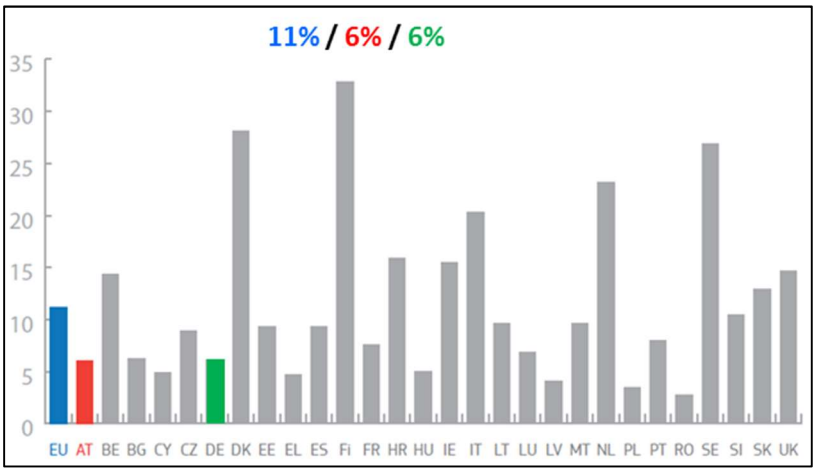


Abbildung 18: Ländervergleich - Cloud-Computing-Dienste in Unternehmen[134]

Auch hinsichtlich des Rechtsverständnisses sind die beiden Länder Österreich und Deutschland im gleichen Rechtskreis (Deutsches Recht) anzusiedeln, wodurch auch rechtlich ein entsprechendes Naheverhältnis gegeben ist, wie die Abbildung 19 zeigt.

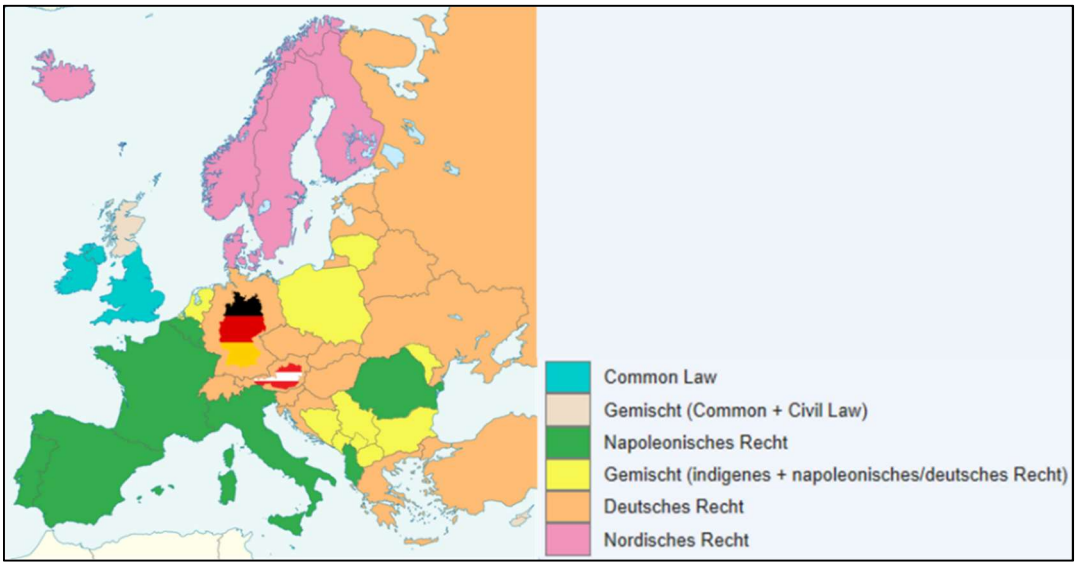


Abbildung 19: Rechtskreise in Europa[135]

Gemäß einer Aussage des Wiener IT-Rechtsexperten Dr. Lukas Feiler, SSCP, CIPP/E (von

[134] eigene Darstellung (EUROPÄISCHE KOMMISSION 2015b, S. 4) und (EUROPÄISCHE KOMMISSION 2015a, S. 4)

[135] eigene Darstellung (Wikipedia 2018, online)

Baker & McKenzie[136]), kann eine eindeutige Verschränkung von Deutschland und Österreich im Rahmen der Gesetzgebung interpretiert werden.

> *„Was auch immer der deutsche Gesetzgeber - gerade im Bereich der Vorratsdatenspeicherung, aber auch in anderen Bereichen des Internetrechts - tut, dem folgt der österreichische Gesetzgeber meistens sehr bereitwillig.“*[137]

Derzeit hat z.B. das Thema um den „Bundestrojaner“, bzw. das „Sicherheitspaket“/ „Überwachungspaket“, eine gewisse öffentliche Aufmerksamkeit in Österreich erlangt. Wie schon 2017 von ExpertInnen prognostiziert, sind hier Parallelen in der Gesetzgebung zum „Überwachungsgesetz“ von Deutschland erkennbar.[138] Auch in der aktuellsten Regierungsvorlage[139] wird das Vorgehen von vielen ExpertInnen kritisch betrachtet.[140]

Im Rahmen der Literaturanalyse wurden vorhandene Gesetze, Verordnungen oder Berichte beider Länder gesichtet und verglichen. Da das Thema eine hohe inhaltliche Bandbreite aufweist, wurde eine Selektion durchgeführt und der Fokus auf die bedeutendsten Kernelemente gelegt. Auf Basis dieser NIS-Themen wurde ein Vergleich von Österreich und Deutschland durchgeführt, eine Bewertung vorgenommen sowie mögliche Auswirkungen auf IT-SP wie auch BwD beschrieben.

2.5.1 Bestimmung der Betreiber wesentlicher Dienste

Im Rahmen der NIS-Richtlinie wird nicht konkret definiert, auf welchem Wege die BwD ermittelt werden sollen. Es werden ausschließlich grobe Rahmenbedingungen vorgegeben und die tatsächliche Aufgabe an die EU-Mitgliedstaaten übertragen.

Da Deutschland bereits entsprechende Gesetze verabschiedete, wurde zur Bestimmung von BwD eine Methodik festgelegt. Ein zentrales Bewertungskriterium ob ein deutscher Betreiber als national kritisch eingestuft werden kann, ist (nach IT-SiG) der Anteil des Unternehmens am Versorgungsgrad der Gesellschaft. Dafür ist es erforderlich, die kritischen (Teil-)Prozesse zu identifizieren, um sie dann mittels quantitativer Schwellenwerte zu beurteilen. Diese sind in den verabschiedeten deutschen BSI-KritisV detailliert berechnet und festgehalten. Anhand der sektorspezifischen Schwellenwerte sind die Unternehmen angehalten, sich selbstständig dahingehend zu prüfen, ob sie ein BwD sind.

Im Vergleich zu den bisher geltenden nationalen Vorgaben in Deutschland ist ein wesentlicher Unterschied, dass die NIS-Richtlinie explizit auch „öffentliche Einrichtungen“ adressiert, sofern sie einen wesentlichen Dienst betreiben.[141]

---

[136] International tätige Anwaltskanzlei im Bereich des Wirtschaftsrechts und eine der global größten Kanzleien.

[137] (Felser 2015, online)

[138] Vgl. (Wimmer 2017, online)

[139] Vgl. (Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz 2018, S. 1ff)

[140] Vgl. (Sulzbacher 2018, online)

[141] Vgl. (Universität Passau, s.a., online)

Ein zentraler Punkt des in Österreich noch offenen NISG wird die Ermittlung der nationalen BwD sein, die eine wesentliche bzw. kritische Dienstleistung erbringen. In Österreich wären innerstaatlich folgende Herangehensweisen denkbar:

1. Durch den Gesetzgeber könnte eine Liste der Betreiber erstellt und veröffentlicht werden. Von Österreich wurde diese Herangehensweise bereits im Rahmen des APCIP gewählt aus dem die ACI-Liste hervorgegangen ist (vgl. Abbildung 10). Ein Nachteil könnte sein, dass durch Veröffentlichung der Liste der Schutz der BwD nur mehr beschränkt gegeben ist.
2. Es könnten vom Gesetzgeber spezifische Schwellenwerte festgelegt werden, auf deren Basis Unternehmen selbst entscheiden müssen, ob sie dem Bereich der BwD zurechenbar sind. Diese Variante wurde in Deutschland mit der BSI-KritisV umgesetzt. Diese Herangehensweise hat primär für Betreiber den Nachteil, dass bis zum Anlassfall keine volle Rechtssicherheit gegeben ist, ob das Unternehmen tatsächlich (nicht) im Anwendungsbereich liegt.
3. Es werden Kriterien bzw. Schwellenwerte durch den Gesetzgeber definiert und dieser identifiziert somit auch selbst die betroffenen Betreiber. Hier wären die betroffenen Betreiber per Bescheid davon in Kenntnis zu setzen.

Dabei wird zu berücksichtigen sein, dass laut österreichischem „Bundesgesetz über die Grundsätze der Deregulierung" bei der Umsetzung von EU-Rechtsakten darauf zu achten ist, dass vorgegebene Standards nicht ohne Grund übererfüllt werden.[142]

Die KSÖ-ExpertInnen sind der Meinung, dass ein künftiges NISG in Österreich den Adressatenkreis klar benennen sollte. Die Herangehensweise zur Bestimmung, wie in Deutschland umgesetzt, wurde teils kritisch gesehen, da zu wenig Klarheit auf Gesetzesebene vermutet wird.[143] Im ExpertInnenkreis wurde auch keine gemeinsame Sichtweise dazu entwickelt, weshalb die nachstehende KSÖ-Empfehlung eher vage ausfällt:

> *„[...] Sinnvoll ist es, den Adressatenkreis zuerst auf die Betreiber der nationalen kritischen Infrastrukturen zu beschränken. Gemäß APCIP zählen die Ministerien und Behörden des Bundes auch dazu. Im Zuge der Konkretisierung des Gesetzestextes könnte eine Fachgruppe [...] darüber beraten und entscheiden,*
>
> - *welche Kriterien im Sinn des Cybersicherheitsgesetzes maßgeblich sind für die Definition eines nationalen kritischen Betreibers im Sinne des Gesetzes*
> - *ob und wie gegebenenfalls die ACI-Liste angepasst wird [...]"*[144]

Einer Selbsteinschätzung zur Ermittlung - analog deutschem Gesetz - stehen KSÖ-ExpertInnen eher ablehnend gegenüber. Eine Ermittlung anhand definierter Kriterien, bzw. Schwellenwerte sowie Identifizierung durch den Gesetzgeber (Herangehensweise 3 auf der vorherigen Seite) wäre ein praktikabler Ansatz.

---

142 Vgl. (Bundeskanzleramt Österreich 2017, S. 1)

143 Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 14)

144 (KSÖ – Kuratorium Sicheres Österreich 2016, S. 15)

Für die IT-SP ist die zukünftige Herangehensweise zur Bestimmung von BwD indirekt von Bedeutung, jedoch nicht sonderlich beeinflussbar. Werden Unternehmen als BwD identifiziert, so können IT-SP davon ausgehen, dass ihnen entsprechende NIS-Vorgaben und Verpflichtungen vorgeschrieben werden.

2.5.2 Definierte Schutzziele

In der NIS-Richtlinie sowie den deutschen Gesetzen, sind vier übergeordnete Schutzziele bzgl. Sicherheit von NIS bzw. bei Störungen definiert. Dabei haben BwD angemessene TOM zur Sicherstellung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme oder -Prozesse zu treffen, um die Funktionsfähigkeit der KI zu schützen. Diese genannten Ziele dienen zur Definition, worauf Maßnahmen im Bereich der Cybersicherheit auszurichten sind, um nachfolgend zu überprüfen, ob die entsprechenden Vorgaben auch erreicht wurden. Folgende drei Elemente bilden die Eckpfeiler des „CIA-Triad“ (= Schutzziel-Trias):

1. Confidentiality (Vertraulichkeit)
2. Integrity (Integrität)
3. Availability (Verfügbarkeit)[145]

Gleichzeitig bilden sie auch die Basis für die ÖSCS. Den ursprünglichen Schutzziel-oberbegriffen wurden in den letzten Jahren weitere hinzugefügt. Als zwei weitere übergeordnete Schutzziele (bzw. Basisschutzziele) können folgende angesehen werden:

1. Contingency (Kontingenz)
2. Transparency (Transparenz)

Darüber hinaus sind weitere Schutzziele anerkannt worden, die aber den oben genannten Oberbegriffen bzw. der „CIA-Triad“ zuordenbar sind:

- Anonymity (Anonymität)
- Accountability (Zurechenbarkeit) / Nonrepudiation (Nicht-Abstreitbarkeit)
- Authenticity (Authentizität)
- Reliability (Verlässlichkeit)[146]

Laut den ExpertInnen des KSÖ können aus diesen generellen Schutzzielen spezifische Vorgaben / Kennzahlen abgeleitet werden. Die daraus zu entwickelnden Schwellenwerte wären konkret messbar und würden sich für die Wirkungsüberprüfung der Sicherheitsmaßnahmen eignen. Derartige Schutzziele könnten z.B.

- als Mindestsicherheitsanforderungen verstanden werden,
- Auskunft darüber geben ab wann das Gemeinwohl existenziell gefährdet ist oder

[145] (Bedner und Ackermann 2010, S. 323)

[146] Vgl. (Bedner und Ackermann 2010, S. 323ff)

- als Schwellenwerte eine Meldeverpflichtung auslösen.

Für Österreich ist das Thema im KSÖ-Whitepaper als Empfehlung an das NISG formuliert.[147]

Für BwD wäre es durchwegs zukunftssicherer, wenn im nationalen Gesetz mehr als nur die vier definierten Schutzziele der NIS-Richtlinie enthalten sind. In Deutschland wurde dies noch nicht umgesetzt und so betroffenen Betreibern auch keine Übererfüllung auferlegt. Da im KSÖ-Whitepaper aber festgehalten wurde, dass die klassische „CIA-Triad" inzwischen überholt ist, sollten im NISG auch weitere Schutzziele berücksichtigt werden.

Den IT-SP´s kann mit jedem weiteren, über die Mindestanforderungen hinausgehenden, Schutzziel eine neue Herausforderung bei Monitoring, Reporting, etc. der IT-Systeme und -Prozesse erwachsen. Im Falle etablierter Systematiken, bzw. eines Managementsystems zur Bewältigung der „CIA-Triad", würden sich die darüberhinausgehenden Aufwände vermutlich in einem überschaubaren Rahmen bewegen.

2.5.3 Branchenspezifische Sicherheitsstandards

Es wird in der NIS-Richtlinie darauf hingewiesen, dass Mitgliedsländer eine Anwendung europäischer bzw. international anerkannter Normen und Spezifikationen für die Sicherheit von NIS fördern sollen. Das hat ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart zu erfolgen.[148] In einer EU-Mitteilung wurde die Unterstützung der Pläne zur Einrichtung eines europäischen Cybersicherheitszertifizierungsrahmens von Weltniveau mitgeteilt, mittels diesem das Vertrauen in digitale Lösungen gestärkt werden soll.[149] Dieses Bestreben würde somit im Einklang mit der NIS-Richtlinie stehen und wäre für die einzelnen Staaten durchaus von Interesse.

Laut konkreter Vorgaben der NIS-Richtlinie sind vom Mitgliedstaat entsprechende Maßnahmen für die BwD vorzugeben. Dies ist in folgendem Artikel 14 (1) der NIS-Richtlinie definiert:

> „*Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, [...].*"[150]

Ob sich Österreich und Deutschland in eine europäisch harmonisierte Richtung orientieren werden bleibt abzuwarten. Es gibt in beiden Ländern jedenfalls Überlegungen wie, bzgl. Zertifizierungen und Branchenstandards, vorgegangen wird.

---

147 Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 18f)

148 Vgl. (Amtsblatt der Europäischen Union 2016, S. 23)

149 Vgl. (Council of the EU 2017, s.p.)

150 (Amtsblatt der Europäischen Union 2016, S. 20)

In Deutschland wurden bereits Strukturen und Vorgaben für branchenspezifische Sicherheitsstandards in Form von B3S etabliert (vgl. Kapitel 2.4.4). In der Orientierungshilfe zur Erarbeitung eines B3S, wird auch zur Einbeziehung anderer internationaler und branchenunabhängiger Normen und Standards wie z.B. ISO 27000-Reihe oder BSI IT-Grundschutz angeregt. Die Orientierungshilfe zum B3S zeigt ein Szenario auf, um einen B3S als deutsche DIN-Norm oder möglicherweise als ISO-Norm (z.B. zwecks europäischer Harmonisierung) weiter zu entwickeln.[151]

In Österreich sind die ExpertInnen noch geteilter Meinung. Gemäß KSÖ-ExpertInnen wird dem Prinzip zugestimmt, dass ein umfassendes Risikomanagement (bzw. ISMS) erforderlich ist, aber bzgl. der konkreten Form der Umsetzung herrscht noch Uneinigkeit. Tendenziell kann, laut KSÖ-Whitepaper, festgehalten werden, dass die Anwendung bestimmter Verfahren und Methoden nicht im NISG, sondern anders geregelt werden soll (z.B. über Verordnung oder Standard). Etwas eindeutiger ist es bei der Frage, ob es für bestimmte Verfahren und Methoden eine Zertifizierungspflicht geben soll.[152] Die österreichische Industriellenvereinigung (Interessensvertretung) ist dazu folgender Meinung:

> *„Die NIS-RL sollte für Österreich [...] das akkordierte Maximum an gesetzlicher Verpflichtung darstellen, darüber hinaus sind brancheninterne Lösungen staatlichen bzw. gesetzlichen Regelungen vorzuziehen, z. B. die Erarbeitung von branchenspezifischen Standards [...].“*[153]

Diese Aussage tendiert in jene Richtung wie es auch in Deutschland mit den B3S etabliert wurde, bzw. wie es im Rahmen der Risikoanalyse der österreichischen Elektrizitätswirtschaft (vgl. Kapitel 2.3.4) durchgeführt wurde.

Für BwD kann dieses Thema bzgl. Systeme und Prozesse, als auch Aufwand bzw. Kosten von zentraler Bedeutung sein. Die Orientierung an bestehende, international etablierte Standards (z.B. ISO 27000-Reihe) kann dabei als relativ zukunftssicher angesehen werden, wie es auch im Fall von Deutschland vorgelebt wird. Hier nehmen Betreiber mit relevanten Zertifizierungen eine vorteilhaftere Position ein.

Ähnliches gilt auch für IT-SP. Es ist absehbar, dass BwD auch von den eigenen (externen / internen) Dienstleistern gewisse Zertifizierungen oder prüfbare Systeme einfordern werden, um möglichst durchgängig den Vorgaben zu entsprechen.

Mit Bezug zur Zusatzfrage Z 2 kann eine zielgerichtete Antwort abgeleitet werden. Mit dem Verweis auf den „Stand der Technik“ bzgl. der zu ergreifenden TOM´s wird es für die BwD ein pragmatischer Weg sein, sich an einem branchenspezifischen Standard oder einer anerkannten Norm zu orientieren. Dabei werden Dritte, die einen wesentlichen Dienst für den BwD erbringen, mehr in die Abläufe des BwD einzubinden sein, um die erforderliche Steuerung verbessern zu können.

---

151 Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017d, S. 12)

152 Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 55)

153 (KSÖ – Kuratorium Sicheres Österreich 2016, S. 43)

2.5.4 Klassifikation von IT-Sicherheitsvorfällen und Meldepflicht

Hinsichtlich der Klassifikation von IT-Sicherheitsvorfällen im Rahmen der CERT-Arbeit können grundsätzlich folgende drei Beweggründe unterschieden werden:

1. Beweggrund: Als Grundlage zur Entscheidungsfindung
2. Beweggrund: Um eine standardisierte Überblicksbeschreibung zu bekommen
3. Beweggrund: Zur Schaffung einer normalisierten Datenbasis über IT-Vorfälle[154]

Zur erfolgreichen Zusammenarbeit der CERT / CSIRT auf nationaler und EU-Ebene wird es von Bedeutung sein, sich auf ein gemeinsames Klassifikationsmodell zu einigen und dieses umzusetzen. Dabei werden zentrale Vorgaben durch die ENISA erwartet. Gemäß NIS-Richtlinie muss auf jeden Fall eingehalten werden, dass die letztgültige Meldepflicht beim jeweiligen BwD verbleibt. Wie folgend in NIS-Richtlinie - Artikel 16 (5) beschrieben:

> „*Nimmt ein Betreiber wesentlicher Dienste für die Bereitstellung eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung ist, die Dienste eines Dritten [...] in Anspruch, so ist jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, von diesem Betreiber zu melden.*“[155]

Die Meldepflicht ist in Deutschland unkompliziert. Bei eingetretenem Ausfall / Beeinträchtigung (= mehr als 50% des Schwellenwertes reduziert) der kritischen Dienstleistung muss, wie auch bei möglichem Ausfall / Beeinträchtigung durch eine außergewöhnlichen IT-Störung, eine Meldung abgesetzt werden (vgl. Abbildung 13). Die Meldepflicht wird wegen der NIS-Richtlinie so angepasst, dass nicht die Schwere des IT-Vorfalls im Fokus steht, sondern die Beeinträchtigung der bereitgestellten Dienstleistung..[156] In Deutschland wird zwischen gewöhnlichen und außergewöhnlichen IT-Störungen unterschieden (vgl. Abbildung 14).

Analog zum Gesetz muss die Meldung einer relevanten IT-Störung unverzüglich nach deren Erkennung erfolgen (ohne schuldhaftes Zögern). Dabei ist wichtig, dass alle Erkenntnisse an das BSI zu melden sind, welche zum Zeitpunkt der Meldung dem Betreiber vorliegen. Falls im Rahmen einer unverzüglichen Meldung noch nicht alle verpflichtenden Angaben gemacht werden können, so ist diese als Erstmeldung zu klassifizieren. Entsprechende Folge- bzw. Abschlussmeldungen sind nachzuliefern. Eine wichtige Kernaussage dabei ist:

> „*Für die Erstmeldung gilt grundsätzlich Schnelligkeit vor Vollständigkeit.*“[157]

In Summe sind 34 Meldungen seit Einführung der Meldepflicht (nach IT-SiG) bis

---

154 Vgl. (Grobauer, Kossakowski und Schreck 2016, S. 18)

155 (Amtsblatt der Europäischen Union 2016, S. 22)

156 Vgl. (Universität Passau s.a., online)

157 (Bundesamt für Sicherheit in der Informationstechnik, s.a., online)

30.06.2017 beim BSI eingelangt.[158] Zukünftig wird es hinsichtlich Akzeptanz und Qualität von großer Bedeutung sein, dass die Meldewege und die Meldeinhalte klar vorgegeben und zweckmäßig sind.

Das für Deutschland verpflichtende Meldeformular ist inhaltlich bereits sehr ausgereift. Dies kann jedoch zu Beginn einer relevanten IT-Störung zu umfangreich bzw. detailliert sein. Grundsätzlich ist das Formular in sieben Kapitel gegliedert, welche die administrativen und fachspezifischen Aspekte abdecken.

Auf europäischer Ebene kann, wie in Kapitel 2.2.2 in Abbildung 7 dargestellt, dass vorgegebene Krisen-Eskalationsmodell angewendet werden. Wie sich im Fall der Ransomware „WannaCry“ gezeigt hat, war dieser Trojaner die erste richtige Bewährungsprobe für den Zusammenschluss der europäischen CSIRT´s.[159] In weltweit über 150 Ländern (siehe Abbildung 20) wurden Systeme infiziert, obwohl es von Anfang an durch den Hersteller entsprechende Patches für betroffene Systeme gegeben hat.[160]

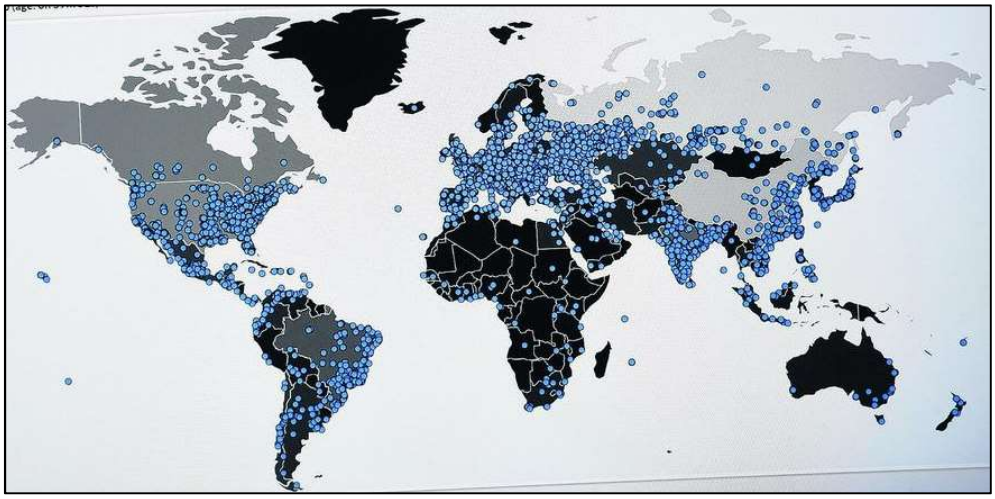


Abbildung 20: Weltkarte des WannaCry Befalls im Jahr 2017[161]

Betroffen waren dabei große Konzerne (auch BwD) in einigen EU-Ländern wie Großbritannien, Frankreich, Deutschland oder Spanien. Das Bestehen und die erfolgreiche Umsetzung eines gemeinsamen, europäischen Krisen-Eskalationsmodells wird auch in Zukunft noch von großer Bedeutung sein.

In Österreich ist die Situation noch unbestimmt. Das entsprechende NISG sollte diese Vorgaben enthalten. Es gibt dazu keine eindeutigen Empfehlungen von Seitens KSÖ. Aus KSÖ-ExpertInnensicht wird die Konkretisierung der Meldepflicht eine der größten

158 Vgl. (Bundesamt für Sicherheit in der Informationstechnik 2017b, S. 10)

159 Vgl. (Schulzki-Haddouti 2017, online)

160 Vgl. (ENISA 2017b, online)

161 (Schulzki-Haddouti, 2017, online)

Herausforderungen werden.[162] Auf Basis des KSÖ-Whitepapers wurden diese Themenbereiche unter den betroffenen österreichischen Unternehmen kontrovers diskutiert. Im Whitepaper wird folgendes hinsichtlich der Meldepflicht angemerkt:

> *„Sowohl der Entwurf der NIS-Richtlinie als auch das deutsche IT-Sicherheitsgesetz verwenden offene und damit unbestimmte Formulierungen, die in hohem Masse interpretationsbedürftig sind.*“[163]

Für Teile des ExpertInnenkreises waren die Formulierungen zu unspezifisch und für Teile gingen diese bereits zu weit. Als konsensuales Ziel wurde schließlich festgehalten, dass ein nationales NISG bei Umsetzung der Meldepflicht präzisierende Vorgaben zu definieren hat. Eine reine Übernahme aus der NIS-Richtlinie wird die Erwartungen der Unternehmen nach präzisen Vorgaben nicht erfüllen.[164]

Für Österreich hat es Potenzial, ein brisantes Thema zu werden. Dies unter dem Aspekt, inwieweit zu einem konkreten Vorfall aus anderen Rechtsmaterien (z.B. DSGVO) Meldepflichten (inkl. Sanktionen) entstehen können und so Doppelbestrafungen resultieren. Für jene Betreiber, die sektorbedingt multiplen Meldeverpflichtungen unterworfen sind, sollte jedenfalls eine einheitliche Meldestelle (z.B. mit der Datenschutzbehörde) eingerichtet werden, damit der Administrationsaufwand nicht ausufert.[165]

Die Bedenken von Österreichs BwD sind nachvollziehbar, jedoch sind die Vorgaben und Regelungen bzgl. der IT-Sicherheitsvorfälle und Meldepflicht in den Gesetzen Deutschlands soweit zweckmäßig ausgestaltet, so dass es vor allem in der Implementierungsphase ein praktikabler Ansatz wäre, sich daran zu orientieren.

Auf die indirekt betroffenen IT-SP ergeben sich daraus auch Anforderungen, die es zukünftig umzusetzen und einzuhalten gilt. Denn wenn - laut NIS-Richtlinie - ein BwD für die Bereitstellung einer kritischen Dienstleistung die Dienste eines Dritten (z.B. IT-SP, AdD) in Anspruch nimmt, so ist jede erhebliche Auswirkung auf die Verfügbarkeit zu melden. Die finale Meldepflicht an zentrale, bzw. nationale SPOC´s, wird dem BwD in vordefinierter Form obliegen. Jedoch ist absehbar, dass hierfür die Einmeldung von relevanten beeinträchtigenden IT-Sicherheitsvorfällen, nach dem Prinzip einer „Melde-Kaskade“, von den IT-SP eingefordert wird.[166]

Zudem wird Unternehmen, die nicht als BwD bzw. AdD ermittelt worden sind, die Möglichkeit eingeräumt, auf freiwilliger Basis Sicherheitsvorfälle (mit erheblicher Auswirkung auf angebotene Dienste) zu melden.[167] Dabei werden durchaus IT-SP´s dazu angehalten, sich in die NIS-Community einzubinden.

---

[162] Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 9)

[163] (KSÖ – Kuratorium Sicheres Österreich 2016, S. 23)

[164] Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 23)

[165] Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 9)

[166] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 22)

[167] Vgl. (EUROPÄISCHE KOMMISSION 2017, S. 24)

Die zu Beginn dieses Unterkapitels festgehaltene klare Formulierung aus der NIS-Richtlinie beantwortet sinngemäß die Hypothese H 1. Der BwD ist dafür verantwortlich, dass jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste durch den Betreiber selbst gemeldet wird. Ein Übertrag der Verantwortung an Dritte ist nach derzeitigem Kenntnisstand somit nicht möglich.

2.5.5 Gesetzliche Vorgaben betreffend Sicherheitsanforderungen

In diesem Kontext wird oft der Begriff „Stand der Technik" strapaziert. Die initial ermittelte Betreiberliste wird zumindest alle zwei Jahre zu überprüfen sein. Damit soll ein EU-weiter Bewertungsmaßstab zur Ermittlung von KI´s geschaffen werden.

Laut NIS-Richtlinie müssen BwD spezielle Sicherheitsanforderungen einhalten. Zu diesem Zweck legt die NIS-Richtlinie fest, dass geeignete und verhältnismäßige TOM zu ergreifen sind, die den „Stand der Technik" unter Einbeziehung von Normen sowie technischen Leitlinien der ENISA berücksichtigen. Gemäß NIS-Richtlinie können EU-Mitgliedsstaaten zudem Bestimmungen aufrechterhalten, bzw. erlassen, mit denen ein höheres Sicherheitsniveau von NIS erreicht wird. Damit soll das Ziel einer Mindestharmonisierung von Schutzmaßnahmen ermöglicht und eine maximale Dienstleistungsverfügbarkeit gefördert werden.[168]

Laut dem KSÖ-Whitepaper war auch in Deutschland die Verwendung des Begriffs „Stand der Technik" für das IT-SiG ein zentraler Diskussionspunkt. Dazu war die finale Schlussfolgerung, dass betroffene Unternehmen mit der Materie hinreichend vertraut sein werden.[169] Die KSÖ-ExpertInnen vertreten hier die Ansicht, dass es in einer Verordnung zum zukünftigen österreichischen NISG möglich sein soll, konkrete Vorgaben zu schaffen.[170] Dieses Anliegen, dass derartige Vorgaben keine mehrdeutigen Begriffe enthalten sollen ist verständlich, jedoch aus einer praxisorientierten Sicht nur schwer auszuführen.

Die Bezeichnung „Stand der Technik" hat sich bis heute bereits über einen langen Zeitraum bewährt. Die Möglichkeit sich auf internationale Standards, Normen oder Frameworks (z.B. ISO 27000-Reihe, ISO 20000, ISO 31000, BSI IT-Grundschutz) zu beziehen, sollte ausreichend Sicherheit betreffend den Vorgabecharakter geben und für die BwD eine wünschenswerte Flexibilität in der Ausgestaltung zulassen. Vor allem wenn bedacht wird, wie komplex bzw. langwierig entsprechende Gesetzesanpassungen in Österreich sein können, sollte eine derart flexible und auch branchenunabhängige Formulierung im NISG herangezogen werden.

Für die IT-SP ist diese Thematik nahezu irrelevant, da sich von Seiten der BwD die Vorgaben auf die eine oder andere Art ergeben werden.

---

[168] Vgl. (Kipker 2016, S. 8f)

[169] Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 40f)

[170] Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 25)

2.5.6 Sanktionen und Bußgelder bei Verstößen

Die NIS-Richtlinie enthält ein kurzes Kapitel zum Thema der Sanktionen bei Verstößen gegen national erlassene Bestimmungen. Es wird festgehalten, dass Mitgliedsstaaten folgendes zu berücksichtigen haben:

> *„[...] Sanktionen müssen wirksam, angemessen und abschreckend sein.“*[171]

Nach Formulierungen im deutschen IT-SiG sind relevante IT-Sicherheitsstandards gemäß „Stand der Technik“ einzuhalten. Wird diese Verpflichtung nachweislich nicht eingehalten, so drohen relativ empfindliche Bußgelder. Um die Einhaltung nachzuvollziehen ist vorgeschrieben, dass KRITIS-Betreiber die Sicherheit zumindest alle zwei Jahre durch Auditoren überprüfen lassen müssen. Zu diesem Zweck ist dem BSI die gesetzliche Befugnis zugeteilt worden (vgl. Kapitel 2.4.4).

Das Kapitel „Bußgeldvorschriften“ im IT-SiG spezifiziert die - gemäß der NIS-Richtlinie vorgesehenen - Sanktionen in ausreichendem Maße. Grundsätzlich können Bußgelder verhängt werden, wenn in definierten Bereichen vorsätzlich oder fahrlässig zuwidergehandelt wird. Darunter fallen z.B. folgende Themen:

- Treffen angemessener TOM zur Aufrechterhaltung von Schutzzielen
- Bereitstellen von Nachweisen aus Audit- oder Zertifizierungen
- Relevante Mindestsicherheitsanforderungen einhalten
- Vorgegebene Meldepflichten einhalten und nachkommen[172]

Dabei werden je nach Kategorie entsprechende Verstöße mit Geldbußen von bis zu 100.000 EUR oder von bis zu 50.000 EUR geahndet. Die Bußgeldhöhe könnte durchaus abschreckend wirken, wobei diese Ansicht je nach Größe des Betreibers differieren wird. Die Bezeichnung „bis zu“ bietet dabei entsprechenden Spielraum.[173]

Für Österreich wird eine Sanktionierung bei Nichteinhaltung tendenziell positiv gesehen. Es wird aber vornehmlich darauf hingewiesen, dass eine Nichteinhaltung von Schutzzielen per NISG sanktioniert werden sollte.[174] In der abgeleiteten Empfehlung wird nur sehr unspezifisch darauf eingegangen, wie folgend ersichtlich-

> *„[...] Betreiber kritischer Infrastrukturen und zuständige Behörden legen gemeinsam fest, wie die Nichteinhaltung der Schutzziele sanktioniert wird.“*[175]

Diese Auslegung ist im Vergleich zum IT-SiG eine deutlich abgeschwächte Form. Ob die Sanktionen bei dieser Eingrenzung (Nichteinhaltung der Schutzziele) nun „wirksam, angemessen und abschreckend“ sind, wäre diskussionswürdig. Die Höhe der möglichen Sanktionen wird noch ein großes Diskussionsthema sein. Eine Bewertung der möglichen

---

171 (Amtsblatt der Europäischen Union 2016, S. 24)

172 Vgl. (Bundesgesetzblatt 2015, S. 4)

173 Vgl. (Bundesgesetzblatt 2015, S. 5)

174 Vgl. (KSÖ – Kuratorium Sicheres Österreich 2016, S. 19)

175 (KSÖ – Kuratorium Sicheres Österreich 2016, S. 20)

Bußgeldhöhe wird dabei nicht vorgenommen. Ein mögliches Extrem könnte die Orientierung an den Strafhöhen der DSGVO sein, welche gegebenenfalls den weltweiten Jahresumsatz als Basis heranziehen kann.

Für Österreichs BwD werden zum Thema der Sanktionen noch zusätzliche Formulierungen erforderlich sein, um zu einem zweckmäßigen Ergebnis zu kommen.

Für IT-SP wird es gegebenenfalls in potenziellen Verträgen bzw. in den jeweiligen Verhandlungen mit den Betreibern zu berücksichtigen sein. Dabei sind allfällige Pönalen, Strafzahlungen, etc. bereits heute in vielen Verträgen bzw. Service Level Agreements (SLA) geregelt.

3. Empirischer Teil

In diesem Kapitel wird die Auswahl der empirischen Methoden erläutert und wie diese angewendet wurden, um zu den anschließenden Forschungsergebnissen zu gelangen.

„*Tatsachen schafft man nicht dadurch aus der Welt, dass man sie ignoriert.*“
(Aldous Huxley, 1894 - 1963)

3.1 Auswahl der empirischen Methodik

Nach einer initialen Literaturrecherche der verfügbaren Dokumente, wurden auf Basis empirischer Methoden Erkenntnisse zur Beantwortung der Forschungsfragen erarbeitet. Generell gibt es auch in der Wirtschaftsinformatik eine Vielzahl an Forschungsansätzen, die grundlegend in die folgenden beiden Paradigmen unterteilt werden können:

1. Gestaltungsorientierte Wirtschaftsinformatik
   Im deutschsprachigen Raum nimmt die gestaltungorientierte Wirtschaftsinformatik eine dominierende Rolle ein, wobei sie auch in anderen europäischen Ländern oft angewendet wird. Das Kernelement dieses Paradigmas ist die Modellierung bzw. die beschreibende Darstellung soziotechnischer Systeme. Als Hauptmerkmal ist dabei die Konstruktion von Artefakten wie z.B. konzeptionelle Modellierung, Referenzmodellierung und Prototyperstellung anzusehen.
2. Verhaltensorientierte Wirtschaftsinformatik
   Im englischsprachigen Sprachraum ist die verhaltensorientierte Wirtschaftsinformatik vorherrschend. Der Fokus der Untersuchungen liegt dabei hauptsächlich auf der Beziehung von Ursache und Wirkung in Systemen, sowie auf Präferenzen und Verhalten von deren NutzerInnen.[176]

In beiden Bereichen stehen viele Methoden zur Verfügung, auf deren Basis Forschungstätigkeiten durchgeführt werden können. Um einen kompakten Überblick zu vermitteln sind in Abbildung 21 bekannte Methoden dargestellt und entsprechend zugeordnet.

gestaltungsorientiert	verhaltensorientiert
- Prototyping - Simulation - Referenzmodellierung - Formal-deduktive, konzeptionell-deduktive und argumentativ-deduktive Analyse - Aktionsforschung	- Grounded Theory (qualitativ) - Quantitativ-empirische Querschnittsanalyse - Qualitativ-empirische Querschnittsanalyse - Fallstudien - Labor- und Feldexperimente - Ethnographie

Abbildung 21: Konsolidiertes Methodenspektrum der Wirtschaftsinformatik[177]

Aus diesem Spektrum wurden für diese Masterarbeit geeignete Methoden ausgewählt, um eine zielgerichtete Beantwortung der Forschungsfragen und Hypothesen zu

[176] Vgl. (Winter und Baskerville 2010, S. 257f)

[177] (Wilde und Hess 2006, S. 10)

erarbeiten. Zur Einordnung der Methoden in die jeweiligen Paradigmen kann die Portfoliodarstellung aus Abbildung 22 herangezogen werden.

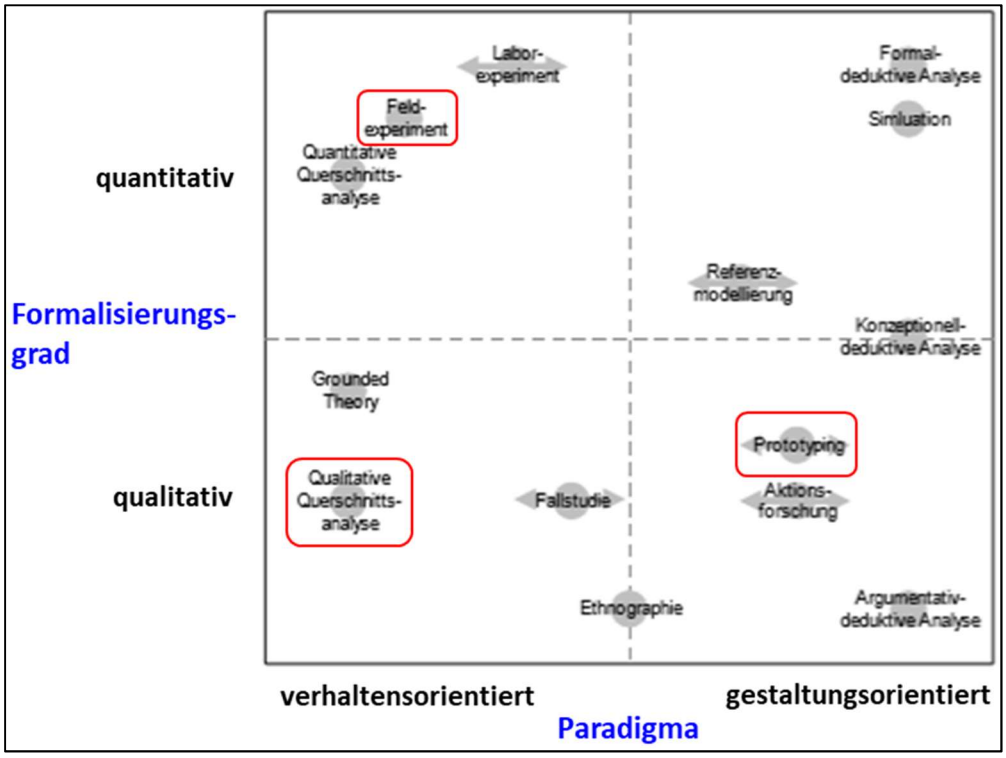


Abbildung 22: Portfolioeinordnung der Methoden[178]

In der obigen Abbildung 22 sind rot umrahmt jene Methoden, die im Zuge dieser Masterarbeit zur Anwendung gekommen sind.

3.1.1 Prototyping

In der gestaltungsorientierten Forschung ist Prototyping ein klassischer Vertreter. Dabei steht eine entsprechende Vorabversion der zu erstellenden Endanwendung, zum Zwecke der späteren Evaluierung, im Zentrum des Interesses.

In der aktuell verfügbaren Literatur existiert derzeit kein Konsens über die Definition von Prototyping als Methode im Bereich der Wirtschaftsinformatik. Als zweckmäßige Definition wird für diese Masterarbeit deshalb folgende herangezogen:

> *„Ein Software-Prototyp ist ein – mit wesentlich geringerem Aufwand als das geplante Produkt hergestelltes – einfach zu änderndes und zu erweiterndes ausführbares Modell des geplanten Software-Produkts oder eines Teiles davon, das nicht notwendigerweise alle Eigenschaften des Zielsystems aufweisen muss, jedoch so geartet ist, dass vor der eigentlichen Systemimplementierung der Anwender die wesentlichen Systemeigenschaften erproben kann.“*[179]

Als grundsätzliche Aussage kann festgehalten werden, dass ein Software-Prototyp

[178] eigene Darstellung (Wilde und Hess 2006, S. 14)

[179] (Pomberger und Pree 2004, S. 27)

- mindestens lauffähig (direkt oder via Simulation.) sein muss, und
- rasch und kostengünstig erstellt werden kann.

Dabei besteht in wissenschaftlichen Kreisen Uneinigkeit hinsichtlich der tatsächlichen Umsetzung eines Prototyps. Dabei gibt es zwei Herangehensweisen:

1. Einerseits kann ein Prototyp als Muster der späteren Endanwendung, mitsamt allen wesentlichen Eigenschaften, realisiert werden.
2. Andererseits kann der Prototyp inkrementell, mit anfänglich nur wenigen Basiseigenschaften, erstellt und nach Anwenderrückmeldung kontinuierlich weiterentwickelt werden.[180]

3.1.2 Qualitative Querschnittsanalyse

Bei dieser Form von empirischer (Sozial-)Forschung wird während der Untersuchung eine einmalige Datenerhebung (z.B. via Beobachtung, Interview, Befragung, Inhaltsanalyse) durchgeführt und dadurch eine Momentaufnahme abgebildet.

Aus einer definierten Grundgesamtheit wird eine Stichprobe von Objekten entnommen, um daraus ein Querschnittsbild zu erstellen, aus dem wiederum Rückschlüsse auf die Grundgesamtheit ermöglicht werden.[181]

Auf dieser Methode ist die, in dieser Masterarbeit, angewendete ExpertInnenbefragung aufgebaut. Aufgrund der ExpertInnenantworten wurden konkrete inhaltliche Rückschlüsse auf das entwickelte „Self Assessment für NIS-Readiness“ und die eigenen Forschungsfragen gezogen.

3.1.3 Feldexperimente

Die Experimente sind dem Bereich der verhaltensorientierten Forschung zuordenbar. Eine der Kernaussagen ist, dass durch Experimente

> *„[...] Erkenntnisse über den in einer Hypothese behauptete Kausalzusammenhang zwischen einer oder mehreren unabhängigen Variablen gewonnen werden.*“[182]

Im Rahmen dieser Methode können existierende, bzw. aufgestellte Theorien nach festgelegten Bedingungen einer Überprüfung unterzogen werden.

Dabei kann allgemein zwischen Labor- und Feldexperiment unterschieden werden. Im Zuge der Masterarbeit wurde jedoch ausschließlich das Feldexperiment durchgeführt, welches auch synonym als Feldversuch bezeichnet wird. Beim Feldexperiment wird der zu untersuchende Gegenstand in seinem natürlichen Umfeld untersucht, wodurch ein realitätsnahes Forschungsergebnis möglich wird.

---

[180] Vgl. (Pomberger und Pree 2004, S. 26ff)

[181] Vgl. (Wilde und Hess 2006, S. 8)

[182] (Heinrich, Heinzl und Riedl 2011, S. 102)

3.1.4 Selektion der ExpertInnen

Bei der Auswahl der Befragten ist es nicht erforderlich eine Zufallsstichprobe zu ziehen, denn es geht im Ergebnis nicht um repräsentative Aussagen, sondern das typische Strukturen und Gegebenheiten bewertet werden. Es ist wichtig, dass von der interviewenden Person, im Sinne der Selbstkontrolle, ausgeschlossen wird, dass nur Personen mit identen Einstellungen zu den eigenen Vorüberlegungen ausgewählt werden.[183] Bei Selektion der ExpertInnen wurde das Hauptaugenmerk auf die Erreichung der beiden folgenden Ziele gelegt:

1. Die ExpertInnenbefragungen sollen einen bestimmten Bereich innerhalb der BwD bzw. IT-SP möglichst detailliert abbilden können und somit die „Tiefe" dieser Masterarbeit gewährleisten.
2. Die „Breite" in dieser Arbeit soll mit der Analyse von mindestens drei unterschiedlichen Branchen der „Betreiber kritischer Dienste" sowie IT-SP erreicht werden.

Im Sinne der obigen Ziele 1. und 2. wurden deshalb sechs Befragte mit IT(-Sicherheit) Expertise aus drei unterschiedlichen Branchen ausgewählt. Im Rahmen der durchgeführten Befragungen wurde in Einzelfällen die Notwendigkeit gesehen, die Identität des/der teilnehmenden ExpertIn anonym und vertraulich zu behandeln. Die folgende Aufzählung der Mitwirkenden unterliegt keiner irgendwie gearteten Reihung und erfolgte rein zufällig:

- ExpertIn I
  Name: Anonym
  Unternehmen: Vertraulich
  Position im Unternehmen: Vertraulich
  Bezug zur NIS-Richtlinie: Potenzieller BwD

- Experte II
  Name: Christian Schwertberger
  Unternehmen: ÖBB-Infrastruktur AG
  Position im Unternehmen: Chief Information Security Officer
  Bezug zur NIS-Richtlinie: Potenzieller BwD

- Experte III
  Name: Johannes Mariel
  Unternehmen: Vertraulich
  Position im Unternehmen: Vertraulich
  Bezug zur NIS-Richtlinie: IT-SP

[183] Vgl. (Buber und Holzmüller 2007, S. 468)

- Experte IV
  Name: Markus Lenikus
  Unternehmen: ÖBB-Infrastruktur AG
  Position im Unternehmen: Information Security Officer
  Bezug zur NIS-Richtlinie: Potenzieller BwD

- Experte V
  Name: Othmar Schöller
  Unternehmen: Raiffeisen Informatik GmbH
  Position im Unternehmen: Chief Security Officer
  Bezug zur NIS-Richtlinie: IT-SP

- Experte VI
  Name: Robert Geist
  Unternehmen: Vertraulich
  Position im Unternehmen: Vertraulich
  Bezug zur NIS-Richtlinie: IT-SP

Die Identität der jeweiligen ExpertInnen ist dem Betreuer der Masterarbeit offengelegt worden und auch die inhaltlichen Freigaben der Ergebnisse sind dem Betreuer bekannt.

3.2 Durchführung der Empirie

Die zentralen empirischen Elemente und Herangehensweisen werden in den nachfolgenden Unterkapiteln im Detail beschrieben. Die Empirie gliedert sich vereinfacht dargestellt in folgende Bereiche auf:

- Entwicklung eines eigenen „Self Assessments für NIS-Readiness“
- Präsentation dieses Self Assessments ausgewählten ExpertInnen mit anschließender Beantwortung eines Fragebogens
- Durchführung eines Feldexperiments mit ausgewählten ExpertInnen auf Basis des vorgestellten Self Assessments

Die so erarbeiteten Ergebnisse sind als Fundament für die Verifikation der Hypothesen und der Beantwortung der Forschungsfragen zu betrachten.

3.2.1 Design der ExpertInnenbefragung

Aufgrund diverser Faktoren ist bei den ExpertInnenbefragungen eine gewisse Ergebnisverzerrung (z.B. Über- / Unterrepräsentation von Unternehmen einer gewissen Größe oder Branche, Affinität zu Informationssicherheit und Sicherheitsbewusstsein) möglich und wahrscheinlich.

Im Zuge der Masterarbeit wurden die Befragten so ausgewählt, dass sie ein tiefergehendes Verständnis und gesteigertes Bewusstsein für die Themen hinsichtlich der NIS-Richtlinie haben. Diese VertreterInnen von Unternehmen aus dem BwD bzw. IT-SP Bereich sind besser darauf vorbereitet, als Personen anderer Unternehmen, die von der NIS-Richtlinie

nicht oder peripher betroffen sind. Aus den Ergebnissen dieser Befragungen kann jedoch kein Anspruch auf Vollständigkeit und Repräsentativität abgeleitet werden. Die reale Situation für den österreichischen Raum könnte somit, gegenüber den in dieser Arbeit dargestellten Resultaten und Erkenntnissen „abweichend" sein, als hier interpretiert wird. Die gegenständliche Situation hinsichtlich NIS-Richtlinie wird nachfolgend zumindest in Bezug auf die Unternehmen der teilnehmenden ExpertInnen beschrieben.

3.2.1.1 Methodik der ExpertInnenbefragung

Die inhaltliche Grundlage für die ExpertInnenbefragung bildet der selbstentwickelte Prototyp des „Self Assessment für NIS-Readiness" (vgl. Kapitel 3.2.2) der einer kritischen Betrachtung unterzogen wurde. Ziel war es, anhand eines (teil-)strukturierten Fragebogens, auf Basis einer persönlich durchgeführten Präsentation des „Self Assessment für NIS-Readiness" qualifizierte Antworten durch ExpertInnen zu erhalten, um neue Erkenntnisse zu gewinnen. Der Ablauf der ExpertInnenbefragung gliederte sich grundlegend in folgende drei Phasen.

1. **Befragungsvorbereitung**

Eine gründliche Vorbereitung wurde als Basis für die Qualität der entsprechenden Befragung durchgeführt. Um zielgerichtetes Nachfragen bzw. Hinterfragen zu ermöglichen und dadurch eine Akzeptanzbasis mit dem/der ExpertIn aufzubauen, war ein entsprechendes thematisches Vorwissen beider Parteien von Nutzen. Dabei können im Allgemeinen folgende drei Typen unterschieden werden:[184]

- Als Peer
  Beide Seiten weisen ein ähnliches Maß an Wissen im relevanten Thema auf.
- Mit moderatem Vorwissen
  Der/Die BefragerIn eignet sich das nötige fachliche Wissen möglichst schnell an.
- Ohne Vorwissen
  Dieser Typus birgt ein entsprechendes Risiko. Oftmals nehmen BefragerInnen (mit fehlendem Vorwissen) nur jene Teile des Interviews auf, welche am verständlichsten erklärt worden sind.

Wichtig bei der Befragung war, dass das Vorwissen der fragenden Partei das Gespräch nicht bestimmen oder in eine Richtung steuern darf.[185] Hinsichtlich des eigenen Wissensstands zum relevanten Forschungsbereich der NIS-Richtlinie und der beruflichen Erfahrung in der IT-Branche, konnte der Befrager / Autor im Rahmen dieser Masterarbeit durchaus als Peer angesehen werden.

2. **Befragungsdurchführung**

Begonnen wurde mit der Visualisierung des Themas (inkl. Ziele, Kontext, etc.). Die Anonymität und Vertraulichkeit wurde standardmäßig zugesichert, sowie das

[184] Vgl. (Buber und Holzmüller 2007, S. 469f)

[185] Vgl. (Buber und Holzmüller 2007, S. 470)

Einverständnis zur Befragungsdokumentation eingeholt.

Zu Beginn des ExpertInnengesprächs wurden einleitende Informationen über den Inhalt der Masterarbeit und die grundlegenden Ideen des „Self Assessment für NIS-Readiness“ vorgestellt. Das Thema wurde mittels spezifischen Beispielen der Situation des/der ExpertIn angepasst, um damit ein Interesse zu wecken und zu halten. So konnte auch eine wertschätzende Gesprächsbasis aufgebaut werden, wodurch die inhaltliche Qualität der Präsentation und der darauffolgenden Befragung positiv beeinflusst wurde.

Als zentrales Element der Befragung wurde die inhaltliche, strukturelle und methodische Ausgestaltung des „Self Assessment für NIS-Readiness“ vorgestellt. Im Zuge dessen wurden spezifische Details und Herangehensweisen erläutert, damit die ExpertInnen darauf aufbauend die 12 Hybridfragen (auch als Mischfragen bekannt) des (teil-)strukturierten Fragebogens seriös beantworten und gegebenenfalls Kommentare verfassen konnten.

Ein primäres Ziel war es, den Zustimmungsgrad der ExpertInnen einzuholen, ob das vorgestellte „Self Assessment für NIS-Readiness“ die Anforderungen erfüllen würde, um den potenziell betroffenen Unternehmen in Österreich eine Hilfestellung geben zu können. Mit möglichst geschlossen gehaltenen Fragen wurde die Möglichkeit gegeben, eindeutige und bestenfalls vergleichbare Antworten (Ja / eher Ja / eher Nein / Nein) abzubilden. Um dennoch das Wissen der ExpertInnen einfließen zu lassen, wurde bewusst die Nutzung des Kommentarfeldes empfohlen. Für den Fall, dass keine dieser vorgegebenen vier Antwortmöglichkeiten zutraf, hatten die ExpertInnen zusätzlich die Option, eine entsprechende offene Antwort (Kommentar zur Antwort „Kommt darauf an“) je Frage zu geben.

Ein wichtiges Thema der Fragebogenausgestaltung war die Ausgestaltung der Skala der Antwortmöglichkeiten. Der Aspekt ob es nun eine Mittelkategorie - wie z.B. neutral oder unentschieden - geben soll, birgt folgende Polemik.

- Falls diese Kategorie vorhanden ist, besteht die erhöhte Tendenz zur Nutzung um auf diesem Weg den kognitiven Aufwand im Rahmen der Beantwortung zu minimieren und nicht die persönliche Einstellung wiederzugeben (auch bekannt als „Tendenz zur Mitte“).
- Ist andererseits die Mittelkategorie nicht vorhanden, so werden befragte Personen in eine Richtung gedrängt obwohl sie tatsächlich neutral zum befragten Thema stehen.[186]

Zu einer Verzerrung der Ergebnisse kann es dabei in beiden Fällen kommen. Verschiedene Studien zeigten auf, dass die Mittelkategorie von befragten Personen nicht nur m Falle einer neutralen Einstellung gewählt wird, sondern auch aus anderen

[186] Vgl. (Menold und Bogner 2015, S. 5)

Gründen wie z.B. soziale Erwünschtheit. Dennoch empfehlen viele Forscher, dass die Mittelkategorie angeboten wird, damit neutral eingestellte Befragte nicht zu einem Ausweichen auf andere Kategorien gezwungen werden und es zu keiner systematischen Verzerrung kommt.[187]

Im Rahmen der Masterarbeit wurde bewusst die Entscheidung getroffen, keine Mittelkategorie zu verwenden, da eine Prototypenpräsentation vor ExpertInnen durchgeführt wurde und darauf aufbauend der Fragebogen behandelt worden ist. Die Annahme war, dass ExpertInnen durchaus eine Meinung in eine gewisse Richtung haben und diese auch äußern. Falls dies gegebenenfalls doch nicht sein sollte, konnte per Antwort „Kommt darauf an" ein Kommentar abgegeben werden. Dadurch war die Möglichkeit einer selbst formulierten Mittelkategorie in abgeänderter Form trotzdem verfügbar.

Im Zuge der Befragung wurde Wert daraufgelegt, die Themen rund um die NIS-Richtlinie aus diversen Blickwinkeln zu beleuchten. Mögliche daraus abgeleitete Annahmen wurden so bereits während der Präsentation einem ersten rudimentären Check unterzogen.

Zum Abschluss des Präsentationstermins und der Befragung wurde nochmals der Dank bezüglich der aufgewendeten Zeit und der interessanten Erkenntnisse ausgesprochen.

3. Befragungsnachbereitung

Primär handelte es sich um einen schriftlichen Fragebogen, welcher von den ExpertInnen während des gemeinsamen Termins erarbeitet wurde und somit am Ende bereits dokumentiert vorlag. In diesem Standardfall war keine besonders aufwändige Nachbereitung mehr notwendig, wie beispielsweise bei einem Interview. Für den Fall, dass dennoch eine Aufzeichnung nötig wurde, konnte auf eine Reihe von Erhebungsmethoden zugegriffen werden. Für die Erstellung dieser Masterarbeit wurden Feldnotizen als klassisches Medium der Aufzeichnung gewählt. Dabei standen zwecks Protokollierung des Erhebungsmaterials verschiedene Techniken zur Verfügung, wie:

- wörtliche Transkription,
- kommentierte Transkription,
- zusammenfassendes Protokoll und
- selektives Protokoll

Es war dabei von Bedeutung, dass ein ausgewogenes Verhältnis von Aufwand, Detaillierungsgrad und Übersichtlichkeit der Transkription gefunden wurde.[188] Das „selektive Protokoll", ist ein inhaltsanalytisches Transkriptionssystem, bei welchem nur bestimmte relevante Teile des Datenmaterials transkribiert werden.[189]

Bei dieser Masterarbeit bzw. Präsentation des Self Assessments handelt es sich um eine Studie mit Fokus auf den Inhalt, weshalb sich das „selektive Protokoll" angeboten hat.

---

[187] Vgl. (Menold und Bogner 2015, S. 6)

[188] Vgl. (Universität Augsburg, s.a., online)

[189] Vgl. (Buber und Holzmüller 2007, S. 663)

Die Dokumentation der Antworten des Fragebogens wurde wie folgt durchgeführt.

1. Die schriftlichen Antworten der ExpertInnen wurden in jedem Fall wortgetreu digitalisiert und als „Originalversion“ gespeichert.
2. Anlassbezogen wurden, in einem eigenen Dokument (Feldnotiz), mitgeschriebene Gesprächsinhalte ergänzend zu den Kommentaren der Originalversion des Fragebogens hinzugefügt und als „Originalversion plus Gesprächsinhalte“ gespeichert.

Den jeweiligen ExpertInnen wurden beide Dokumentenversionen per E-Mail zur schriftlichen Freigabe der gewünschten Version (obige Punkt 1 bzw. 2) übermittelt. In diesem Zuge wurde ebenso die schriftliche Rückmeldung betreffend der Wahrung von Anonymität und Vertraulichkeit der Identität im Rahmen der Masterarbeit eingeholt.

Die beantworteten Fragebögen sind im Anhang B dokumentiert.

3.2.1.2 Fragebogen und Themenbereiche

Der Fragebogen wurde in 3 Themenbereiche (TB) gesplittet, in denen mittels möglichst geschlossen gehaltenen Fragen relevante Bereiche der NIS-Richtlinie und Cybersicherheit im Kontext mit dem „Self Assessment für NIS-Readiness“ behandelt wurden. Die TB wurden wie folgt gruppiert und beinhalten jeweils vier Fragen:

- TB1: Inhalt des Self Assessments
- TB2: Methodik des Self Assessments
- TB3: Darstellung und Querbezug des Self Assessments

Der ‚Fragebogen diente als Werkzeug dazu, die ausgewählten ExpertInnen an die konkrete Problemstellung heranzuführen und auch einen Rahmen vorzugeben.

Standardmäßig wurde eine ungefähre Befragungsdauer vorab bekanntgegeben, um die Zeit der ExpertInnen nicht über Gebühr zu beanspruchen und auch das eigene Zeitmanagement zu verbessern. Da in der ExpertInnenbefragung teilweise auch auf sensiblere Informationen (z.B. IT-Sicherheitsstrategie, NIS-Kommunikationsstrukturen) einzugehen war, wurde den ExpertInnen versichert, dass die Angaben auf Wunsch vertraulich und anonym behandelt werden.

Die 12 themenbezogenen Fragen der definierten Bereiche konnten anlassbezogen bereits während der Präsentation des Self Assessments beantwortet werden. Ebenso konnten die Fragen auch während eines Dialogs näher erläutert und behandelt werden, damit eine zielgerichtete Antwort gegeben wurde. In den meisten Fällen erfolgte die Beantwortung des Fragebogens im Anschluss an die Präsentation und nach vertiefenden Rückfragen.

Da die Befragten durchgängig ExpertInnen mit Bezug zur NIS-Richtlinie und Cybersicherheit sind, waren vor und während der Befragung keine besonderen Hilfestellungen mit Erklärungen und Beispielen zur Fragebogenbeantwortung notwendig.

Während des Termins wurden mögliche, nicht als Kommentar im Fragebogen erfasste, Gesprächsinhalte schriftlich mitdokumentiert. Die folgende Transkription und inhaltliche

Zusammenführung erfolgte ohne Beisein der ExpertInnen. Die daraus resultierenden Ergebnisse wurden zur Prüfung auf inhaltliche Korrektheit und Vollständigkeit retourniert. Nach entsprechendem Feedback und Freigabe wurden die Resultate für den weiteren Erkenntnisgewinn und zur Ableitung von Empfehlungen herangezogen.

Die Befragungen wurden zwischen 12.4.2018 und 3.5.2018 in Wien geführt. Die Dauer (inkl. Self Assessment Präsentation) hat sich zwischen 60 und 130 Minuten bewegt.

3.2.1.3 Vollständiger Fragebogen

Der vollständige Fragebogen zum „Self Assessment für NIS-Readiness“ - mit all den relevanten Fragen, Aussagen und Kommentaren je ExpertIn - ist in Anhang B festgehalten. Nachfolgend sind die definierten Fragen je Themenbereich angeführt.

TB1: Inhalt des Self Assessments

1. Genügt das „Self Assessment für NIS-Readiness“ ihrer Meinung nach inhaltlich den bisher bekannten Anforderungen aus der NIS-Richtlinie?

2. Ist das vorgestellte „Self Assessment für NIS-Readiness“ ihrer Meinung nach hinsichtlich Inhalt und Umfang zweckmäßig ausgestaltet und somit für Fachkundige hinsichtlich der Komplexität nutzbar?

3. Sind ihnen im Rahmen eines derartigen „Self Assessment für NIS-Readiness" technische und organisatorische Auswirkungen aufgezeigt worden, die sich auf Basis der NIS-Richtlinie ergeben könnten?

4. Würden Sie sagen, dass dieses „Self Assessment für NIS-Readiness“ - aus inhaltlicher Sicht - potenziell betroffenen Unternehmen in Österreich eine Hilfestellung bezüglich Umsetzung der NIS-Richtlinie geben kann?

TB2: Methodik des Self Assessments

5. Ist aus ihrer Sicht ein „Self Assessment für NIS-Readiness“ zur initialen Bewertung der Vorgaben aus der NIS-Richtlinie ein zweckmäßiges Mittel?

6. Ist ihrer Meinung nach eine Bewertung der NIS-Readiness anhand des angewendeten Reifegradmodells (nach CMMI) zweckmäßig?

7. Ist ihrer Meinung nach die Nutzung eines „Gesamtergebnis CMMI Ziel-Reifegrads“ wie im vorgestellten Self Assessment sinnvoll?

8. Ist für Sie ein „Self Assessment für NIS-Readiness“ hilfreich, um eventuell identifizierte Maßnahmen einer möglichen Behandlung zuzuführen?

TB3: Darstellung und Querbezug des Self Assessments

9. Finden Sie die grafische Aufbereitung der „NIS-Readiness im Self Assessment“ in Form eines Spinnennetzdiagramms verständlich?

10. Ist ihrer Meinung nach die hier vorgenommene Einschätzung (teils abweichend von CMMI) der Reifegrade zur Berechnung des „NIS-Readiness Werts“ realitätsnah?

11. Ist ihrer Meinung nach die verhältnismäßig intensive Einbindung von Inhalten der ISO 27001 in das Self Assessment ein zielführender Ansatz?

12. Haben aus ihrer Sicht Unternehmen, welche bereits ISO 27001 zertifiziert sind, im Rahmen der kommenden Umsetzung der NIS-Richtlinie bzw. des NISG einen Vorsprung hinsichtlich der nötigen technischen und organisatorischen Maßnahmen?

3.2.2 „Self Assessment für NIS-Readiness”

Von Bedeutung zur Entwicklung dieses „Self Assessment für NIS-Readiness“ kann der folgende Artikel 14 (2) der NIS-Richtlinie angesehen werden:

> „*Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen ergreifen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.*“[190]

Es ist somit nur eine Frage der Zeit, bis von Seiten Österreichs entsprechende Vorgaben erlassen werden, welche die BwD dazu verpflichten geeignete Maßnahmen zu ergreifen. Dabei ist die Formulierung „geeignete Maßnahmen“ äußerst interpretierbar. Der selbstentwickelte Prototyp (= Self Assessment) in dieser Masterarbeit sollte als Werkzeug dienen, um diese Maßnahmen anhand des aktuellen Wissens abzuleiten, auszuformulieren und sicherzustellen, so dass diese in Zukunft eingehalten werden können.

Das entwickelte Self Assessment zur Bestimmung der eigenen unternehmensspezifischen „NIS-Readiness“ zielt primär auf die Anwendung durch BwD und IT-SP ab, wobei hier nicht zwischen den beiden unterschieden wurde. Hauptgrund dafür war, dass BwD zwar die Verantwortungen nicht an Dritte (z.B. IT-SP) übertragen können (vgl. z.B. Kapitel 2.4.4 oder 2.5.4), aber es in Zukunft durchaus vertragliche Regelungen geben kann, die einer Angleichung nahekommen könnten. Die nach NIS-Richtlinie definierten AdD werden zwar auf Basis der Richtlinie in Teilbereichen ähnlichen Vorgaben unterworfen, jedoch ist ein erheblicher Anteil der Vorgaben hinsichtlich z.B. Sicherheitsanforderungen, Meldepflicht, Aufsicht nur in abgeschwächter Form umzusetzen.

Folgend soll die Wortkreation „NIS-Readiness“ erläutert werden, um ein gemeinsames Verständnis für die weiteren Kapitel zu schaffen. Als „NIS-Readiness“ wird im Rahmen dieser Masterarbeit der Zustand verstanden, den ein Unternehmen erreichen sollte, um die potenziellen Kriterien der NIS-Richtlinie bzw. des zukünftigen österreichischen NISG zu erfüllen. Dabei werden wesentliche Rahmenbedingungen berücksichtigt, sowie

[190] (Amtsblatt der Europäischen Union 2016, S. 20)

relevante TOM´s um ein angemessenes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen und aufrechtzuerhalten.

Der selbstentwickelte Prototyp des „Self Assessment für NIS-Readiness“ ist im Anhang A dieser Masterarbeit verfügbar.

3.2.2.1 Methodik des “Self Assessment für NIS-Readiness”

Das Self Assessment (auch als Selbsteinschätzung bekannt) ist in dieser Masterarbeit eine Herangehensweise bzw. ein Werkzeug, dass es Unternehmen erlaubt, die Erfüllung von Kriterien der NIS-Richtlinie anhand eines Reifegrads zu bewerten. Dieses selbstentwickelte „Self Assessment für NIS-Readiness“ zeigt anhand eigener Antworten, sowohl textuell wie auch grafisch, entsprechende Handlungsfelder oder Stärken auf und liefert im Anlassfall bereits konkrete Hinweise, aus denen sich Maßnahmen ableiten lassen.

Auf Basis der umfangreichen Literaturrecherche sind viele Themen mit Bezug zu NIS, Informationssicherheit, IT-Sicherheit, usw. erhoben worden. Um all dieses dokumentierte Wissen in eine sinnstiftende und für Unternehmen hilfreiche Form zu bringen, wurden verschiedene Überlegungen angestellt. Wie bereits in Kapitel 2.3.4 beschrieben, wurden in Österreich beispielsweise risikoorientierte Ansätze verfolgt. Auch eine Ausarbeitung in Form einer klassischen Checkliste wäre ein praktikabler Ansatz gewesen. Da sich viele Elemente der NIS-Richtlinie als Prozesse darstellen lassen und prozesshaft zu entwickeln sind, wurde die Entscheidung getroffen, eine Bewertung anhand eines Modells aus dem Prozessmanagement vorzunehmen. Anhand von sogenannten „Reifegraden“ lässt sich der erreichte Grad eines spezifischen Prozesses oder einer Prozessverbesserung darstellen.

Im deutschsprachigen Raum hat sich im Laufe der letzten Jahre das Qualitätsmanagementmodell nach ISO 9001 weit verbreitet. Alternativ wäre mit dem Prozessreferenzmodell nach ISO 15504 (auch als SPICE bekannt) noch ein anderer fachspezifischer Standard zweckmäßig anwendbar gewesen, da dieser inhaltlich weitestgehend den gleichen Bereich wie CMMI abdeckt und eine ähnliche Bewertung des Reifegrads vorsieht. Da CMMI jedoch entsprechende themennahe „Best Practices“ bietet, war dieses Modell zielführender, da es spezifische Inhalte betrachtet und der Fokus nicht auf allgemeine abstrakte Formulierungen - wie öfters in ISO-Normen der Fall - gelegt wird.

Allgemein verfolgt CMMI das Ziel, die Arbeitsabläufe innerhalb einer Organisation zu verbessern. Es sind die wesentlichen Elemente wirksamer Prozesse eines oder mehrerer Fachgebiete enthalten und es wird ein evolutionärer Verbesserungsweg beschrieben.[191]

Wie in Abbildung 23 dargestellt, ist im CMMI prinzipiell zwischen den beiden Ansätzen der Prozessverbesserung auf Basis von „Reifegrad“ (spezifische Ziele) und „Fähigkeitsgrad“ (generische Ziele) zu unterscheiden. Im Rahmen dieses Self Assessments wurde nach eingehendem Literaturstudium die Entscheidung getroffen, die Bewertung der Prozessgebiete auf Basis von Reifegraden (rot umrahmt) vorzunehmen.

[191] Vgl. (CMMI Product Team 2011, S. 17)

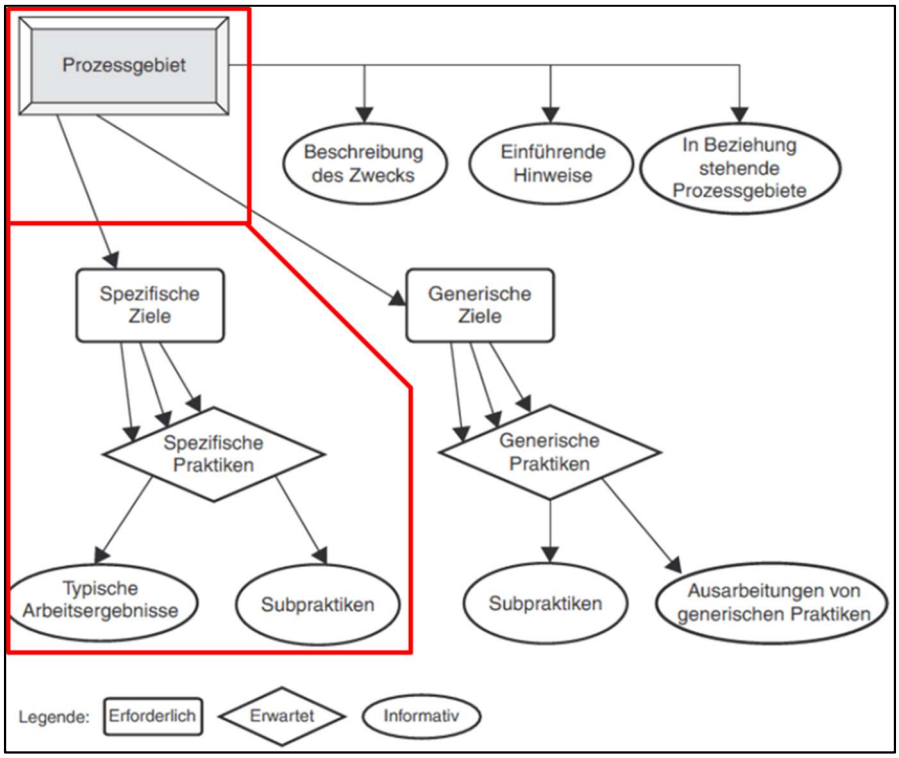


Abbildung 23: CMMI-Modellkomponenten[192]

Laut der CMMI-Literatur bezieht sich die Darstellung in Reifegraden standardmäßig auf die Gesamtreife eines festgelegten Satzes von Prozessen. Somit beziehen sich Reifegrade darauf, wie gut / schlecht eine Organisation die Prozessverbesserungen auf mehreren Prozessgebieten erreicht. Sinn und Zweck dieser Grade ist es, jene Prozesse zu verbessern, die zu einer definierten Menge von Prozessgebieten gehören.[193] Da die im Self Assessment enthaltenen Themen in vielen Bereichen als Gruppierungen einzelner Prozesse angesehen werden können bzw. eine Prozessverbesserung auf mehreren Prozessgebieten angestrebt werden sollte, war die Darstellungsform in Reifegraden zweckmäßiger.

Da es sich beim Thema Cybersicherheit bzw. konkret bei der NIS-Richtlinie um ein sehr spezifisches Thema handelt, wurde methodisch der CMMI-Ansatz in angepasster Form angewendet. Im Self Assessment wurde deshalb eine modifizierte CMMI-Darstellungsform von NIS-relevanten Prozessgebieten gewählt. Die zur Anwendung gekommenen Ziel-Reifegrade wurden auf Basis der drei CMMI-Modelle (vgl. Kapitel 2.1.4) ermittelt, auf Anwendbarkeit abgeglichen und entsprechend adaptiert im Self Assessment festgelegt.

3.2.2.2 Technische Umsetzung

In der heutigen Zeit stehen in der IT eine Fülle an Werkzeugen zur Verfügung um ein solches Self Assessment zu entwickeln und bereitzustellen. Ob dies nun in Form von z.B.

- Webformular,
- Selbstentwickelte Anwendung oder
- Standardapplikation

[192] (CMMI Product Team 2011, S. 22)

[193] Vgl. (CMMI Product Team 2011, S. 35)

umgesetzt wird, kann individuell sehr unterschiedlich sein. Auch wird die gewählte Form oftmals davon abhängig sein, in welcher Phase der Entwicklung (z.B. Anforderungsdefinition, Konzeption und Entwicklung, Test) sich das Thema befindet.

Ebenso mussten Überlegungen mit einfließen, wo und wie die potenziellen Informationen gespeichert werden und wem diese zugänglich sind. Vor allem wenn es sich - wie in diesem Fall - um sensible Daten handelte, sind Vorkehrungen zwecks Datenschutz und Informationssicherheit zu berücksichtigen. Je nachdem ob die Bereitstellung und Nutzung „Online“ und / oder „Offline“ angestrebt wird, können diverse organisatorische und technische Möglichkeiten angewendet werden.

Im gegenständlichen Fall, wurde vorerst ein Prototyp des „Self Assessment für NIS-Readiness“ entwickelt, um theoretische Überlegungen in eine prinzipielle Funktionsweise zu überführen und um eine Bewertung vornehmen zu können. Aus diesem Grunde wurde zwecks Prototyping die Nutzung einer weitverbreiteten (prinzipiell) offlinefähigen Standardapplikation als zweckmäßiger Ansatz gewählt.

Im Rahmen des verfügbaren Microsoft Office 2016 Pakets wurde die lokal installierte Anwendung „Microsoft® Excel® 2016“ als Werkzeug zur Entwicklung genutzt. Vor allem die weite Verbreitung dieser Anwendung (auch im Unternehmensbereich), die relativ einfache Handhabung durch die AnwenderInnen sowie die Abwärtskompatibilität zu den eigenen Vorgängerversionen waren überzeugende Argumente.

3.2.2.3 Struktur und Inhalt des Self Assessments

Da während des Erstellungszeitraums dieser Masterarbeit kein, für Österreich anwendbares, NISG in Kraft war bzw. auch kein diesbezüglicher Gesetzesentwurf öffentlich zugänglich war, ist das gegenständliche Self Assessment auf Basis folgender Richtlinien (bzw. Gesetze) und Normen entwickelt worden:

- NIS-Richtlinie und IT-SiG (BSI-KritisV) Inhalte
- ISO 27001:2013 (vgl. Kapitel 2.1.6.1) und ISO 27017:2015 (vgl. Kapitel 2.1.6.2)

Diese Vielfalt an Quellen ergab sich dadurch, dass zentrale Inhalte der NIS-Richtlinie äußerst vage und allgemein formuliert sind, wie z.B. „Stand der Technik“. Hier ist die Gesetzgebung in Deutschland bereits konkreter mit Verweisen auf branchenspezifische Sicherheitsstandards (B3S) und entsprechenden Inhalten. Der Bezug zum deutschen IT-SiG war in diesem Sinne naheliegend (vgl. Kapitel 2.5). Da jedoch diese B3S auch auf internationale Normen referenzieren und ein starker Querbezug hergestellt wird, so war es erforderlich diverse Inhalte der beiden genannten ISO-Normen zu integrieren.

Erst mit Berücksichtigung dieses umfangreichen, dokumentieren Wissens, konnte eine konkrete Hilfestellung in Form eines Self Assessments entwickelt werden. In diesem Rahmen wurden technische und organisatorische Auswirkungen ausformuliert und es ließen sich relevante Themen ableiten um sicherzustellen, dass NIS-Vorgaben auch laufend auf Einhaltung geprüft werden können.

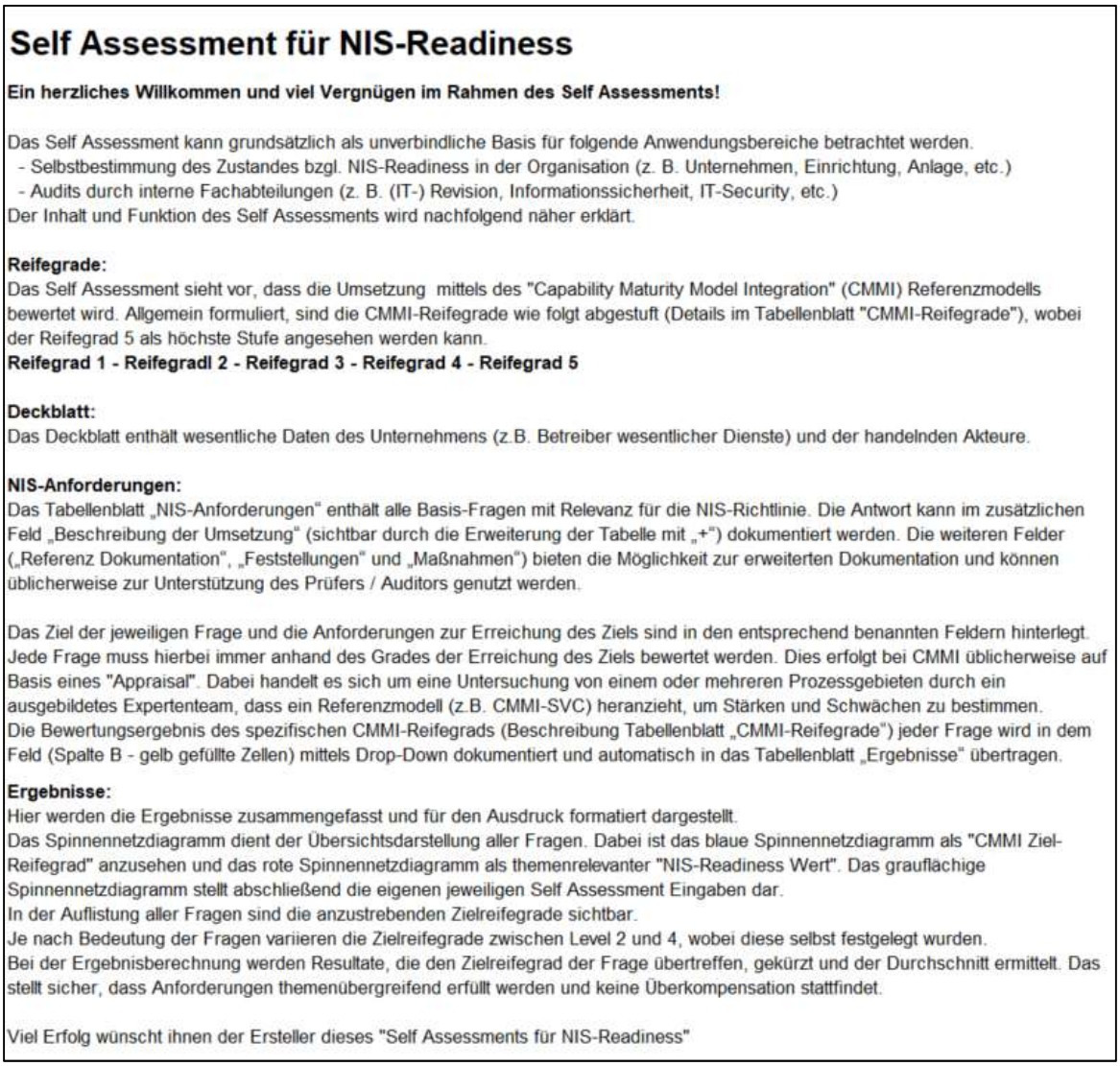
Das Self Assessment ist dabei nicht als vollumfängliche inhaltliche Aufzählung aller kritischen Bereiche zu sehen, sondern soll aktuelle, grundlegende, technische und organisatorische Rahmenbedingungen für BwD, wie auch IT-SP, adressieren. Dadurch soll ein erster Einblick zur eigenen „NIS-Readiness“ geschaffen werden, so dass sich aus abgeleiteten Maßnahmen eine Steuerung unterstützen bzw. realisieren lässt.

Die so erarbeiteten:

- 11 NIS-Themenbereiche mit
- insgesamt 26 spezifischen NIS-Themen

sind, gemäß der Forschungsfrage F 1 (vgl. Kapitel 1.4) als jene technischen und organisatorischen Auswirkungen anzusehen, die sich durch das Inkrafttreten der NIS-Richtlinie auf die betroffenen IT-SP in Österreich sowie die BwD ergeben.

Grundlegend unterteilt sich das „Self Assessment für NIS-Readiness“ in fünf einzelne Tabellenblätter um eine Übersichtlichkeit und Nutzungsfreundlichkeit zu gewährleisten. Als Einstieg wird im Tabellenblatt „Willkommen“ (vgl. Abbildung 24) eine Kurzerklärung über Aufbau, Inhalt, Verwendung und Ergebnisdarstellung des Self Assessments gegeben.



Self Assessment für NIS-Readiness

Ein herzliches Willkommen und viel Vergnügen im Rahmen des Self Assessments!

Das Self Assessment kann grundsätzlich als unverbindliche Basis für folgende Anwendungsbereiche betrachtet werden.
- Selbstbestimmung des Zustandes bzgl. NIS-Readiness in der Organisation (z. B. Unternehmen, Einrichtung, Anlage, etc.)
- Audits durch interne Fachabteilungen (z. B. (IT-) Revision, Informationssicherheit, IT-Security, etc.)

Der Inhalt und Funktion des Self Assessments wird nachfolgend näher erklärt.

Reifegrade:
Das Self Assessment sieht vor, dass die Umsetzung mittels des "Capability Maturity Model Integration" (CMMI) Referenzmodells bewertet wird. Allgemein formuliert, sind die CMMI-Reifegrade wie folgt abgestuft (Details im Tabellenblatt "CMMI-Reifegrade"), wobei der Reifegrad 5 als höchste Stufe angesehen werden kann.
Reifegrad 1 - Reifegradl 2 - Reifegrad 3 - Reifegrad 4 - Reifegrad 5

Deckblatt:
Das Deckblatt enthält wesentliche Daten des Unternehmens (z.B. Betreiber wesentlicher Dienste) und der handelnden Akteure.

NIS-Anforderungen:
Das Tabellenblatt „NIS-Anforderungen“ enthält alle Basis-Fragen mit Relevanz für die NIS-Richtlinie. Die Antwort kann im zusätzlichen Feld „Beschreibung der Umsetzung“ (sichtbar durch die Erweiterung der Tabelle mit „+“) dokumentiert werden. Die weiteren Felder („Referenz Dokumentation“, „Feststellungen“ und „Maßnahmen“) bieten die Möglichkeit zur erweiterten Dokumentation und können üblicherweise zur Unterstützung des Prüfers / Auditors genutzt werden.

Das Ziel der jeweiligen Frage und die Anforderungen zur Erreichung des Ziels sind in den entsprechend benannten Feldern hinterlegt. Jede Frage muss hierbei immer anhand des Grades der Erreichung des Ziels bewertet werden. Dies erfolgt bei CMMI üblicherweise auf Basis eines "Appraisal". Dabei handelt es sich um eine Untersuchung von einem oder mehreren Prozessgebieten durch ein ausgebildetes Expertenteam, dass ein Referenzmodell (z.B. CMMI-SVC) heranzieht, um Stärken und Schwächen zu bestimmen.
Die Bewertungsergebnis des spezifischen CMMI-Reifegrads (Beschreibung Tabellenblatt „CMMI-Reifegrade“) jeder Frage wird in dem Feld (Spalte B - gelb gefüllte Zellen) mittels Drop-Down dokumentiert und automatisch in das Tabellenblatt „Ergebnisse“ übertragen.

Ergebnisse:
Hier werden die Ergebnisse zusammengefasst und für den Ausdruck formatiert dargestellt.
Das Spinnennetzdiagramm dient der Übersichtsdarstellung aller Fragen. Dabei ist das blaue Spinnennetzdiagramm als "CMMI Ziel-Reifegrad" anzusehen und das rote Spinnennetzdiagramm als themenrelevanter "NIS-Readiness Wert". Das grauflächige Spinnennetzdiagramm stellt abschließend die eigenen jeweiligen Self Assessment Eingaben dar.
In der Auflistung aller Fragen sind die anzustrebenden Zielreifegrade sichtbar.
Je nach Bedeutung der Fragen variieren die Zielreifegrade zwischen Level 2 und 4, wobei diese selbst festgelegt wurden.
Bei der Ergebnisberechnung werden Resultate, die den Zielreifegrad der Frage übertreffen, gekürzt und der Durchschnitt ermittelt. Das stellt sicher, dass Anforderungen themenübergreifend erfüllt werden und keine Überkompensation stattfindet.

Viel Erfolg wünscht ihnen der Ersteller dieses "Self Assessments für NIS-Readiness"

Abbildung 24: Tabellenblatt „Willkommen“ im „Self Assessment für NIS-Readiness“

Obwohl eine Bewertung auf Basis des Reifegradmodells CMMI angewendet wurde, kann ein flächendeckender detaillierter Einblick nicht erwartet werden. Vor diesem Hintergrund wurde im zweiten Tabellenblatt „CMMI-Reifegrade“ (vgl. Abbildung 25) eine zusammenfassende Erklärung gegeben, was Reifegrade generell sind und welche bei CMMI bestehen.

Self Assessment für NIS-Readiness

Erläuterung des CMMI-Modells und der darin enthaltenen Reifegrade

Die Bewertung der Reifegrade erfolgt auf Basis des CMMI Refernzmodell. Das Reifegradmodell unterscheidet hierbei folgende fünf verschiedene Reifegrade:

- Reifegrad 1: Initial
- Reifegrad 2: Geführt
- Reifegrad 3: Definiert
- Reifegrad 4: Quantitativ geführt
- Reifegrad 5: Prozessoptimierung

Gemäß CMMI können Organisationen die eigene Reife progressiv verbessern, indem sie die Steuerung anfangs auf Projektebene übernehmen und dann bis zur höchsten Ebene fortschreiten. In diesem Zusammenhang sind dabei qualtitative wie auch quanitative Daten zur Entscheidungsfindung zu nutzen. Standardmäßig bildet dabei jeder CMMI-Reifegrad eine erforderliche Basis für den darauf folgenden bzw. jeder CMMI-Reifegrad beinhaltet alle Fähigkeiten des vorangegangenen Reifegrads, und ist als Basis für die weitere Prozessverbessserung zu betrachten. Es kann als kontraproduktiv angesehen werden, dass ein Reifegrad ausgelassen wird.

Abbildung 25: Tabellenblatt „CMMI-Reifegrade“

Damit potenzielle AnwenderInnen eine seriöse Selbsteinschätzung vornehmen und von einem gemeinsamen Verständnis ausgehen können, wurden die einzelnen Reifegrade in den Abbildung 26 und Abbildung 27 näher beschrieben.

Reifegrad 1:
Bei diesem Reifegrad 1 ist festzuhalten, dass die Arbeitsabläufe üblicherweise ad hoc und chaotisch durchgeführt werden. Die Prozesse sind nur rudimentär oder gar nicht definiert. Oftmals ist eine große Abhängigkeit vom individuellem Einsatz und der Kompetenz weniger einzelner Mitarbeiter gegeben.

Reifegrad 2:
Bei diesem Reifegrad 2 ist festzuhalten, dass
- sichergestellt ist, dass die Arbeitsabläufe entsprechend der Leitlinien geplant und ausgeführt werden.
- Fachpersonal mit ausreichenden Ressourcen eingesetzt werden, damit kontrollierte Ergebnisse erzeugt werden.
- relevante Stakeholder einbezogen werden.
- Arbeitsabläufe entsprechend überwacht, gesteuert und geprüft werden
- die Einhaltung der Prozessbeschreibung einer Bewertung unterzogen wird.
- Arbeitsergebnisse und Dienstleistungen spezifizierten Prozessbeschreibungen, Normen und Verfahren erfüllen.

Reifegrad 3:
Bei diesem Reifegrad 3 ist festzuhalten, dass die Arbeitsabläufe gut charakterisiert und verstanden sind. Sie werden zudem in Form von entsprechenden Normen, Verfahren, Hilfsmitteln und Methoden beschrieben. Die relevanten Standardprozesse, welche die Basis für den Reifegrad 3 bilden, sind etabliert und wurden mit der Zeit verbessert.

Wesentliche Unterschiede zwischen den Reifegraden 2 und 3 sind:
- der Geltungsbereich der Normen, Prozessbeschreibungen und Verfahren. Bei Reifegrad 2 können sich diese zwischen einzelnen Umsetzungen eines Prozesses (z.B. für ein bestimmtes Projekt) erheblich unterscheiden. Im Falle des Reifegrad 3, werden diese andererseits passend für z.B. ein bestimmtes Projekt aus einem Set von Standardprozessen abgeleitet.
- das Prozesse auf Reifegrad 3 üblicherweise strenger als auf Reifegrad 2 zu beschreiben sind. Ein definierter Prozess hat klar beschrieben, den Zweck, die Eingangsgrößen, Eingangskriterien, Tätigkeiten, Rollen, Messgrößen, Verifizierungsschritte, Ergebnisse und Ausgangskriterien. Die Prozesse werden auf Reifegrad 3 stärker proaktiv geführt.

In diesem Reifegrad 3 werden jene Prozesse durch die Organisation weiter verbessert, welche zu den Prozessgebieten gemäß des Reifegrad 2 gehören.

Abbildung 26: Tabellenblatt „CMMI-Reifegrade“ Reifegrad 1 - 3

Reifegrad 4: Sobald eine Organisation Standardprozesse implementiert hat, wird gemäß CMMI als nächster Schritt eine intensive Nutzung von Metriken und Kennzahlen empfohlen. So soll für Verbesserungsmaßnahmen eine bessere Entscheidungsgrundlage erlangt werden. Bei diesem Reifegrad 4 werden für die Organisation quantitative Ziele für die Qualitäts- und Prozessleistung etabliert und als Kriterien zum Zwecke des Managements verwendet. Diese quantitativen Ziele basieren auf den Bedürfnissen - der Kunden - der Endanwender - der Organisation und - der Prozessbeteiligten. Qualitäts- und Prozessleistung sind statistische Größen. Es werden bestimmte Messwerte der Prozessleistung für festgelegte (Teil-)Prozesse erfasst und statistisch analysiert. Anhand von Prozessleistungs-Baselines und Prozessleistungsmodellen können Qualitäts- und Prozessleistungsziele aufgestellt werden, welche beim Erreichen relevanter Geschäftsziele helfen. Als bedeutender Unterschied zwischen Reifegrad 3 und 4 kann die Vorhersagbarkeit der Prozessleistung betrachtet werden. Im Reifegrad 4 wird die Leistung ausgewählter (Teil-)Prozessen mittels statistischer und verschiedener quantitativer Techniken gesteuert. Vorhersagen erfolgen teilweise auf Basis von statistischen Analysen detaillierter Prozessdaten.
Reifegrad 5 Dabei handelt es sich um die höchste Stufe im Modell. Das Hauptaugenmerk wird auf die kontinuierliche Weiterentwicklung bzw. Verbesserung des Prozesses gelegt. Als Schwerpunkt dieses Reifegrads kann die kontinuierliche Verbesserung der Prozessleistung durch inkrementelle und innovative Technologie- und Prozessverbesserung angesehen werden. Die jeweiligen Qualitäts- und Prozessleistungsziele der Organisation sind - etabliert, - werden kontinuierlich überarbeitet, um Änderungen widerzuspiegeln, und - werden als Kriterien für das Management der Prozessverbesserung verwendet. Die Auswirkungen angewendeter Prozessverbesserungen werden beispielsweise mit statistischen und verschiedenen quantitativen Techniken gemessen und darauf folgend mit den entsprechenden Qualitäts- und Prozessleistungszielen verglichen. Der wesentliche Unterschied zwischen Reifegrad 4 und 5 kann darin gesehen werden, dass der Schwerpunkt auf das Management und die Verbesserung der Organisationsleistung gelegt wird. Die Organisation beschäftigt sich im Reifegrad 5 mit der Gesamtleistung der Organisation und zieht dazu mehrere erfasste Daten heran. Im Zuge der Datenanalyse werden Mängel und Lücken in der Leistung aufgezeigt, welche zu organisationsweiten Prozessverbesserungen anregen.

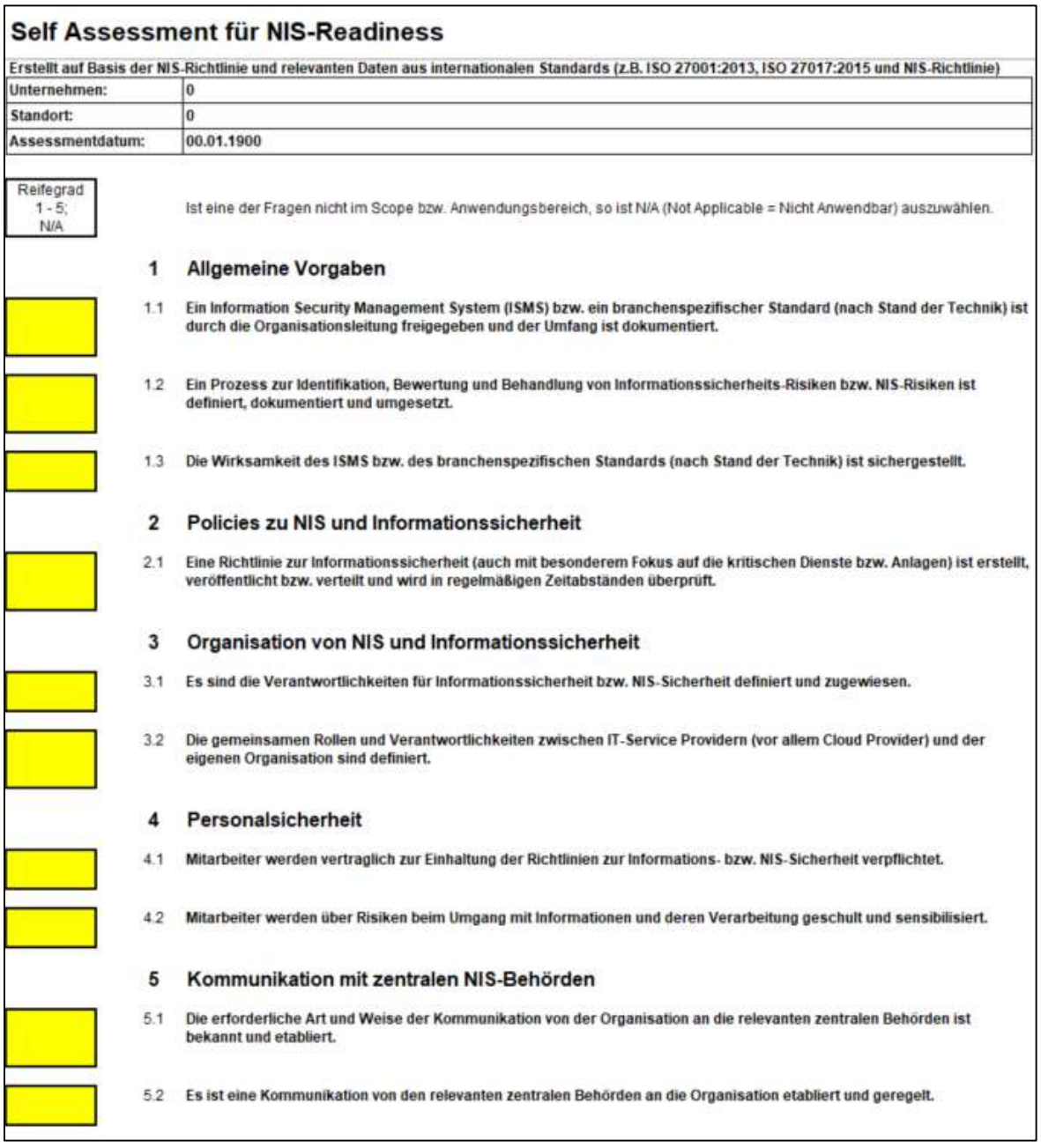
Abbildung 27: Tabellenblatt „CMMI-Reifegrade“ Reifegrad 4 – 5

Abgeleitet aus dem Anspruch, dass dieses Self Assessment auch nachvollziehbar und transparent sein soll, wurden im Tabellenblatt „Deckblatt“ (vgl. Abbildung 28) diverse Informationen (primär zum Unternehmen und jeweils mitwirkenden Personen) abgefragt.

Self Assessment für NIS-Readiness	
Konzern / Gruppe:	
Unternehmen:	
Standort:	
Anschrift:	
Website:	
Assessmentdatum:	
Ansprechpartner:	
Telefon bzw. Mobil Nr.:	
E-Mail Adresse:	
Ersteller:	
Telefon bzw. Mobil Nr.:	
E-Mail Adresse:	
Geschäftsführung:	
Unterschrift:	
Version: 1.0.0 / Datum	

Abbildung 28: Tabellenblatt „Deckblatt“

Im eigenen Tabellenblatt „NIS-Anforderungen“ (vgl. Abbildung 29) wurde das verfügbare dokumentierte Wissen mit Bezug zur NIS-Richtlinie verarbeitet. Gesamthaft sind 11 NIS-Themenbereiche (z.B. „1 Allgemeine Vorgaben“) mit 26 spezifischen NIS-Themen (z.B. „1.1 Ein Information Security Management System [...].“) darin ausgestaltet. Diese Darstellungsform diente dazu, dass thematisch eine relativ rasche Orientierung möglich war.



Self Assessment für NIS-Readiness

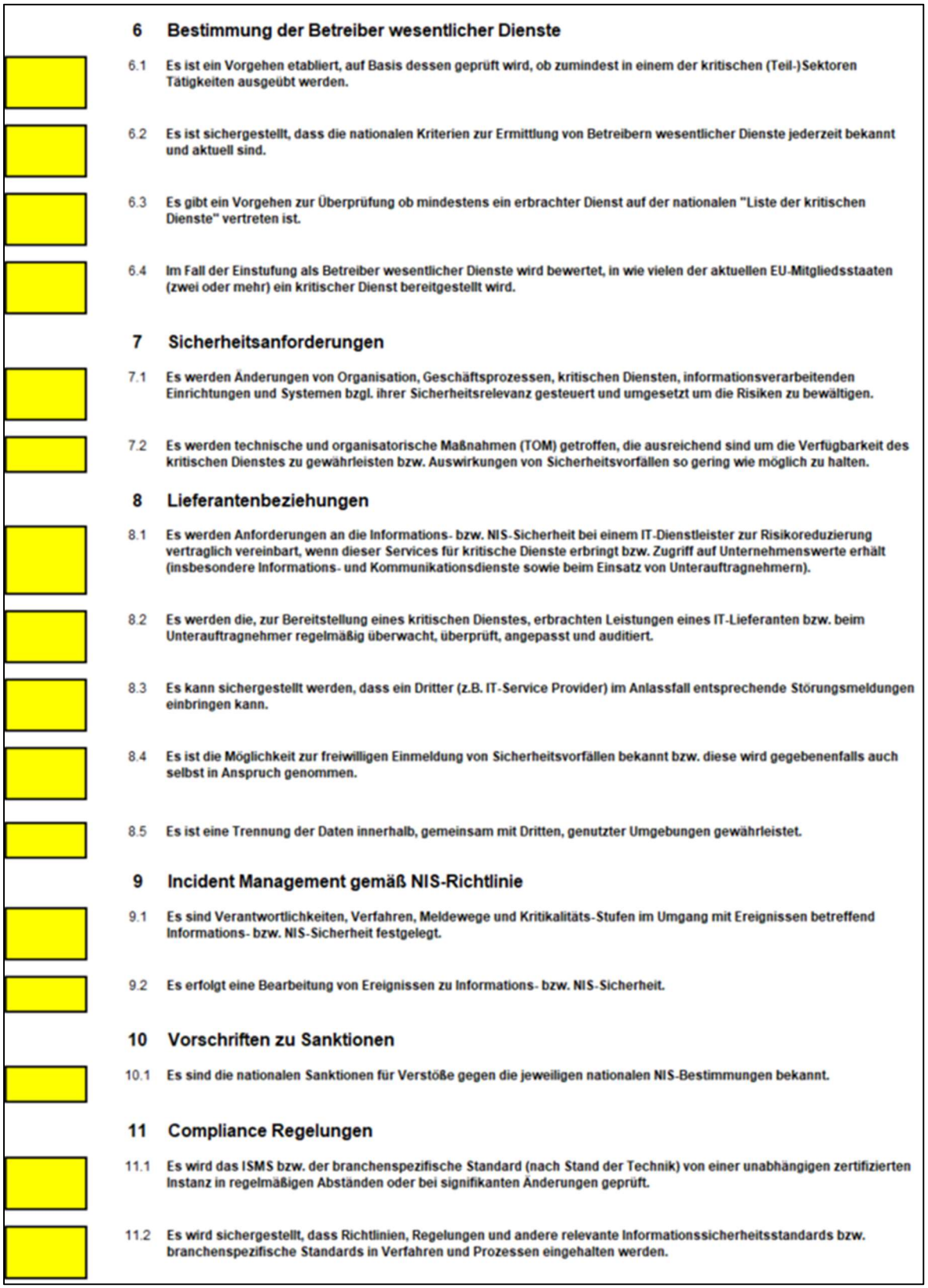
Erstellt auf Basis der NIS-Richtlinie und relevanten Daten aus internationalen Standards (z.B. ISO 27001:2013, ISO 27017:2015 und NIS-Richtlinie)

Unternehmen:	0
Standort:	0
Assessmentdatum:	00.01.1900

Reifegrad 1 - 5; N/A		
		Ist eine der Fragen nicht im Scope bzw. Anwendungsbereich, so ist N/A (Not Applicable = Nicht Anwendbar) auszuwählen.
	1	**Allgemeine Vorgaben**
	1.1	Ein Information Security Management System (ISMS) bzw. ein branchenspezifischer Standard (nach Stand der Technik) ist durch die Organisationsleitung freigegeben und der Umfang ist dokumentiert.
	1.2	Ein Prozess zur Identifikation, Bewertung und Behandlung von Informationssicherheits-Risiken bzw. NIS-Risiken ist definiert, dokumentiert und umgesetzt.
	1.3	Die Wirksamkeit des ISMS bzw. des branchenspezifischen Standards (nach Stand der Technik) ist sichergestellt.
	2	**Policies zu NIS und Informationssicherheit**
	2.1	Eine Richtlinie zur Informationssicherheit (auch mit besonderem Fokus auf die kritischen Dienste bzw. Anlagen) ist erstellt, veröffentlicht bzw. verteilt und wird in regelmäßigen Zeitabständen überprüft.
	3	**Organisation von NIS und Informationssicherheit**
	3.1	Es sind die Verantwortlichkeiten für Informationssicherheit bzw. NIS-Sicherheit definiert und zugewiesen.
	3.2	Die gemeinsamen Rollen und Verantwortlichkeiten zwischen IT-Service Providern (vor allem Cloud Provider) und der eigenen Organisation sind definiert.
	4	**Personalsicherheit**
	4.1	Mitarbeiter werden vertraglich zur Einhaltung der Richtlinien zur Informations- bzw. NIS-Sicherheit verpflichtet.
	4.2	Mitarbeiter werden über Risiken beim Umgang mit Informationen und deren Verarbeitung geschult und sensibilisiert.
	5	**Kommunikation mit zentralen NIS-Behörden**
	5.1	Die erforderliche Art und Weise der Kommunikation von der Organisation an die relevanten zentralen Behörden ist bekannt und etabliert.
	5.2	Es ist eine Kommunikation von den relevanten zentralen Behörden an die Organisation etabliert und geregelt.

Abbildung 29: Tabellenblatt „NIS-Anforderungen“ Thema 1 - 5

Wie in Abbildung 30 ersichtlich ist, wurde vor allem dem Themenbereich „8 Lieferantenbeziehungen“ mit fünf spezifischen Themen („8.1“ - „8.5“) eine größere Bedeutung beigemessen. Denn wie sich im Laufe der Literaturrecherche zunehmend herausstellte, können die BwD die Verantwortung nicht an die IT-SP übertragen, auch wenn diese kritische Dienstleistungen erbringen sollten. In diesem Sinne wird es zukünftig von besonderer Bedeutung sein, entsprechende Regelungen (z.B. SLA) mit den Vertragspartnern zu vereinbaren und diese einer zweckmäßigen Steuerung zu unterziehen (vgl. z.B. Kapitel 2.5.5 und 2.5.6).



	6	**Bestimmung der Betreiber wesentlicher Dienste**
	6.1	Es ist ein Vorgehen etabliert, auf Basis dessen geprüft wird, ob zumindest in einem der kritischen (Teil-)Sektoren Tätigkeiten ausgeübt werden.
	6.2	Es ist sichergestellt, dass die nationalen Kriterien zur Ermittlung von Betreibern wesentlicher Dienste jederzeit bekannt und aktuell sind.
	6.3	Es gibt ein Vorgehen zur Überprüfung ob mindestens ein erbrachter Dienst auf der nationalen "Liste der kritischen Dienste" vertreten ist.
	6.4	Im Fall der Einstufung als Betreiber wesentlicher Dienste wird bewertet, in wie vielen der aktuellen EU-Mitgliedsstaaten (zwei oder mehr) ein kritischer Dienst bereitgestellt wird.
	7	**Sicherheitsanforderungen**
	7.1	Es werden Änderungen von Organisation, Geschäftsprozessen, kritischen Diensten, informationsverarbeitenden Einrichtungen und Systemen bzgl. ihrer Sicherheitsrelevanz gesteuert und umgesetzt um die Risiken zu bewältigen.
	7.2	Es werden technische und organisatorische Maßnahmen (TOM) getroffen, die ausreichend sind um die Verfügbarkeit des kritischen Dienstes zu gewährleisten bzw. Auswirkungen von Sicherheitsvorfällen so gering wie möglich zu halten.
	8	**Lieferantenbeziehungen**
	8.1	Es werden Anforderungen an die Informations- bzw. NIS-Sicherheit bei einem IT-Dienstleister zur Risikoreduzierung vertraglich vereinbart, wenn dieser Services für kritische Dienste erbringt bzw. Zugriff auf Unternehmenswerte erhält (insbesondere Informations- und Kommunikationsdienste sowie beim Einsatz von Unterauftragnehmern).
	8.2	Es werden die, zur Bereitstellung eines kritischen Dienstes, erbrachten Leistungen eines IT-Lieferanten bzw. beim Unterauftragnehmer regelmäßig überwacht, überprüft, angepasst und auditiert.
	8.3	Es kann sichergestellt werden, dass ein Dritter (z.B. IT-Service Provider) im Anlassfall entsprechende Störungsmeldungen einbringen kann.
	8.4	Es ist die Möglichkeit zur freiwilligen Einmeldung von Sicherheitsvorfällen bekannt bzw. diese wird gegebenenfalls auch selbst in Anspruch genommen.
	8.5	Es ist eine Trennung der Daten innerhalb, gemeinsam mit Dritten, genutzter Umgebungen gewährleistet.
	9	**Incident Management gemäß NIS-Richtlinie**
	9.1	Es sind Verantwortlichkeiten, Verfahren, Meldewege und Kritikalitäts-Stufen im Umgang mit Ereignissen betreffend Informations- bzw. NIS-Sicherheit festgelegt.
	9.2	Es erfolgt eine Bearbeitung von Ereignissen zu Informations- bzw. NIS-Sicherheit.
	10	**Vorschriften zu Sanktionen**
	10.1	Es sind die nationalen Sanktionen für Verstöße gegen die jeweiligen nationalen NIS-Bestimmungen bekannt.
	11	**Compliance Regelungen**
	11.1	Es wird das ISMS bzw. der branchenspezifische Standard (nach Stand der Technik) von einer unabhängigen zertifizierten Instanz in regelmäßigen Abständen oder bei signifikanten Änderungen geprüft.
	11.2	Es wird sichergestellt, dass Richtlinien, Regelungen und andere relevante Informationssicherheitsstandards bzw. branchenspezifische Standards in Verfahren und Prozessen eingehalten werden.

Abbildung 30: Tabellenblatt „NIS-Anforderungen“ Thema 6 - 11

In den jeweils zugeordneten Gelb hinterlegten Zellen (vgl. Abbildung 31 rot umrahmt war der themenspezifische Reifegrad auszuwählen, wobei ausschließlich die Werte 1, 2, 3, 4, 5 oder N/A systemtechnisch zulässig sind. Andere Wert-Eingaben werden im Rahmen der Datenüberprüfung aufgrund der getroffenen Einschränkungen als unzulässig abgelehnt.

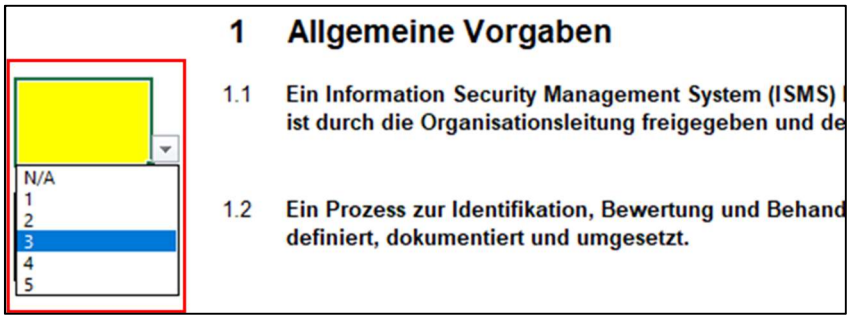


Abbildung 31: Auswahlliste der Reifegrade

Als ein repräsentatives Beispiel soll anhand des NIS-Thema 8.1 (vgl. Abbildung 32) die generelle Struktur innerhalb dieses Tabellenblatts im „Self Assessment für NIS-Readiness“ erläutert werden. Dieser strukturelle Aufbau ist durchgängig auf alle 26 Themen angewendet worden, wobei die einzelnen, gruppierten Ebenen individuell erweitert bzw. reduziert werden können.

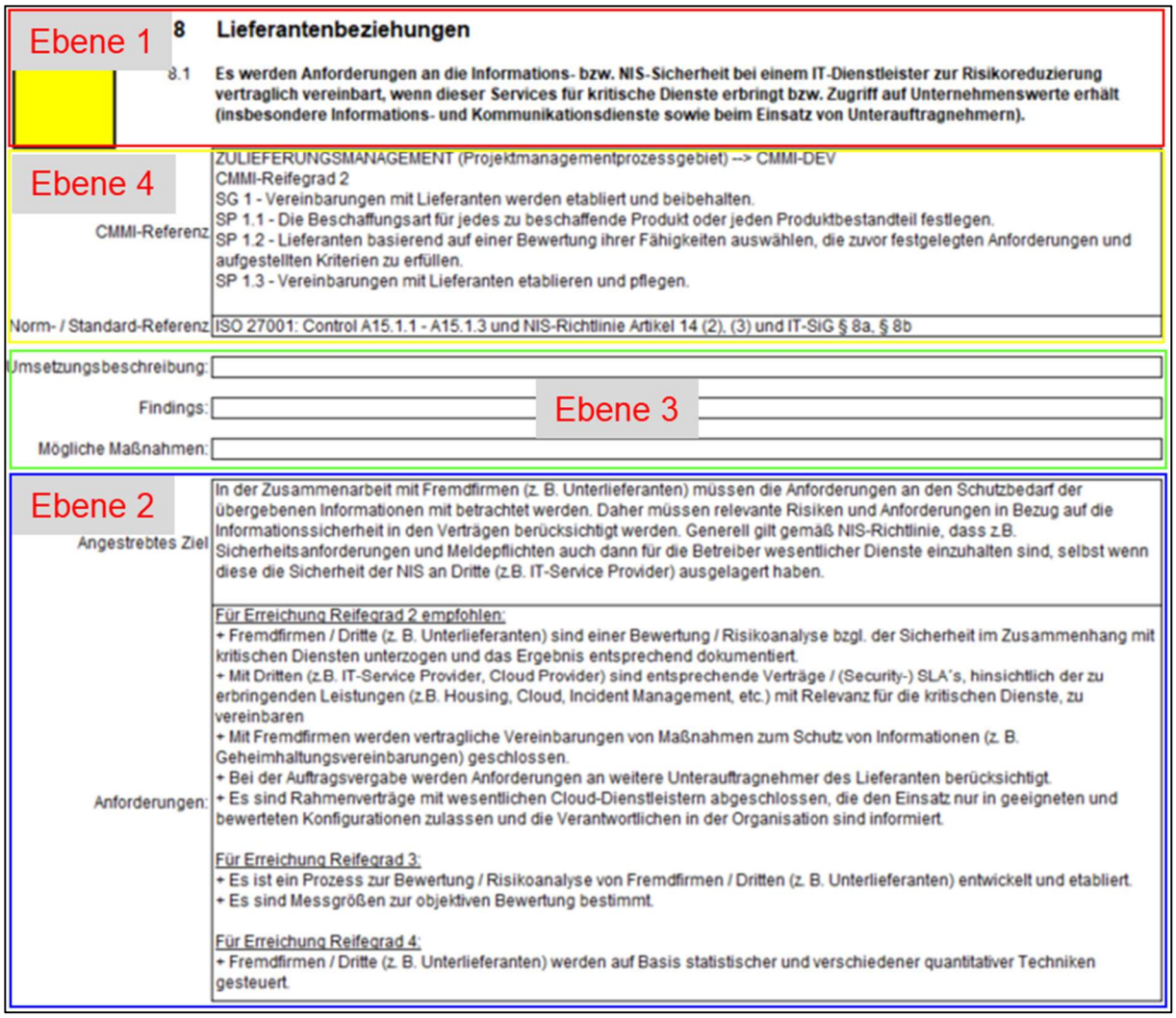


Abbildung 32: Repräsentatives NIS-Thema 8.1

Auf Ebene 1 (rot umrahmt in Abbildung 32) wird die oberste Ebene des Self Assessments dargestellt. Diese besteht aus den 11 NIS-Themenbereichen (hier „8 Lieferanten-beziehungen“) und den 26 spezifischen NIS-Themen (hier „8.1“). Diese Ebene kann im Gegensatz zu den anderen drei Ebenen nicht reduziert werden.

Die Ebene 2 (blau umrahmt in Abbildung 32) enthält das konkret ausformulierte Ziel, welches im Rahmen dieses NIS-Thema angestrebt wird, Ebenso sind die Anforderungen dargestellt, die zur Umsetzung empfohlen werden. Je nach erforderlichem Reifegrad sind dabei Mindestanforderungen beschrieben oder themenspezifisch auch Empfehlungen für höhere Reifegrade eingearbeitet. Diese Ebene kann somit als zentrales Element der tatsächlichen Bewertung angesehen werden.

Im Rahmen der Ebene 3 (grün umrahmt in Abbildung 32) können mittels Freitext die Felder für die Umsetzungsbeschreibung, diverse Findings und mögliche Maßnahmen genutzt werden. Diese Ebene kann im Falle von relevanten Informationen herangezogen werden und hat somit hauptsächlich Dokumentationscharakter.

Anhand der Informationen auf Ebene 4 (gelb umrahmt in Abbildung 32) kann nachvollzogen werden, woraus sich das jeweilige Thema abgeleitet hat und wie der Querbezug zu relevanten Quellen ist. Einerseits wird auf die Elemente der NIS-Richtlinie, bestehender deutscher Gesetze oder von IT-relevanten Normen verwiesen und andererseits ist die Referenz zum entsprechenden CMMI-Reifegrad hergestellt.

Im abschließenden Tabellenblatt „Ergebnisse“ (vgl. Abbildung 33) wird auf Basis der vorhin bewerteten Reifegrade (vgl. Abbildung 31), das Gesamtergebnis des „Self Assessment für NIS-Readiness“ zum Einstieg grafisch dargestellt.

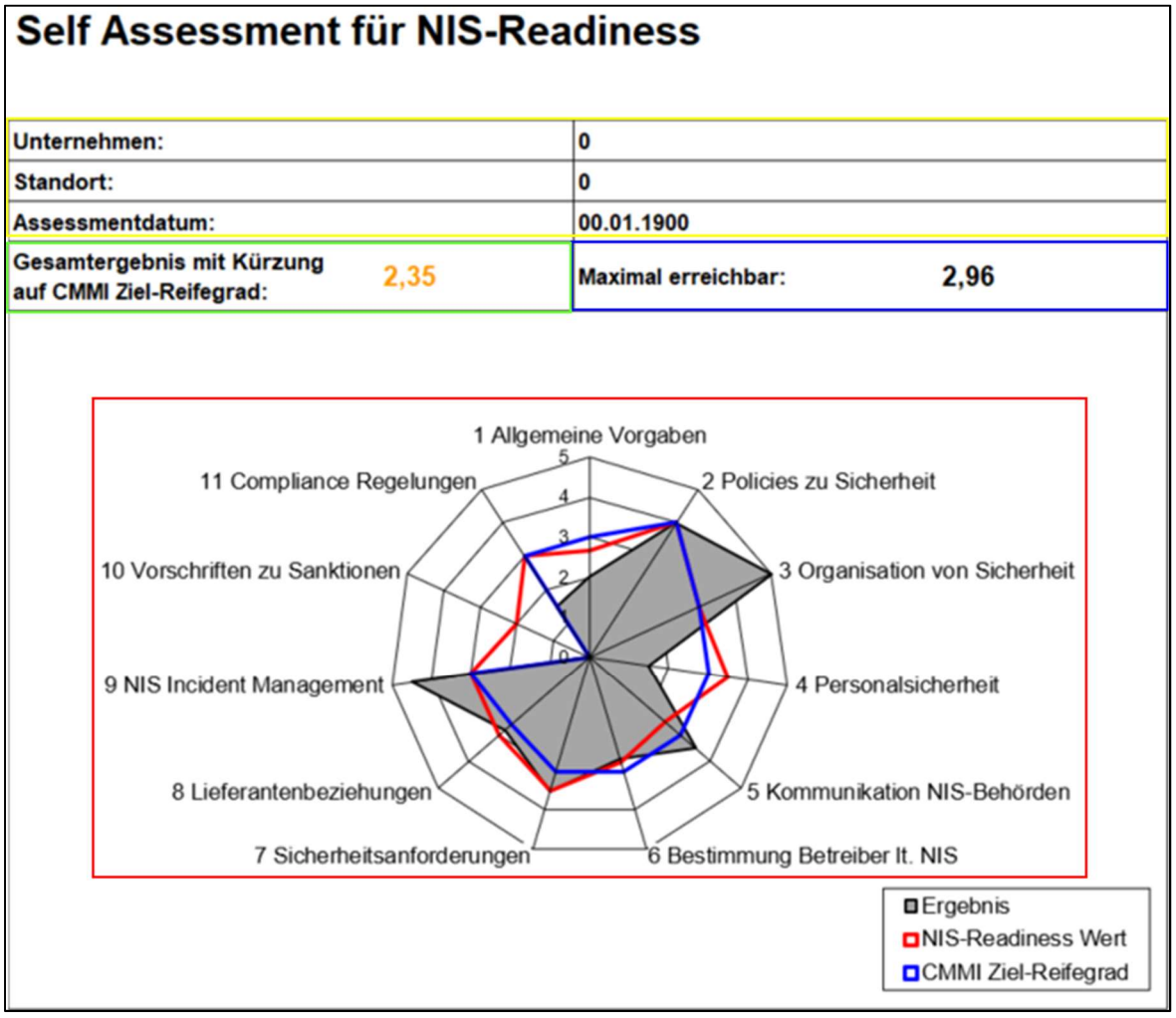


Abbildung 33: Spinnennetzdiagramm des „Self Assessment für NIS-Readiness“

Als Darstellungsform wurde dafür das Spinnennetzdiagramm (rot umrahmt in Abbildung 33) gewählt, in dem die kalkulierten „CMMI-Ziel-Reifegrade“ und die eigens definierten „NIS-Readiness Werte“ den aktuellen Ist-Reifegraden (= Ergebnis) des eigenen Unternehmens gegenübergestellt werden. Der NIS-Readiness Wert unterscheidet sich dahingehend vom CMMI Ziel-Reifegrad, dass CMMI zwar konkrete IT-Themen berücksichtigt, jedoch die NIS-Richtlinie in einigen Bereichen spezielle Elemente adressiert. Um diese Besonderheiten entsprechend zu würdigen, wurden auf Basis der umfangreichen Literaturrecherche und der eigenen Expertise themenspezifisch eigene Ziel-Reifegrade definiert, welche sich im NIS-Readiness Wert darstellen. Im beschriebenen „Self Assessment für NIS-Readiness“ Prototyp, ist dieser NIS-Readiness Wert jedoch ausschließlich als informativ anzusehen und fließt in keine der spezifischen Berechnungen ein.

Diese Interpretation bietet sich durchaus für Managementzwecke an, da rasch eine Orientierung bzgl. der 11 übergeordneten Themenbereiche möglich ist und vordergründig gewisse Abweichungen zu erfassen sind. In diesem Beispiel in Abbildung 33 wurden zur Veranschaulichung beliebige Reifegrade in der Reihenfolge 1, 2, 3, 4, 5 und N/A in das Tabellenblatt „NIS-Anforderungen“ eingetragen.

Auf Basis der bis zu 26 NIS-Themen kann ein maximal erreichbarer NIS-Readiness Wert (blau umrahmt in Abbildung 33) kalkuliert werden. Dieser Wert errechnet sich gemäß Abbildung 34.

$$Maximal\ erreichbar\ = \frac{\sum\ CMMI\ Ziel - Reifegrade}{\sum Anzahl\ bewertete\ NIS - Themen}$$

Abbildung 34: Formel für „Maximal erreichbaren NIS-Readiness Wert“

Dabei wurde die Annahme getroffen, dass jedes NIS-Thema welches mit N/A bewertet wird, sowohl im Zähler wie auch im Nenner, nicht in die Berechnung einfließt. So sollen Verzerrungen aufgrund verschiedener Rahmenbedingungen reduziert werden.

Eine High-Level Kennzahl wie das „Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad“ (grün umrahmt in Abbildung 33) kann als „Score“ des eigenen Unternehmens interpretiert werden. Dabei errechnet sich der Wert wie in Abbildung 35 ersichtlich.

$$\begin{matrix} Gesamtergebnis\ mit\ Kürzuung \\ auf\ CMMI\ Ziel - Reifegrad \end{matrix} = \frac{\sum eingetragene\ Ist - Reifegrade}{\sum Anzahl\ bewertete\ NIS - Themen}$$

Abbildung 35: Formel für „Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad“

Wie bereits vorhin beschrieben, werden mit N/A bewertete Themen aus der Kalkulation ausgeschlossen. Es wurde zudem noch eine weitere spezielle Annahme für die Berechnung getroffen: Es könnte der Fall eintreten, dass durch einzelne sehr hoch bewertete Ist-Reifegrade (bei den 26 NIS-Themen) andere stark unterdurchschnittliche Ist-Reifegrade ausgeglichen werden und so dennoch eine Erreichung des CMMI Ziel-Reifegrads möglich wäre. Dieser Umstand wird im Rahmen dieser Masterarbeit als sogenannte Überkompensation bezeichnet. Um eine Verzerrung der „NIS-Readiness“ anhand dieser Überkompensation zu vermeiden, wird systemtechnisch jeder eingetragene Ist-Reifegrad anlassbezogen auf den CMMI Ziel-Reifegrad gedeckelt.

Als zusätzliche Orientierungshilfe wird für das „Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad“ noch die Darstellungsform des Ampelsystems (vgl. Abbildung 33 und Abbildung 36) angewendet. Dabei wurden folgende Schwellwerte als praktikabel definiert:

- Rot und somit als kritisch anzusehen, wenn das Gesamtergebnis einen Wert von <= 70% des maximal erreichbaren NIS-Readiness Wert aufweist.
- Orange und deshalb mit Optimierungspotenzial, wenn das Gesamtergebnis einen Wert von <= 90% des maximal erreichbaren NIS-Readiness Wert aufweist.
- Grün und somit als NIS-Ready anzusehen, wenn das Gesamtergebnis einen Wert von > 90% des maximal erreichbaren NIS-Readiness Wert aufweist.

Die in Abbildung 33 gelb umrahmten Datenfelder befüllen sich automatisch aus dem Tabellenblatt „Deckblatt“, sofern darin die Informationen eingetragen wurden.

Als zweiter Teil des Tabellenblatts „Ergebnisse“ (vgl. Abbildung 36) werden die bewerteten Ist-Reifegrade der 26 NIS-Themen in verdichteter Tabellenform dargestellt.

Self Assessment für NIS-Readiness
Ergebnisse

Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad:	2,35	Maximal erreichbar:	2,96

Details:

Spezifisches Ziel Nr.	Themen	CMMI Ziel-Reifegrad	Ergebnis
1.1	Freigabe eines ISMS oder branchenspezifischen Standards	3	1
1.2	Prozess für Risikomanagement bzgl. Informations- bzw. NIS-Sicherheit	3	2
1.3	Wirksamkeit des ISMS oder branchenspezifischen Standards	3	3
2.1	Richtlinie für Informations- bzw. NIS-Sicherheit	4	4
3.1	Verantwortlichkeiten für Informations- bzw. NIS-Sicherheit	3	5
3.2	Definierte Rollen und Verantwortlichkeiten mit IT-Service Providern	N/A	N/A
4.1	Vertragsverpflichtung der Mitarbeiter zur Informations- bzw. NIS-Sicherheit	3	1
4.2	Sensibilisierung und Schulung der Mitarbeiter bzgl. Risiken	3	2
5.1	Kommunikationsschiene an nationale zentrale Behörden	3	3
5.2	Kommunikationsschiene von Seiten der nationalen zentralen Behörden	3	4
6.1	Prüfung über Tätigkeiten in kritischen (Teil-)Sektoren	3	5
6.2	Nationale Kriterien bzgl. Betreiber wesentlicher Dienste	N/A	N/A
6.3	Prüfung der nationalen "Liste der kritischen Dienste"	3	1
6.4	Erbringung kritischer Dienste in mehreren EU-Mitgliedsstaaten	3	2
7.1	Änderungsmanagement zur Risikobewältigung	3	3
7.2	Angemessene TOM zwecks Verfügbarkeit des kritischen Dienstes	3	4
8.1	Vertragliches Risikomanagement bei Zusammenarbeit mit IT-Dienstleister	2	5
8.2	Überprüfung erbrachter Leistungen von IT-Lieferanten	3	3
8.3	Anlassbezogene Störungsmeldung durch IT-Dienstleister	2	1
8.4	Freiwillige Einmeldung von Sicherheitsvorfällen	3	2
8.5	Trennung von Informationen in gemeinsam genutzten Umgebungen (Cloud)	3	3
9.1	Berichtswesen für Vorfälle bzgl. Informations- bzw. NIS-Sicherheit	3	4
9.2	Bearbeitung von Vorfällen zu Informations- bzw. NIS-Sicherheit	3	5
10.1	Nationale Sanktionen bei Verstößen gegen NIS-Bestimmungen	N/A	N/A
11.1	Unabhängige Prüfung des ISMS bzw. branchenspezifischen Standards	3	1
11.2	Wirksamkeitsprüfung des ISMS bzw. branchenspezifischen Standards	3	2

Methode:
- Vergleich von 26 ausgewählten IT-Sicherheits-Themen mit NIS-Bezug
- basierend auf Controls von ISO 27001 und ISO 27017
- basierend auf Vorgaben der NIS-Richtlinie und des deutschen IT-SiG
- bewertet nach Reifegraden gemäß CMMI V1.3

Abbildung 36: Themen und Ergebnisse des „Self Assessment für NIS-Readiness“

Die beiden, in obiger Abbildung 36, blau und grün umrahmten Werte sind deckungsgleich mit jenen aus Abbildung 33.

Der gelb umrahmte Bereich in Abbildung 36 enthält in verdichteter Form die einzelnen 26 NIS-Themen die es mittels Reifegrad zu bewerten galt. Die Zahlen in der Spalte „Spezifisches Ziel Nr." sind mittels Hyperlink in diesem Dokument mit dem jeweiligen NIS-Thema im Tabellenblatt „NIS-Anforderungen" verknüpft.

Der wesentlichste Bereich ist in Abbildung 36 rot umrahmt. Darin werden die einzelnen eingetragenen Ist-Reifegrade den jeweiligen vorgeschlagenen CMMI Ziel-Reifegraden gegenübergestellt und verglichen. Wie bereits für Abbildung 33 festgehalten, kommt auch hier folgendes Ampelsystem zur Anwendung um eine Bewertung deutlich zu machen:

- Rot und somit als kritisch anzusehen, wenn das Ergebnis des NIS-Thema eine negative Abweichung von >= 2 vom definierten CMMI Ziel-Reifegrad aufweist (vgl. z.B. Spezifisches Ziel Nr. 1.1).
- Orange und deshalb mit Optimierungspotenzial, wenn das Ergebnis des NIS-Thema eine negative Abweichung von = 1 vom definierten CMMI Ziel-Reifegrad aufweist (vgl. z.B. Spezifisches Ziel Nr. 1.2).
- Grün und somit NIS-Ready, wenn das Ergebnis des NIS-Themas keine negative Abweichung vom definierten CMMI Ziel-Reifegrad aufweist (vgl. z.B. Spezifisches Ziel Nr. 1.3) oder diesen sogar übertrifft (vgl. z.B. Spezifisches Ziel Nr. 1.4).

Diese tabellarische Darstellungsform kann ebenfalls für Managementzwecke genutzt werden. Diese detailliertere Darstellung könnte bevorzugt durch verantwortliche Führungskräfte oder FachexpertInnen in Anspruch genommen werden, da in einem ersten Schritt bereits die kritischen Themen klar aufgezeigt werden, für welche es Maßnahmen zu entwickeln gibt und die umzusetzen sind.

Mittels diesem „Self Assessment für NIS-Readiness" ist eine Ausgangsbasis geschaffen worden, damit vielfältige TOM´s geprüft, aufgezeigt und gegebenenfalls einer Steuerung unterzogen werden können.

Das vollinhaltliche „Self Assessment für NIS-Readiness" kann dem Anhang B dieser Masterarbeit entnommen werden.

Die Forschungsfrage F 1 kann mit dem hier vorgestellten Inhalt des „Self Assessment für NIS-Readiness" (konkret das Tabellenblatt „NIS-Anforderungen") beantwortet werden. Es sind in Summe 26 spezifische NIS-Themen erarbeitet worden, die sich aus Vorgaben und Inhalten von Richtlinien, Gesetzen und Normen ableiten. Aus diesen ergeben sich im Detail die technischen und organisatorischen Auswirkungen, mit denen sich zukünftig die nationalen BwD und IT-SP befassen sollten, um den Anforderungen der NIS-Richtlinie bzw. des NISG zu genügen.

3.2.3 Einzelauswertung der ExpertInnenbefragungen

Das soeben beschriebene „Self Assessment für NIS-Readiness" soll für BwD wie auch IT-SP – bzgl. der Umsetzung und Steuerung von NIS-Vorgaben - eine Unterstützung bei

einer möglichst objektiven Selbsteinschätzung bieten. Aus diesem Grund wurde das Self Assessment einem definierten ExpertInnenkreis vorgestellt und Feedback eingeholt.

Die Präsentationen und Befragungen haben zeitlich und räumlich wie folgt stattgefunden.

- ExpertIn I: Befragung am 27.4.2018 von 10:00 – 11:00 in Wien (vor Ort)
- Experte II: Befragung am 23.4.2018 von 09:00 – 10:30 in Wien (vor Ort)
- Experte III: Befragung am 12.4.2018 von 17:20 – 19:30 in Wien (vor Ort)
- Experte IV: Befragung am 23.4.2018 von 09:00 – 10:30 in Wien (vor Ort)
- Experte V: Befragung am 20.4.2018 von 08:00 – 09:30 in Wien (vor Ort)
- Experte VI: Befragung am 3.5.2018 von 10:00 – 11:00 in Wien (virtuell)

Die nachfolgenden Ergebnisse, in den jeweiligen Unterkapiteln, sind die verdichteten Antworten der ExpertInnen, welche auf Basis des Fragebogens im Rahmen der Präsentation des Self Assessments erhoben wurden.

3.2.3.1 Inhalt des Self Assessments

Thematisch befassen sich die vier gestellten Fragen vornehmlich mit dem Inhalt und ob dadurch eine Hilfestellung für Unternehmen gegeben wird.

Frage 1: Genügt das „Self Assessment für NIS-Readiness" ihrer Meinung nach inhaltlich den bisher bekannten Anforderungen aus der NIS-Richtlinie?

Wie in Tabelle 1 ersichtlich, war die Beantwortung äußerst homogen. Mit „eher Ja" sind alle ExpertInnen der Meinung, dass dieses Self Assessment inhaltlich den Anforderungen entspricht.

Frage 1	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I		X			
Experte II		X			
Experte III		X			
Experte IV		X			
Experte V		X			
Experte VI		X			
Summe	0	**6**	0	0	0

Tabelle 1: Auswertung der Frage 1

Wie von einigen ExpertInnen angemerkt, wird als ein wesentlicher Faktor der Umstand gesehen, dass es in Österreich noch keine gesetzlichen Vorgaben (z.B. NISG) gibt.

Der Kommentar von Experte III lautet dazu: „*Vorbehaltlich der endgültigen gesetzlichen Vorgaben, welche in Österreich als Gesetzesentwurf noch durch die Gesetzgeber zu begutachten sind.*"

Thematisch in dieselbe Richtung geht der Kommentar des Experten IV: „*Problemfeld Österreich, Gesetz noch nicht fertig.*"

Auch die Anmerkung von Experte V deutet darauf hin: „*Es fehlen noch die Schwellwerte, die jedoch im Falle von Österreich erst in der zukünftigen Richtlinie / Gesetz ersichtlich sein werden.*“

Für zukünftige Weiterentwicklungen des Prototyps können noch die folgenden Kommentare der ExpertInnen angesehen werden.

Für ExpertIn I wären inhaltlich diese speziellen Themen von Bedeutung: „*Trendverlauf wäre für tourliche Assessments sinnvoll. Gesamtscore auf alle Fälle sinnvoll. Bei Überkompensation angeben, dass hier keine weitere Verbesserung möglich / sinnvoll ist.*“

Aus Sicht Experte II wäre folgender Aspekt noch von Interesse: „*Grundsätzlich ja, jedoch wird in diesem Zusammenhang „nur“ die eigene (persönliche bzw. unternehmensinterne) Sichtweise widergegeben. Das heißt, dass eine andere Meinung / Sichtweise von einer „unbefangenen“ Person z.B. Auditor (o.Ä.) sinnvoll wäre, damit das Assessment als OK einzustufen wäre.*“

Die Rückmeldung von Experten VI besagt: „*Der Fragebogen liefert einen guten ersten Eindruck über die Zielerreichung.*“

Zusammenfassend kann dazu angemerkt werden, dass - aus Sicht der teilnehmenden ExpertInnen - das „Self Assessment für NIS-Readiness“ inhaltlich den bisher bekannten Anforderungen weitestgehend genügt.

Frage 2: Ist das vorgestellte „Self Assessment für NIS-Readiness“ ihrer Meinung nach hinsichtlich Inhalt und Umfang zweckmäßig ausgestaltet und somit für Fachkundige hinsichtlich der Komplexität nutzbar?

Wie in Tabelle 2 zu sehen, sind alle ExpertInnen mit „Ja“ oder „eher Ja“ der Meinung, dass das Self Assessment zweckmäßig ausgestaltet und für Fachkundige nutzbar ist.

Frage 2	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I		X			
Experte II	X				
Experte III	X				
Experte IV		X			
Experte V	X				
Experte VI		X			
Summe	**3**	**3**	0	0	0

Tabelle 2: Auswertung der Frage 2

Laut Aussage von ExpertIn I besteht eventuell folgender Vorbehalt: „*Für Spezialisten & Fachexperten großer Unternehmen kein Problem, bei kleineren Unternehmen sehe ich die Gefahr, dass Fragestellungen nicht exakt bewertet werden können.*“

Der Kommentar des Experten VI beinhaltet zusätzlich eine Anregung für einen praktischen Verbesserungsvorschlag: „*Nutzbar für Fachabteilungen – weniger nutzbar für*

Geschäftsführung, da die Ergebnisse zwar Abweichungen zeigen, allerdings keine Maßnahmen davon abgeleitet werden können. Verbesserungsvorschlag:

- *Abgeleitet vom Ergebnis einen Maßnahmenkatalog mit den NIS Anforderungen pro Fachabteilung (HR, Sicherheit, Technology, etc.)*
- *Transformierung des einzelnen Reifegrads in einem Risiko Wert (Stichwort: Große Abweichung des CMMI bei 7.1 hat hohes Risiko vs. CMMI von 11.2 hat ein geringes Risiko)*"

Eine Erweiterung um z.B. einen extrahierten Maßnahmenkatalog je Fachbereich oder eine Risikobewertung könnte praktikabel sein. Wie in Kapitel 3.2.1 beschrieben, sind die mitwirkenden Personen durchwegs ExpertInnen im Bereich der NIS-Richtlinie bzw. IT(-Sicherheit). Es könnte eventuell hier der Umstand eintreten, dass zu dieser Frage eine „positivere" Einschätzung gegeben wird, als es z.B. bei „durchschnittlichen" potenziell betroffenen Unternehmen der Fall gewesen wäre.

Frage 3: Sind ihnen im Rahmen eines derartigen „Self Assessment für NIS-Readiness" technische und organisatorische Auswirkungen aufgezeigt worden, die sich auf Basis der NIS-Richtlinie ergeben könnten?

Wie in Tabelle 3 dargestellt, sind vier von sechs ExpertInnen mit „Ja" oder „eher Ja" der Meinung, dass dieses Self Assessment durchaus technische und organisatorische Auswirkungen aufgezeigt hat, welche sich auf Basis der NIS-Richtlinie ergeben könnten. Auf einen ersten Blick wirkt die Verteilung der ExpertInnenmeinungen inhomogen.

Frage 3	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I		X			
Experte II	X				
Experte III		X			
Experte IV	X				
Experte V				X	
Experte VI			X		
Summe	**2**	**2**	1	1	0

Tabelle 3: Auswertung der Frage 3

Der Kommentar von Experte VI ist als Anregung zur weiteren Konkretisierung der TOM´s dieses Self Assessments anzusehen: „*Gerade TOM's sollten besser ausspezifiziert werden – Referenz zur ISO ist gut, aber Auswirkungen werden nicht sichtbar gemacht.*"

Die eine „Nein"-Beantwortung durch Experte V kann mittels folgendem Kommentar erläutert werden: „*Durch andere Anforderungen wie etwa PSD II, MiFID, EZB, usw. sind Meldungen dieser Art bereits im eigenen Unternehmen bekannt. Audits auf Basis von / gegen Standards oder Normen wie z.B. ISAE 3402 Typ-2 oder ISO 27001:2013 tragen auch wesentlich zur Vorbereitung bei.*" In Kapitel 3.2.4.2 wird dies nochmals relativiert, dass es überwiegend dem tiefgehenden historischen Wissen im Unternehmen geschuldet ist und andernfalls das Self Assessment durchaus TOM´s aufzeigen würde.

Vor allem in Hinblick auf die Verifizierung der Hypothese H 5 sind die Rückmeldungen der ExpertInnen von Bedeutung. Grundlegend kann dazu festgehalten werden, dass sich mittels dieses Prototyps des „Self Assessment für NIS-Readiness" entsprechende technische und organisatorische Auswirkungen aufzeigen lassen können. Je nachdem wie intensiv die Unternehmen bereits mit der Materie in Berührung gekommen sind, ist auch das Potenzial entsprechende TOM´s aufzuzeigen unterschiedlich hoch. Vor allem in einer zukünftigen Anpassung des „Self Assessment für NIS-Readiness" sollte eine weiterführende Spezifizierung der TOM´s angedacht werden.

Frage 4: Würden Sie sagen, dass dieses „Self Assessment für NIS-Readiness" - aus inhaltlicher Sicht - potenziell betroffenen Unternehmen in Österreich eine Hilfestellung bezüglich Umsetzung der NIS-Richtlinie geben kann?

Gemäß den Informationen aus Tabelle 4 vertreten alle ExpertInnen mit „Ja" oder „eher Ja" die Meinung, dass dieses Self Assessment potenziell betroffenen Unternehmen in Österreich eine Hilfestellung bezüglich Umsetzung der NIS-Richtlinie geben kann.

Frage 4	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I	X				
Experte II	X				
Experte III		X			
Experte IV	X				
Experte V	X				
Experte VI		X			
Summe	**4**	2	0	0	0

Tabelle 4: Auswertung der Frage 4

Aus Sicht von ExpertIn I ist die angesprochene Hilfestellung im folgenden Bereich von Bedeutung: „*Auf alle Fälle KMU´s.*"

Von Seiten des Experten III wird angemerkt: „*Vorbehaltlich, wie konkret die gesetzliche Vorgabe in Österreich endgültig ausgestaltet und zur Umsetzung freigegeben wird.*"

„*Es werden die wesentlichen Disziplinen abgefragt.*" kommentiert Experte V.

Für den Experten VI gilt inhaltlich der gleiche Kommentar bzgl. der Antwort wie bereits für Frage 2 gegeben.

Mit Bezug zur Hypothese H 4 lässt sich in diesem Zusammenhang gänzlich bestätigen, dass aus Sicht der ExpertInnen ein Self Assessment eine Hilfestellung für potenziell betroffene Unternehmen sein kann. Im Kontext einer Hilfestellung sind auch Themen wie Bewertung und Einschätzung (vgl. Wortlaut Hypothese H 4) darin zu finden. Möglicherweise kann noch differenziert werden um welche Art von Unternehmen es sich handelt, ein Maßnahmenkatalog je Fachbereich extrahiert werden oder eine Risikobewertung miteinfließen. Der Nutzen wird jedoch für alle potenziell betroffenen Unternehmen in Österreich gesehen.

3.2.3.2 Methodik des Self Assessments

Die Inhalte der nachfolgenden vier gestellten Fragen zielen hauptsächlich darauf ab, die Methodik des Self Assessments zu prüfen und ob es in dieser Konstellation entsprechend sinnvoll angewendet und umgesetzt ist.

Frage 5: Ist aus ihrer Sicht ein „Self Assessment für NIS-Readiness" zur initialen Bewertung der Vorgaben aus der NIS-Richtlinie ein zweckmäßiges Mittel?

Wie in Tabelle 5 festgehalten, sind fünf von sechs ExpertInnen mit „Ja" oder „eher Ja" der Meinung, dass ein Self Assessment zur initialen Bewertung der NIS-Vorgaben ein zweckmäßiges Mittel darstellt.

Frage 5	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I					X
Experte II	X				
Experte III		X			
Experte IV	X				
Experte V	X				
Experte VI		X			
Summe	**3**	2	0	0	1

Tabelle 5: Auswertung der Frage 5

Die eine „Kommt drauf an"-Beantwortung durch ExpertIn I kann mittels folgendem Kommentar erläutert werden: „*Ob es zweckmäßig ist, kann ich aus dem heutigen Termin nicht beantworten.*" Somit konnte diese Frage mangels Detailtiefe im Rahmen dieses einen Präsentationstermins am 27.4.2018 nicht umfassend behandelt werden.

Aus Sicht des Experten VI stellt sich der Sachverhalt wie folgt dar: „*Initial ja – wobei eine „Stufe 2" für Fachabteilungen der nächste Schritt sein sollte.*"

Hinsichtlich der Hypothese H 4 kann in diesem Rahmen weitestgehend bestätigt werden, dass aus Sicht der ExpertInnen ein Self Assessment zur initialen Bewertung der Vorgaben aus der NIS-Richtline als zweckmäßig angesehen werden kann

Frage 6: Ist ihrer Meinung nach eine Bewertung der NIS-Readiness anhand des angewendeten Reifegradmodells (nach CMMI) zweckmäßig?

Wie in Tabelle 6 zu sehen ist, sind fünf von sechs befragten ExpertInnen mit „Ja" oder „eher Ja" der Meinung, dass eine Bewertung der NIS-Readiness auf Basis des angewendeten Reifegradmodells nach CMMI zweckmäßig ist.

Frage 6	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I		X			
Experte II	X				
Experte III			X		
Experte IV	X				
Experte V	X				
Experte VI	X				
Summe	**4**	1	1	0	0

Tabelle 6: Auswertung der Frage 6

Als wertvolle Rückmeldung bzgl. Weiterentwicklung des Prototyps ist der Kommentar von Experte III anzusehen: „*Ist hilfreich für Unternehmen, die noch keine eigene Bewertung aus Unternehmenssicht haben. Für Unternehmen die bereits intern eigene entsprechende Reifegrade bzw. Kennzahlen für die Themen vorgesehen oder etabliert haben, wäre es zweckmäßig diese im Self Assessment dar- bzw. gegenüberstellen zu können.*“

Der Kommentar von Experte V ist als durchaus differenziert zu betrachten: „*Die Anwendung eines Reifegradmodells ist durchaus branchenüblich bzw. kann je nach Branche als Standard angesehen werden.*“

Die fachliche Begründung zur „Ja“ Antwort von Experte VI lautet: „*CMMI liefert einen guten Eindruck über den Reifegrad.*“

Konkret kann laut den Kommentaren der ExpertInnen die Hypothese H 6, unter Berücksichtigung gewisser Rahmenbedingungen, als weitestgehend bestätigt betrachtet werden. Ein Reifegradmodell (z.B. CMMI) ist je nach Branche eventuell sogar als Standard anzusehen. Dennoch kann individuell eingeschränkt werden, dass je nach „Reife“ des Unternehmens, eigene unternehmensinterne Reifegrade bzw. Kennzahlen etabliert sind und diese bevorzugt angewendet werden würden.

Frage 7: Ist ihrer Meinung nach die Nutzung eines „Gesamtergebnis CMMI Ziel-Reifegrads“ wie im vorgestellten Self Assessment sinnvoll?

In Tabelle 7 ist dargestellt, dass vier von sechs ExpertInnen mit „Ja“ oder „eher Ja“ die Nutzung eines „Gesamtergebnis CMMI Ziel-Reifegrads“ als durchaus sinnvoll ansehen. Die Meinung ist hier also durchaus differenzierter.

Frage 7	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I		X			
Experte II	X				
Experte III				X	
Experte IV	X				
Experte V	X				
Experte VI			X		
Summe	**3**	1	1	1	0

Tabelle 7: Auswertung der Frage 7

Dabei kann aufgrund der Kommentare der ExpertInnen ein Vorbehalt gesehen werden, bzw. die ablehnende Haltung erklärt werden.

Experte III meint zum Sachverhalt: „*Die Darstellung des Ergebnisses als eine Gesamtkennzahl ist wenig aussagekräftig und kann als trügerisch angesehen werden. Es ist aussagekräftiger und zweckmäßiger, die einzelnen 26 IT-Sicherheits-Themen bzw. die 11 Themenbereiche des Self Assessments im Detail zu betrachten.*“

Eine in Teilen ähnliche Ansicht vertritt auch Experte II, wobei hier das Potenzial (deshalb die „Ja“ Antwort) auf den oberen Managementebenen hervorgehoben wird: „*Dieses „Gesamtergebnis CMMI Ziel-Reifegrad“ kann vor allem für die oberen / obersten Managementebenen hilfreich sein. Für eine Detailanalyse sind die Einzelwerte der jeweiligen Themen(-bereiche) mehr von Bedeutung.*“

Die Einschätzung von Experte VI lautet: „*Zu pauschal das Gesamtergebnis (siehe auch Antwort 2). Zielerreichung per Fachabteilung bzw. Thema mit einer automatisierten Liste an ToDo's.*“

Nach Meinung des Experten V bietet das „Gesamtergebnis CMMI Ziel-Reifegrad“ jenen Nutzen: „*Gibt einen guten Überblick für das Top-Management des Unternehmens.*“

Die Einzelergebnisse aus 26 NIS-Themen auf ein Gesamtergebnis zu aggregieren und als eine Kennzahl darzustellen ist möglicherweise sehr extrem und kann diverse Fehlinterpretationen zulassen. Um dem Problem – wie von Experten III und Experten VI angemerkt - vorzubeugen, sollte eine zwingende Berücksichtigung der Ergebnisse aus den jeweiligen 11 Themenbereichen bzw. der einzelnen 26 NIS-Themen (mit möglichen Maßnahmen) vorgesehen werden.

Frage 8: Ist für Sie ein „Self Assessment für NIS-Readiness“ hilfreich, um eventuell identifizierte Maßnahmen einer möglichen Behandlung zuzuführen?

Gemäß den Informationen aus Tabelle 8 vertreten fünf der sechs befragten ExpertInnen mit „Ja“ oder „eher Ja“ die Meinung, dass dieses Self Assessment hilfreich sein kann, um identifizierte Maßnahmen einer möglichen Behandlung zuzuführen.

Frage 8	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I			X		
Experte II		X			
Experte III	X				
Experte IV		X			
Experte V	X				
Experte VI		X			
Summe	2	**3**	1	0	0

Tabelle 8: Auswertung der Frage 8

Der Kommentar von Experten V dazu ist: „*Ein Self Assessment ist ein anerkanntes Verfahren, wie z.B. Audit.*“

Gemäß Betrachtung des Experten VI liegt folgende Situation vor: „*Wenn besser automatisiert mit Zielabweichungen - derzeit ist ein Maßnahmenkatalog nicht sichtbar.*“

3.2.3.3 Darstellung und Querbezug des Self Assessments

Diese letzten vier gestellten Fragen des Fragebogens bieten die Möglichkeit, sich von Seiten der ExpertInnen, eine qualifizierte Rückmeldung zu erhalten, ob eigene getroffene Annahmen in Zusammenhang mit der NIS-Richtlinie zielführend sind.

Frage 9: Finden Sie die grafische Aufbereitung der „NIS-Readiness im Self Assessment“ in Form eines Spinnennetzdiagramms verständlich?

Wie in Tabelle 9 zu erkennen ist, sind sich bei dieser Frage alle ExpertInnen einig. Die Darstellung in Form eines Spinnennetzdiagramms wird in der grafischen Aufbereitung als soweit verständlich und mit „Ja“ oder „eher Ja“ bewertet.

Frage 9	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I	X				
Experte II	X				
Experte III	X				
Experte IV	X				
Experte V	X				
Experte VI		X			
Summe	**5**	1	0	0	0

Tabelle 9: Auswertung der Frage 9

„*Gibt einen guten Überblick für das Top-Management des Unternehmens.*“ ist in diesem Zusammenhang die Meinung des Experten V.

In dieselbe Richtung geht die Aussage von Experten VI: „*Gute Management Übersicht.*“

Frage 10: Ist ihrer Meinung nach die hier vorgenommene Einschätzung (teils abweichend von CMMI) der Reifegrade zur Berechnung des „NIS-Readiness Werts“ realitätsnah?

Wie in Tabelle 10 ersichtlich, sind auch hier fünf der sechs ExpertInnen mit „Ja“ oder „eher Ja“ der Meinung, dass die hier vorgenommene Einschätzung der Reifegrade zur Berechnung des „NIS-Readiness Werts“ als realitätsnah angesehen werden kann.

Frage 10	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I		X			
Experte II		X			
Experte III					X
Experte IV		X			
Experte V	X				
Experte VI	X				
Summe	2	**3**	0	0	1

Tabelle 10: Auswertung der Frage 10

Die Einschätzung des Experten V lautet: „*Stufen im CMMI sind gut gewählt.*“

Die eine Bewertung „Kommt drauf an“ von Experte III ist wie folgt erklärbar: „*Aus Zeitgründen wurde diese konkrete Fragestellung nicht in der erforderlichen Tiefe erschöpfend behandelt und kann somit nicht bewertet werden.*“ Somit konnte diese Frage mangels Detailtiefe im Rahmen dieses einen Präsentationstermins am 12.4.2018 nicht ausreichend behandelt werden.

Thematisch ist eine Orientierung an den standardmäßigen CMMI-Reifegraden sinnvoll. Eine starre Ausrichtung an diesen CMMI-Reifegraden scheint jedoch nicht zweckmäßig zu sein, da die NIS-Richtlinie in gewissen Themenbereichen äußerst spezifische Anforderungen vorsieht. Aus diesem Grund kann die eigene Expertise in den Vordergrund gerückt werden und stattdessen ein selbstdefinierter „NIS-Readiness Wert“ je Themenbereich bzw. NIS-Thema eingearbeitet werden.

Frage 11: Ist ihrer Meinung nach die verhältnismäßig intensive Einbindung von Inhalten der ISO 27001 in das Self Assessment ein zielführender Ansatz?

In Tabelle 11 ist dargestellt, dass abermals fünf von sechs ExpertInnen mit „Ja“ oder „eher Ja“ die verhältnismäßig intensive Einbindung der ISO 27001 als zielführenden Ansatz empfinden.

Frage 11	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I	X				
Experte II					X
Experte III		X			
Experte IV	X				
Experte V	X				
Experte VI	X				
Summe	**4**	1	0	0	1

Tabelle 11: Auswertung der Frage 11

Bereits mit Ausblick auf das zukünftige NISG in Österreich wurde von Experten V folgende Antwort festgehalten: „*Das in Österreich noch zu verabschiedende Gesetz (NIS-Gesetz) wird auch Verweise auf die ISO 27001 enthalten. Des Weiteren ist die ISO 27001 ein Qualitätsmerkmal beim NIS-Gesetz.*“

Ähnlich schätzt Experte VI die Situation ein: „*ISO 27001 ist der (vermutlich) bekannteste ISMS Standard.*“

Die Antwort „Kommt drauf an“ von Seiten des Experten II zu diesem Thema ist: „*Die ISO 27001 ist nur zum Teil für die Umsetzung und Erfüllung des nationalen Gesetzes in Österreich relevant.*“

Als Teilaspekt zur Hypothese H 3 ist es von Interesse, dass mit der ISO 27001 in Bezug zur NIS-Richtlinie - zumindest in Teilen - dem Thema rund um die Informationssicherheit auch eine zentralere Rolle eingeräumt wird.

Frage 12: Haben aus ihrer Sicht Unternehmen, welche bereits ISO 27001 zertifiziert sind, im Rahmen der kommenden Umsetzung der NIS-Richtlinie bzw. des NISG einen Vorsprung hinsichtlich der nötigen technischen und organisatorischen Maßnahmen?

Laut Tabelle 12 sind fünf von sechs ExpertInnen mit „Ja" der Meinung, dass bereits ISO 27001 zertifizierte Unternehmen einen Vorsprung hinsichtlich der nötigen TOM´s im Rahmen der Umsetzung der NIS-Richtlinie haben werden.

Frage 12	Ja	eher Ja	eher Nein	Nein	Kommt drauf an (auf was?)
ExpertIn I			X		
Experte II	X				
Experte III	X				
Experte IV	X				
Experte V	X				
Experte VI	X				
Summe	**5**	0	1	0	0

Tabelle 12: Auswertung der Frage 12

Mit der Antwort „eher Nein" ist ExpertIn I mehr folgender Meinung: „*Eher aus der DSGVO & den notwendigen TOM´s.*"

Aus Sicht des Experten V ist die ISO 27001 ein wesentlicher Faktor, wie im Kommentar deutlich wird: „*Auf jeden Fall, da die Eckpunkte der Norm (ISO 27001) das NIS-Gesetz unterstützen bzw. darin behandelt werden.*"

Auch Experte VI vertritt hier eine eindeutige Meinung: „*Definitiv ja.*"

Hinsichtlich der Verifizierung der Hypothese H 3 sind diese Rückmeldungen der ExpertInnen von großem Nutzen. Mehrheitlich vertreten die ExpertInnen die klare Meinung, dass sich nach ISO 27001 zertifizierte Unternehmen bereits einen Vorsprung erarbeitet haben, welcher im Rahmen der Umsetzung der NIS-Richtlinie bei den nötigen TOM´s angesiedelt ist. Als Unternehmen sind in diesem Zusammenhang sowohl BwD wie auch IT-SP zu verstehen. Da gewisse Eckpunkte der ISO 27001 (z.B. ISMS) wahrscheinlich auch direkt in das österreichische NISG einfließen werden, so haben darauf ausgerichtete Unternehmen bereits entsprechende Vorarbeiten geleistet.

3.2.4 Self Assessment im Feldexperiment

Wie bereits zu Beginn dieser Masterarbeit in Kapitel 1.3 festgehalten, repräsentiert das „Self Assessment für NIS-Readiness" das Herzstück dieser Masterarbeit. Das Feedback der ExpertInnen (vgl. Kapitel 3.2.3) war fachlich äußerst fundiert und konnte deshalb sehr gut zum Ergebnis der Forschung herangezogen werden.

Es unterstütze die Praxisorientierung in einem hohen Maße, dass die Anwendbarkeit des selbstentwickelten Prototyps einem Feldexperiment unterzogen wurde. Zu diesem Zweck wurde mit einem potenziellen BwD und einem indirekt betroffenen IT-SP das „Self Assessment für NIS-Readiness" auf Basis realer Gegebenheiten verprobt und die Ergebnisse in den folgenden Unterkapiteln festgehalten. Als Einschränkung ist

anzumerken, dass im Rahmen der Feldexperimente keine vollumfängliche objektive Bewertung der vorhandenen erforderlichen Dokumentation (z.B. Richtlinien, Leitfäden) durchgeführt wurde, sondern weitestgehend die subjektive Bewertung der jeweiligen ExpertInnen als Tatsache anerkannt wurde.

Die beiden durchgeführten „Self Assessment für NIS-Readiness“ sind vollständig im Anhang C dieser Masterarbeit dokumentiert.

3.2.4.1 Feldexperiment ÖBB-Infrastruktur AG

Im Sine der Übersichtlichkeit werden ausschließlich die relevanten Inhalte des Tabellenblatts „Ergebnisse“ (vgl. Abbildung 37 und Abbildung 38) dargestellt.

Unternehmen:		**ÖBB-Infrastruktur AG**	
Standort:		**Praterstern 3**	
Assessmentdatum:		**23.04.2018**	
Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad:	**2,83**	**Maximal erreichbar:**	**2,91**

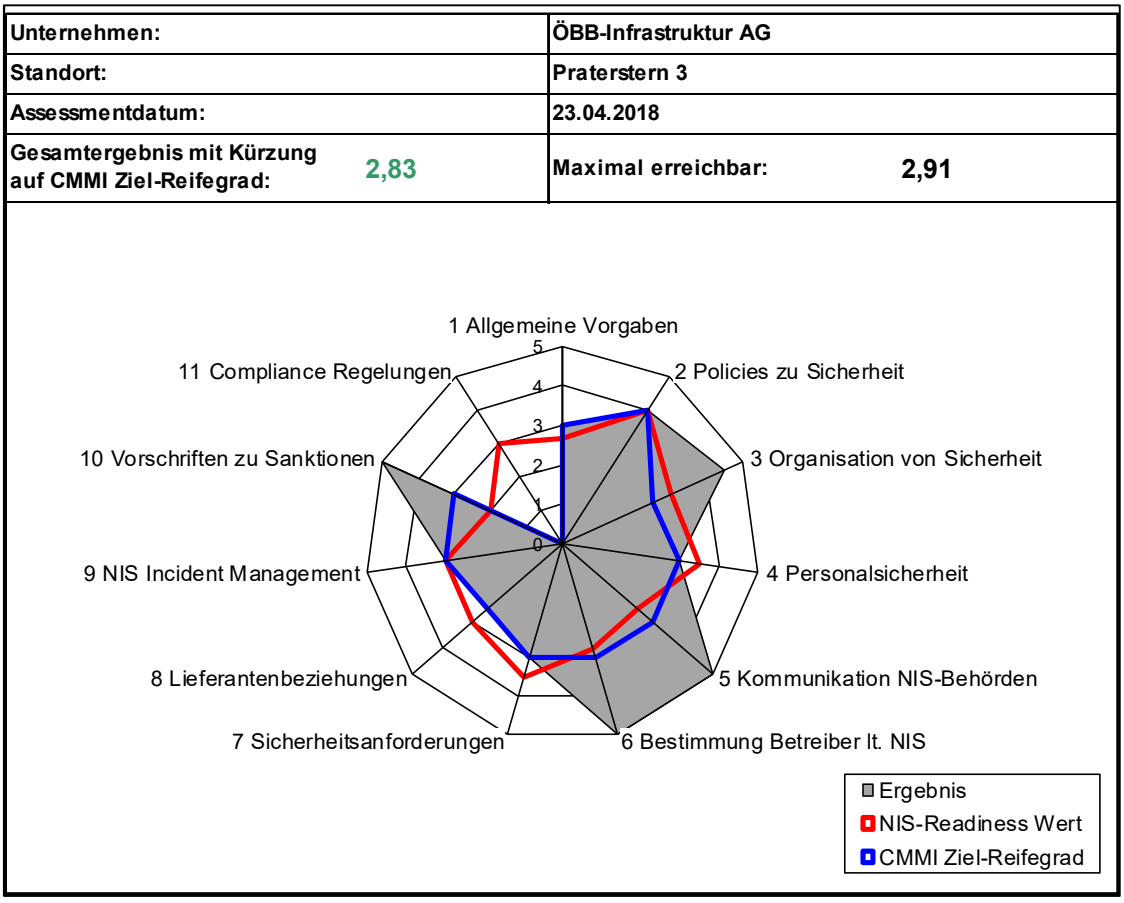


Abbildung 37: Self Assessment Spinnennetzdiagramm ÖBB-Infrastruktur AG

Wie im Spinnennetzdiagramm ersichtlich, erreicht die ÖBB-Infrastruktur AG in den 10 anwendbaren NIS-Themenbereichen die vorgegebenen CMMI Ziel-Reifegrade und würde mit einem Gesamtergebnis von 2,83 soweit als NIS-Ready anzusehen sein. Im Fall einer Anwendung des selbst definierten „NIS-Readiness Wert“, wären mögliche negative Abweichungen in einzelnen Themenbereichen (z.B. Personalsicherheit) erkennbar.

In der detaillierteren tabellarischen Gegenüberstellung (vgl. Abbildung 38) ist ableitbar, dass in den beiden spezifischen NIS-Themen 4.2 (Sensibilisierung und Schulung der Mitarbeiter bzgl. Risiken) und 8.2 (Überprüfung erbrachter Leistungen von IT-Lieferanten) entsprechende negative Abweichungen gegenüber dem CMMI Ziel-Reifegrad bestehen. Hier könnte somit ein Optimierungspotenzial bestehen.

Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad:	2,83	Maximal erreichbar:	2,91

Details:

Spezifisches Ziel Nr.	Themen	CMMI Ziel-Reifegrad	Ergebnis
1.1	Freigabe eines ISMS oder branchenspezifischen Standards	3	3
1.2	Prozess für Risikomanagement bzgl. Informations- bzw. NIS-Sicherheit	3	3
1.3	Wirksamkeit des ISMS oder branchenspezifischen Standards	3	3
2.1	Richtlinie für Informations- bzw. NIS-Sicherheit	4	4
3.1	Verantwortlichkeiten für Informations- bzw. NIS-Sicherheit	3	5
3.2	Definierte Rollen und Verantwortlichkeiten mit IT-Service Providern	2	4
4.1	Vertragsverpflichtung der Mitarbeiter zur Informations- bzw. NIS-Sicherheit	3	4
4.2	Sensibilisierung und Schulung der Mitarbeiter bzgl. Risiken	3	2
5.1	Kommunikationsschiene an nationale zentrale Behörden	3	5
5.2	Kommunikationsschiene von Seiten der nationalen zentralen Behörden	3	5
6.1	Prüfung über Tätigkeiten in kritischen (Teil-)Sektoren	3	5
6.2	Nationale Kriterien bzgl. Betreiber wesentlicher Dienste	3	5
6.3	Prüfung der nationalen "Liste der kritischen Dienste"	3	5
6.4	Erbringung kritischer Dienste in mehreren EU-Mitgliedsstaaten	3	5
7.1	Änderungsmanagement zur Risikobewältigung	3	3
7.2	Angemessene TOM zwecks Verfügbarkeit des kritischen Dienstes	3	3
8.1	Vertragliches Risikomanagement bei Zusammenarbeit mit IT-Dienstleister	2	2
8.2	Überprüfung erbrachter Leistungen von IT-Lieferanten	3	2
8.3	Anlassbezogene Störungsmeldung durch IT-Dienstleister	2	3
8.4	Freiwillige Einmeldung von Sicherheitsvorfällen	3	3
8.5	Trennung von Informationen in gemeinsam genutzten Umgebungen (Cloud)	N/A	N/A
9.1	Berichtswesen für Vorfälle bzgl. Informations- bzw. NIS-Sicherheit	3	3
9.2	Bearbeitung von Vorfällen zu Informations- bzw. NIS-Sicherheit	3	3
10.1	Nationale Sanktionen bei Verstößen gegen NIS-Bestimmungen	3	5
11.1	Unabhängige Prüfung des ISMS bzw. branchenspezifischen Standards	N/A	N/A
11.2	Wirksamkeitsprüfung des ISMS bzw. branchenspezifischen Standards	N/A	N/A

Abbildung 38: Self Assessment Ergebnis Einzelthemen ÖBB-Infrastruktur AG

Als Feedback des Experten II, im Rahmen des Feldexperiments, können folgende zwei Kommentare zitiert werden

Auf die Frage hin, „ob im Rahmen dieses „Self Assessment für NIS-Readiness" technische und organisatorische Auswirkungen aufgezeigt worden sind, die sich auf Basis der NIS-Richtlinie ergeben könnten?“ wurde folgende Antwort gegeben:

> *„Innerhalb des eigenen Unternehmens sind diese technischen und organisatorischen Auswirkungen bereits bewusst gewesen. Wenn sich das Unternehmen jedoch noch nicht intensiv damit befasst hätte, wären durchaus Auswirkungen aufgezeigt worden. Für andere eventuell betroffene Unternehmen könnte dies durchaus der Fall sein.“*

Auf Basis einer anderen Frage „ob die verhältnismäßig intensive Einbindung von Inhalten der ISO 27001 in das Self Assessment ein zielführender Ansatz ist?“ war die persönliche Meinung des Experten II folgende:

> *„In Österreich wird nicht nur die ISO 27001 ausschlaggebend sein. Das heißt, die Nutzung dieser Norm ist sicher hilfreich, aber nicht vollständig bzw. ausschließlich.“*

3.2.4.2 Feldexperiment Raiffeisen Informatik GmbH

Im Sine der Übersichtlichkeit werden hier ebenso nur die relevanten Inhalte des Tabellenblatts „Ergebnisse“ (vgl. Abbildung 39 und Abbildung 40) dargestellt.

Unternehmen:		**Raiffeisen Informatik GmbH**	
Standort:		**Lilienbrunngasse 7-9**	
Assessmentdatum:		**20.04.2018**	
Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad:	**2,85**	**Maximal erreichbar:**	**2,92**

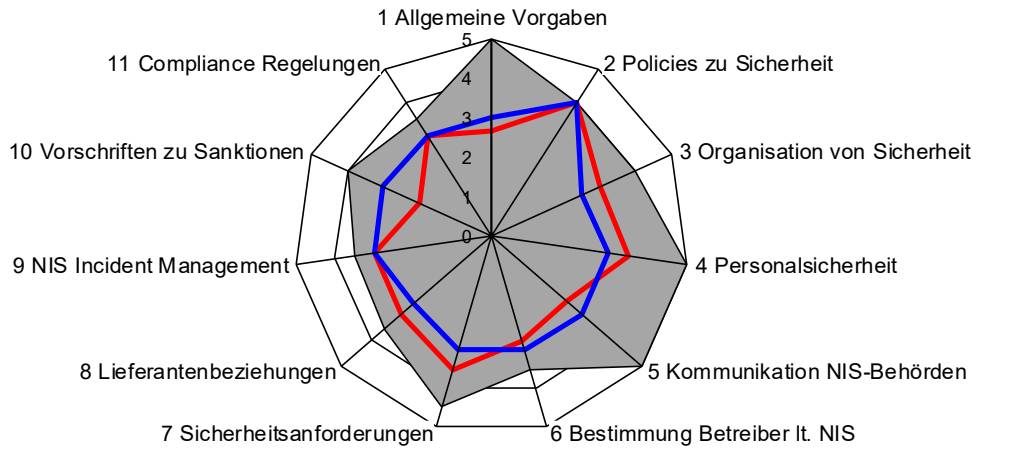


Abbildung 39: Self Assessment Spinnennetzdiagramm Raiffeisen Informatik GmbH

Wie im Spinnennetzdiagramm ersichtlich, erreicht die Raiffeisen Informatik GmbH in den 11 anwendbaren NIS-Themenbereichen die vorgegebenen CMMI Ziel-Reifegrade und würde mit einem Gesamtergebnis von 2,85 als NIS-Ready zu betrachten sein. Auch im Fall einer Anwendung des selbst definierten „NIS-Readiness Wert“, würden die Ziel-Reifegrade der einzelnen Themenbereiche erreicht. Jedoch könnte nicht ausgeschlossen werden, dass eine Verzerrung aufgrund von Überkompensation besteht.

In der detaillierteren Gegenüberstellung (vgl. Abbildung 40) ist erkennbar, dass im spezifischen NIS-Thema 8.4 (Freiwillige Einmeldung von Sicherheitsvorfällen) eine deutliche negative Abweichung gegenüber dem CMMI Ziel-Reifegrad besteht. Hier könnte somit eine gewisse Kritikalität interpretiert werden.

Gesamtergebnis mit Kürzung auf CMMI Ziel-Reifegrad:	2,85	Maximal erreichbar:	2,92

Details:

Spezifisches Ziel Nr.	Themen	CMMI Ziel-Reifegrad	Ergebnis
1.1	Freigabe eines ISMS oder branchenspezifischen Standards	3	5
1.2	Prozess für Risikomanagement bzgl. Informations- bzw. NIS-Sicherheit	3	5
1.3	Wirksamkeit des ISMS oder branchenspezifischen Standards	3	5
2.1	Richtlinie für Informations- bzw. NIS-Sicherheit	4	4
3.1	Verantwortlichkeiten für Informations- bzw. NIS-Sicherheit	3	5
3.2	Definierte Rollen und Verantwortlichkeiten mit IT-Service Providern	2	3
4.1	Vertragsverpflichtung der Mitarbeiter zur Informations- bzw. NIS-Sicherheit	3	5
4.2	Sensibilisierung und Schulung der Mitarbeiter bzgl. Risiken	3	5
5.1	Kommunikationsschiene an nationale zentrale Behörden	3	5
5.2	Kommunikationsschiene von Seiten der nationalen zentralen Behörden	3	5
6.1	Prüfung über Tätigkeiten in kritischen (Teil-)Sektoren	3	5
6.2	Nationale Kriterien bzgl. Betreiber wesentlicher Dienste	3	3
6.3	Prüfung der nationalen "Liste der kritischen Dienste"	3	3
6.4	Erbringung kritischer Dienste in mehreren EU-Mitgliedsstaaten	3	3
7.1	Änderungsmanagement zur Risikobewältigung	3	5
7.2	Angemessene TOM zwecks Verfügbarkeit des kritischen Dienstes	3	4
8.1	Vertragliches Risikomanagement bei Zusammenarbeit mit IT-Dienstleister	2	5
8.2	Überprüfung erbrachter Leistungen von IT-Lieferanten	3	5
8.3	Anlassbezogene Störungsmeldung durch IT-Dienstleister	2	4
8.4	Freiwillige Einmeldung von Sicherheitsvorfällen	3	1
8.5	Trennung von Informationen in gemeinsam genutzten Umgebungen (Cloud)	3	3
9.1	Berichtswesen für Vorfälle bzgl. Informations- bzw. NIS-Sicherheit	3	3
9.2	Bearbeitung von Vorfällen zu Informations- bzw. NIS-Sicherheit	3	4
10.1	Nationale Sanktionen bei Verstößen gegen NIS-Bestimmungen	3	4
11.1	Unabhängige Prüfung des ISMS bzw. branchenspezifischen Standards	3	4
11.2	Wirksamkeitsprüfung des ISMS bzw. branchenspezifischen Standards	3	3

Abbildung 40: Self Assessment Ergebnis Einzelthemen Raiffeisen Informatik GmbH

Als Feedback des Experten V, im Rahmen des Feldexperiments, können folgende drei Kommentare zitiert werden

Auf die Frage hin, „ob im Rahmen dieses „Self Assessment für NIS-Readiness" technische und organisatorische Auswirkungen aufgezeigt worden sind, die sich auf Basis der NIS-Richtlinie ergeben könnten?“ wurde folgende Antwort gegeben:

> *„Aufgrund der Historie des eigenen Unternehmens - im Kontext mit erforderlicher (Informations-)Sicherheit wurden im Self Assessment keine neuen technischen und organisatorischen Auswirkungen aufgezeigt. Wenn dieses tiefgehende historische Wissen im Unternehmen nicht bereits vorhanden wäre, wäre die Antwort ein „Ja“.“*

Auf Basis der Frage, „ob dieses „Self Assessment für NIS-Readiness“ - aus inhaltlicher Sicht - potenziell betroffenen Unternehmen in Österreich eine Hilfestellung bezüglich Umsetzung der NIS-Richtlinie geben kann?“ wurde folgende Antwort gegeben:

> *„Das Self Assessment ist sinnvollerweise im Anschluss (nach Verabschiedung des österreichischen NIS-Gesetzes) noch z.B. um Indicators of Compromise (IOC´s), bzw. Schwellwerte zu ergänzen, dann wäre es optimal.“*

Konkrete fachspezifische Kommentare des Experten V zum Inhalt und Aufbau des „Self Assessment für NIS-Readiness“ haben sich auf nachfolgende Themen bezogen:

- Thema 3.2 („Definierte Rollen mit IT-Service Providern“)
  „*In diesem Zusammenhang wäre es sinnvoll, konkret auf das Vorhandensein bzw. die verfügbaren Service Level Agreements (SLA) in der jeweiligen Organisation einzugehen.*“
- Thema 4.1 („Vertragsverpflichtung Mitarbeiter zur Sicherheit“)
  „*In diesem Kontext wäre es sinnvoll den Begriff "vertraglich" konkreter zu benennen. In diesem Kontext könnte es z.B. eine Dienstanweisung (DA) oder Betriebsvereinbarung (BV) sein.*“
- Thema 6.3 und Thema 6.4 („Prüfung "Liste der kritischen Dienste"“ und „Erbringung kritischer Dienste in mehreren EU-Mitgliedsstaaten“)
  „*Dieses Thema wird in Österreich nach aktuellem Wissensstand nicht relevant sein, da die Bestimmung der "kritischen Dienste" und somit jene der "Betreiber wesentlicher Dienste" (BwD) durch Behördenbescheid erfolgt.*“
- Thema 8.5 („Trennung von Informationen in Clouds“)
  „*In diesem Zusammenhang wäre es sinnvoll, noch konkret auf das derzeit sehr intensiv diskutierte Thema "Datenschutz" einzugehen.*“
- Thema 9.1 („Berichtswesen für Vorfälle“)
  „*WAS zu MELDEN ist wäre fein, gegebenenfalls sollte später ein Link auf die geltenden Vorgaben eingefügt werden, ist aktuell aber nicht bekannt.*
  Als mögliche Orientierungshilfe kann auf Quellen der ENISA verwiesen werden.“
- Thema 11.1 („Unabhängige Prüfung ISMS“)
  „*In diesem Zusammenhang wäre es durchaus sinnvoll gegebenenfalls einen externen Verweis auf den B3S-Standard einzufügen, da dieser nicht so bekannt ist, bzw. eher auch gleich das BSI (BSI - IT-Grundschutz-Kataloge) mit aufnehmen.*“

Vor allem die Hinweise zum Thema 3.2 hinsichtlich der verfügbaren SLA und zum Thema 8.5 mit Bezug zur Thematik des Datenschutzes sind im Kontext dieser Masterarbeit durchwegs von Bedeutung und als wertvolle Anregungen zu verstehen.

3.3 Ergebnisse der Forschung

In diesem Kapitel werden die Ergebnisse der empirischen Arbeit mit den zu Beginn der Masterarbeit gestellten Forschungsfragen (vgl. Kapitel 1.4) und aufgestellten Hypothesen (vgl. Kapitel 1.5) verglichen. Der Vergleich wurde durch die, in diesem Rahmen durchgeführten sechs ExpertInnenbefragungen und zwei Feldexperimente unterstützt.

3.3.1 Beantwortung und Interpretation der Forschungsfragen

Für die Masterarbeit von zentraler Bedeutung war die Beantwortung der Forschungsfrage bzw. der dazugehörigen Zusatzfragen. Im Rahmen der Literaturrecherche und der empirischen Studien wurden diese, in Kapitel 1.4 beschriebenen Fragen, einer spezifischen Beantwortung zugeführt und folgende Erkenntnisse daraus gewonnen.

Um die zentrale **Forschungsfrage F 1** „Welche technischen und organisatorischen Auswirkungen werden sich durch das Inkrafttreten der NIS-Richtlinie auf die betroffenen IT-Service Provider in Österreich sowie „Betreiber wesentlicher Dienste“ ergeben?“ zu beantworten, sind mittels Bearbeitung der folgenden drei Zusatzfragen wesentliche Erkenntnisse erlangt worden, welche abschließend in die Beantwortung eingeflossen sind. Als Quintessenz für F 1 sind dabei die Inhalte des Kapitels 3.2.2 „Self Assessment für NIS-Readiness” zu interpretieren zu interpretieren. Mit in Summe folgenden 11 NIS-Themenbereichen, die 26 spezifische NIS-Themen beinhalten, ist eine umfangreiche Sammlung an technischen und organisatorischen Auswirkungen erstellt worden:

- Allgemeine Vorgaben
- Policies zu NIS und Informationssicherheit
- Organisation von NIS und Informationssicherheit
- Personalsicherheit
- Kommunikation mit zentralen NIS-Behörden
- Bestimmung der Betreiber wesentlicher Dienste
- Sicherheitsanforderungen
- Lieferantenbeziehungen
- Incident Management gemäß NIS-Richtlinie
- Vorschriften zu Sanktionen
- Compliance Regelungen

Daraus abgeleitete TOM´s werden mit Inkrafttreten der NIS-Richtlinie bzw. des nationalen NISG auf die betroffenen IT-Service Provider in Österreich sowie „Betreiber wesentlicher Dienste“ zukommen. Dabei sind Kernelemente der NIS-Richtlinie, des deutschen IT-SiG und der Normen ISO 27001 sowie ISO 27017 in die Betrachtung eingeflossen. Auf diese Weise soll so weit wie möglich sichergestellt werden, dass angemessene Maßnahmen getroffen werden können die dem jeweiligen „Stand der Technik“ entsprechen.

Die Mehrheit der befragten ExpertInnen bejahte die Frage, dass im Rahmen des selbstentwickelten Prototyps „Self Assessment für NIS-Readiness" technische und organisatorische Auswirkungen aufgezeigt worden sind, die sich auf Basis der NIS-Richtlinie ergeben könnten. Es wurde jedoch eine Abhängigkeit davon gesehen, wie stark das jeweilige Unternehmen zu dem Zeitpunkt bereits in die Materie vertieft ist (vgl. Kapitel 3.2.3.1). Einschränkend auf Österreich sei hierbei noch festgehalten, dass mehrere ExpertInnen im Rahmen des gemeinsamen Termins anmerkten, dass es in Österreich zum Zeitpunkt noch keine gesetzlichen Vorgaben /z.B. NISG) gegeben hat und somit noch ein gewisser Unsicherheitsfaktor existiert.

Die **Zusatzfrage Z 1** befasst sich mit „Sind aus dem bestehenden deutschen IT-Sicherheitsgesetz Erkenntnisse für das noch ausstehende österreichische NISG zu gewinnen?“

Wie ausführlich im Kapitel 2.5 erklärt und bewertet, lassen sich durchaus spezifische Erkenntnisse für Österreich gewinnen. Im Rahmen der Literaturrecherche und der durchgeführten Vergleiche von Österreich und Deutschland sind Themen aufgezeigt worden, welche in das zukünftige österreichische NISG einfließen könnten. Im Wesentlichen könnte sich Österreich bei der Ausgestaltung des NISG an folgenden Inhalten der relevanten Gesetze in Deutschland orientieren:

- definierte Schwellenwerte (jedoch auf Österreich modifiziert)
- Möglichkeit von branchenspezifischen Sicherheitsstandards
- Sanktionierung und Bußgelder (jedoch auf Österreich modifiziert)
- Klassifikation von IT-Sicherheitsvorfällen
- Vorgaben betreffend Sicherheitsanforderungen („Stand der Technik“)

Andere Themen werden für den Standort Österreich als nicht praktikabel betrachtet und dementsprechend zurück gereiht:

- Bestimmung der BwD (Österreich hat im Rahmen von APCIP ein eigenes funktionierendes Modell entwickelt und verprobt)
- Meldepflichten (da Österreich dezentral und Deutschland zentral organisiert ist)
- Definierte Schutzziele (Österreich sollte in diesem Zusammenhang höhere Mindestanforderungen, als in der NIS-Richtlinie oder IT-SiG definiert, einführen)

Wie das österreichische NISG schlussendlich inhaltlich ausgestaltet sein wird, sollte sich zeitnah herauskristallisieren, da es faktisch ab 10.5.2018 als nationales Recht umgesetzt hätte sein sollen.

Die **Zusatzfrage Z 2** lautet „Welche Steuerungsmaßnahmen sind in Unternehmen zu etablieren, damit entsprechende Verantwortlichkeiten auch an externe IT-Service Provider in Österreich übertragen werden können?“

Abgeleitet aus den Ergebnissen der Kapitel 2.4.4 und 2.5.3 lässt sich die Antwort soweit zusammenfassen, dass umfängliche Verantwortlichkeiten vom BwD nicht an externe IT-SP übertragen werden können. Wie in der NIS-Richtlinie ausformuliert, sollten BwD die Sicherheit der von ihnen verwendeten NIS gewährleisten. Ob diese Netz- und Informationssysteme von internem IT-Personal betreut werden oder die Sicherreit Dritten übertragen wurde, ist nahezu unerheblich. Die relevanten Meldepflichten und Sicherheitsanforderungen sollten für die BwD unabhängig davon gelten, welche der beiden Varianten (In- oder Outsourcing) umgesetzt wird.

Es könnte sich der BwD als wirksame Steuerungsmaßnahme nach einem spezifischen Managementsystem ausrichten (z.B. ISO 27001) und sich in weiterer Folge einer entsprechenden Unternehmenszertifizierung unterziehen. Es ist dabei üblicherweise gängige Praxis, dass in diesem Rahmen auch relevante Themen wie z.B. Lieferantenbeziehungen, Handhabung von Informationssicherheitsvorfällen eine zentrale Rolle einnehmen.

Alternativ sind vertragliche Vereinbarungen hinsichtlich der Durchführung von externen Audits beim leistungserbringenden Dritten (z.B. IT-SP) ein zielführendes Instrument, welches in manchen Bereichen bereits heute branchenüblich ist.

Im IT-Kontext ist es zudem ein etablierter Ansatz, die Leistungserbringung durch Dritte (z.B. externe IT-Service Provider) im Rahmen von SLA´s vertraglich zu vereinbaren und weiters einer zweckmäßigen Steuerung zu unterziehen (vgl. Kapitel 3.2.2.3). Für IT-SP wird dies auch zukünftig in potenziellen Verträgen, bzw. in den Verhandlungen mit den BwD zu berücksichtigen sein.

Eine klare Mehrheit der ExpertInnen hat mit „Ja" auf die Frage geantwortet, ob dieses „Self Assessment für NIS-Readiness" - aus inhaltlicher Sicht - potenziell betroffenen Unternehmen in Österreich eine Hilfestellung bezüglich Umsetzung der NIS-Richtlinie geben kann (vgl. Kapitel 3.2.3.1).

Jedoch ist darauf hinzuweisen, dass nach aktuellem Wissensstand die letztgültige Verantwortung nur beim BwD verbleiben kann.

Zusatzfrage Z 3 behandelt das Thema „Wie können IT-Service Provider und „Betreiber wesentlicher Dienste" in Österreich die aus der NIS-Richtlinie entstehenden relevanten Themen ableiten und sicherstellen, dass NIS-Vorgaben auch eingehalten werden?"

Der relevante Themenkreis zur NIS-Richtlinie ist, wie in dieser Masterarbeit dargestellt, sehr umfangreich und komplex. Erst mit Berücksichtigung des dokumentieren Wissens war es möglich, eine praktikable Hilfestellung in Form eines Self Assessments zu entwickeln. Darin enthalten sind die identifizierten TOM´s. Zusätzlich lassen sich daraus ebenfalls relevante Themen ableiten um sicherzustellen, dass NIS-Vorgaben auch laufend auf Einhaltung geprüft werden können (vgl. Kapitel 3.2.2.3).

Ein Self Assessment im Allgemeinen und der hier entwickelte Prototyp des „Self Assessment für NIS-Readiness" im Speziellen, kann als unterstützendes Werkzeug angesehen werden. Eine Mehrheit der befragten sechs ExpertInnen war im Rahmen der Befragung der Meinung, dass ein „Self Assessment für NIS-Readiness" hilfreich wäre, um eventuell identifizierte Maßnahmen einer möglichen Behandlung zuzuführen (vgl. Kapitel 3.2.3.2). Ebenso ist in der empirischen Studie festgestellt worden, dass die Mehrheit der ExpertInnen mit „Ja" oder „eher Ja" auf die Frage antworteten, ob ein „Self Assessment für NIS-Readiness" zur initialen Bewertung der Vorgaben aus der NIS-Richtlinie ein zweckmäßiges Mittel wäre (vgl. Kapitel 3.2.3.2). Eine verhältnismäßig eindeutige Zustimmung gab es hinsichtlich der Zweckmäßigkeit einer Bewertung der NIS-Readiness auf Basis des angewendeten Reifegradmodells nach CMMI (vgl. Kapitel 3.2.3.2)

Die klare Mehrheit der ExpertInnen vertritt mit „Ja" die Meinung, dass bereits ISO 27001 zertifizierte Unternehmen einen Vorsprung bezüglich der nötigen TOM´s im Rahmen der Umsetzung der NIS-Richtlinie haben werden (vgl. Kapitel 3.2.3.3). Eine bereits erfolgte Ausrichtung an ein etabliertes Managementsystem wird also in weiten Teilen als vorteilhaft angesehen. Vor allem vor dem Hintergrund, dass die ISO 27001 als Managementsystem auch Korrekturmaßnahmen oder eine fortlaufende Verbesserung einfordert.

3.3.2 Verifikation der Hypothesen

Auf Basis der durchgeführten Literaturrecherche und der empirischen Studien werden nachfolgend die in Kapitel 1.5 aufgestellten Hypothesen beschrieben und verifiziert bzw. falsifiziert.

In diesem Zusammenhang war bzgl. der empirischen Ergebnisse die in Kapitel 3.2.1 festgehaltene Thematik zu berücksichtigen, dass die befragten ExpertInnen ein tiefergehendes Verständnis und gesteigertes Bewusstsein für die Themen hinsichtlich der NIS-Richtlinie hatten. Somit könnten die hier erzielten Ergebnisse eine überdurchschnittliche Wertung haben, die im Vergleich zu anderen durchschnittlichen Unternehmen, die potenziell von der NIS-Richtlinie betroffen sein könnten, anders ausfallen würden.

In der **Hypothese H 1** ist die Annahme getroffen worden, dass die „Betreiber wesentlicher Dienste“ die Möglichkeit haben sollen, die Verantwortung auch an externe IT-Service Provider zu übertragen. Wie anhand der erarbeiteten Ergebnisse (vgl. Kapitel 2.4.4 und 2.5.4) dargestellt, kann die letztgültige Verantwortung nicht vom „Betreiber wesentlicher Dienste“ an mögliche Dritte übertragen werden. Eine gewisse Absicherung des BwD könnte dabei vornehmlich auf Basis von vertraglichen Regelungen wie z.B. durch SLA´s erfolgen. Diese Hypothese kann in diesem Sinne nicht bestätigt werden und ist zum jetzigen Zeitpunkt mit den heutigen Informationen falsifiziert.

Die **Hypothese H 2** lautete, dass es für Österreich ratsam wäre, sich bei ausgewählten Fragestellungen (z.B. sektorale Schwellenwerte, Sanktionen, Meldestruktur) zum NISG an bereits bestehenden Gesetzestexten aus Deutschland zu orientieren. Auf Basis des Naheverhältnisses der beiden Länder, wurden in Kapitel 2.5 verschiedene Aspekte aufgezeigt und erarbeitet die bestätigen, dass für spezifische Themenbereiche der NIS-Richtlinie eine Ausrichtung an Deutschland (für etablierte Vorgaben) ratsam wäre. Die Hypothese H 2 kann in diesem Sinne als bestätigt angesehen werden und ist somit zum jetzigen Zeitpunkt verifiziert.

Die **Hypothese H 3** beinhaltet die Annahme, dass „Betreiber wesentlicher Dienste“ und IT-Service Provider die schon auf Basis der ISO 27001 zertifiziert sind, bezüglich der Anforderungen aus der NIS-Richtlinie bereits viel Vorarbeit geleistet hätten. Im Rahmen der empirischen Studien wurde dies im Wesentlichen bestätigt. Wie in Kapitel 3.2.3.3 festgehalten, sind fünf von sechs ExpertInnen dieser Meinung. Ebenso wurde in Kapitel 2.4.4 und 2.5.3 der Querbezug zum Modell in Deutschland hergestellt, wo eine klare Empfehlung zugunsten der ISO 27001 formuliert ist. Die Hypothese ist somit, mit dem heutigen Kenntnisstand, verifiziert.

Im Rahmen der **Hypothese H 4** wurde angenommen, dass ein „Self Assessment für NIS-Readiness” von potenziell betroffenen Unternehmen zur Bewertung und Einschätzung als positiv angesehen werden kann. Alle für diese Hypothese dazu erhaltenen Rückmeldungen (zu relevanten Fragen) waren in diesem Kontext mit „Ja“ oder „eher Ja“ positiv. Dabei könnten in einem zukünftigen Schritt noch Themen wie die Extrahierung eines Maßnahmenkatalogs je Fachbereich oder eine Risikobewertung berücksichtigt

werden. Die Rückmeldungen der ExpertInnen (vgl. Kapitel 3.2.3.1 und 3.2.3.2) haben mehrheitlich diese Hypothese bestätigt.

Die **Hypothese H 5** befasste sich mit dem Thema, dass im Zuge eines strukturierten „Self Assessment für NIS-Readiness" technische und organisatorische Aspekte, die sich aus der NIS-Richtlinie ergeben, aufgezeigt und so einer möglichen Behandlung zugeführt werden können. Von Seiten der ExpertInnen (vgl. Kapitel 3.2.3.1 oder 3.2.4.1 oder 3.2.4.2) wurde diese Hypothese mit gewissen Einschränkungen bestätigt. Insgesamt waren vier von sechs erhaltenen Rückmeldungen zu dieser Hypothese mit „Ja" oder „eher Ja" bewertet, wobei ein „eher Nein" Expertenkommentar besagte „*TOM's sollten besser ausspezifiziert werden*". In den beiden Feldexperimenten wurde darauf verwiesen, dass aufgrund des unternehmenseigenen hohen Bewusstseins die aufgezeigten TOM´s weitestgehend bekannt waren. Es wurde jedoch von den ExpertInnen die Meinung geäußert, dass für andere, potenziell betroffene Unternehmen durchaus technische und organisatorische Aspekte aufgezeigt werden können. Wenngleich es abhängig davon sein wird, wie intensiv die Unternehmen bereits mit der Materie in Berührung gekommen sind, ist die Hypothese H5 mit heutigem Wissen im Wesentlichen bestätigt

Die finale **Hypothese H 6** basierte auf der Annahme, dass eine Bewertung der NIS-Readiness anhand eines Reifegradmodells hinsichtlich einer objektiven Bewertung als zweckmäßig angesehen werden kann. Die Meinung der ExpertInnen (vgl. Kapitel 3.2.3.2) ging mehrheitlich (fünf von sechs) in die Richtung, dass dies mit „Ja" oder „eher Ja" der Fall sein wird. Die eine „eher Nein"-Meinung des Experten verwies darauf, dass es eher für Unternehmen hilfreich sein wird die noch keine eigene Bewertung aus Unternehmenssicht haben werden. In diesem Sinne konnte die gegenständliche Hypothese aus heutiger Sicht mehrheitlich bestätigt werden.

4. Conclusio

In diesem finalen Kapitel werden gewonnene Ergebnisse und Erkenntnisse zusammengefasst, kritisch bewertet, und ein Ausblick auf mögliche, zukünftige Aktivitäten gegeben.

„*Erfahrung ist der Anfang aller Kunst und jedes Wissens.*“
(Aristoteles, 384 v.Chr. - 322 v.Chr.)

4.1 Ergebnisse und Fazit

Wie im ersten Kapitel der Masterarbeit festgehalten, soll mittels der NIS-Richtlinie die Möglichkeit geschaffen werden, die Gefahr und das Schadensausmaß von Cybervorfällen, wie etwa Cyberkriminalität und staatlich unterstützte böswillige Cyberaktivitäten, einzudämmen. Zu diesem Zweck scheint die aktuelle NIS-Richtlinie ein erster zweckmäßiger Schritt für den Anwendungsbereich innerhalb der EU zu sein. So werden auf nationaler Ebene Cybersicherheitskapazitäten gestärkt, die Mitgliedstaaten zur tiefergehenden Zusammenarbeit aufgefordert, relevante Branchen adressiert und schwere Sicherheitsvorfälle einer Meldeverpflichtung unterworfen.

Ein vollständiges Ausschließen dieser unerwünschten Cyberaktivitäten kann durch die NIS-Richtlinie nicht erzielt werden. Jedoch ist der Auftrag dieser Richtlinie den Schutz von kritischen Infrastrukturen und kritischen Dienstleistungen zu gewährleisten.

Mitte 2017 zu Beginn der Masterarbeit war die NIS-Richtlinie knapp ein Jahr zuvor in Kraft getreten. Aufgrund der darin enthaltenen Fristen zur nationalen Umsetzung und der Komplexität der gegenständlichen Materie, war zu dem Zeitpunkt die eigene Annahme, dass im Fall von Österreich bereits 2017 ein NISG begutachtet oder sogar verabschiedet werden würde. Ob nun den politischen Gegebenheiten, möglichen Interessenskonflikten oder einfach dem Themenkomplex geschuldet, so hat sich diese Annahme als Irrglaube erwiesen. Auch wenn es positiv zu werten ist, dass andere Themen wie beispielsweise die DSGVO oder das Sicherheitspaket so medienwirksam und politisch aktiv behandelt wurden, so sollte in Österreich auch das NISG zeitnah mit dem erforderlichen Nachdruck behandelt werden.

Ein Inkrafttreten des nationalen NISG in Österreich ist mit Abgabe dieser Masterarbeit noch nicht erfolgt, wobei gemäß NIS-Richtlinie bis zum 9. Mai 2018 entsprechende Rechts- und Verwaltungsvorschriften zu erlassen gewesen wären. Damit geht Österreich das Risiko ein, dass eine Sanktion durch die EU folgen kann, und dass sich die Unternehmen nicht an konkreten Vorgaben orientieren können. Für die potenziell betroffenen Unternehmen in Österreich stellt dieser Umstand einen gewissen Unsicherheitsfaktor dar, da vor allem zentrale Kernelemente (z.B. Schwellenwerte) nicht umfänglich bekannt sind und dies in einem potenziell auftretenden Notfall entsprechend, kurzfristige Maßnahmen erfordern könnte.

Die im Rahmen dieser Masterarbeit in Kapitel 1.4 gestellten Forschungsfragen und die aufgestellten Hypothesen (vgl. Kapitel 1.5), konnten auf Basis wissenschaftlicher Methoden im vorangegangenen Kapitel 3.3 ausreichend beantwortet werden.

Die Auswirkungen, welche sich aufgrund der NIS-Richtlinie bzw. eines zukünftigen NISG in Österreich auf die betroffenen IT-Service Provider sowie „Betreiber wesentlicher Dienste“ ergeben werden, werden umfangreich und komplex sein. Das hat sich dadurch gezeigt, dass es nötig war einige Querbezüge zu anderen (inter-)nationalen Vorschriften, Normen und Standards herzustellen. Die so aufbereiteten 26 spezifischen NIS-Themen bilden damit ein solides Fundament.

Mit dem daraus entwickelten „Self Assessment für NIS-Readiness“ haben die Unternehmen ein Hilfsmittel um sich initial selbst einzuschätzen, aber auch eine Steuerung, um eventuell erforderliche Maßnahmen durchzuführen. Denn eine abschließende Verantwortung muss, aus Sicht der NIS-Richtlinie, immer beim BwD verbleiben und kann nicht Dritten überbunden werden. Unter diesem Gesichtspunkt kann eine weiterführende Ausrichtung an etablierte Managementsysteme, wie z.B. ISO 27001 sowohl für BwD wie auch für IT-SP, als gewisser Vorteil angesehen werden.

Auch wenn sich die Rahmenbedingungen der Standorte Österreich und Deutschland in einigen Bereichen unterscheiden, so könnte die österreichische Gesetzgebung durchaus in einigen Aspekten Anleihe, bei den bereits verabschiedeten deutschen NIS-relevanten Gesetzen, nehmen.

Die durchgeführten ExpertInnengespräche im Rahmen der Präsentation des „Self Assessment für NIS-Readiness“ waren äußerst aufschlussreich. Die Ergebnisse der Befragung haben dabei zu kritischen Überlegungen geführt.

In der Prototypentwicklung des „Self Assessment für NIS-Readiness“ gab es Unsicherheiten zur Thematik hinsichtlich Methodik, Ausgestaltung und Inhalt. Die vorausgehende Literaturrecherche konnte zwar viele Elemente aufzeigen und interpretierbar machen, jedoch sind viele inhaltliche Aspekte der NIS-Richtlinie vage gehalten und weisen mehr Empfehlungs- als Vorgabecharakter auf. Bei den teilnehmenden ExpertInnen ist das Self Assessments im Rahmen der Präsentation durchwegs gut aufgenommen worden und die positive Resonanz hat die anfänglichen Unsicherheiten zerstreut. Besonders beeindruckend war die gebündelte Fachkompetenz bei den ExpertInnen rund um das Thema der NIS-Richtlinie und den daraus resultierenden Auswirkungen. Die Bereitschaft Auskünfte zu geben und relevante Informationen zu teilen, war für diese Masterarbeit äußerst hilfreich.

Die durchgeführten Feldexperimente haben die Expertise der teilnehmenden ExpertInnen noch weiter bekräftigt. Innerhalb des gegebenen Rahmens und der verfügbaren Zeit sich thematisch so rasch in die Materie einzulesen und auskunftsfähig zu sein, war beeindruckend. Die Anwendbarkeit des selbstentwickelten Prototyps „Self Assessment für NIS-Readiness“ und somit die Praxistauglichkeit wurde in diesem Rahmen von den mitwirkenden ExpertInnen bestätigt.

Mit diesem „Self Assessment für NIS-Readiness“ wurde eine Möglichkeit geschaffen, potenziell betroffenen Unternehmen in Österreich die Auswirkungen der NIS-Richtlinie (auf technischer und organisatorischer Ebene) aufzuzeigen, sowie eine Hilfestellung bei deren Maßnahmensteuerung zu geben.

4.2 Methoden

Die in der Masterarbeit angewendeten wissenschaftlichen Methoden waren für die angestrebten Ziele zweckmäßig, damit entsprechende Ergebnisse für die Forschungsfragen und Hypothesen erarbeitet werden konnten.

Durch die Literaturrecherche konnte ein breites Fundament geschaffen werden, auf dessen Basis die weiteren Aktivitäten entwickelt werden konnten. Die bearbeiteten Richtlinien, Gesetze, Whitepapers, Studien, uvm. finden sich sowohl als Resultate und Ergebnisdokumente in der Masterarbeit wieder und haben den Ablauf der ExpertInnengespräche konstruktiv beeinflusst.

Ein Hauptgrund den Prototyping Ansatz zu wählen war, dass der gestaltungorientierte Ansatz des „Self Assessment für NIS-Readiness“ konkrete Ergebnisse brachte und die Thematik damit einfacher interpretierbar wurde. So wurde das abstrakt wirkende Thema rund um die NIS-Richtlinie, sowohl für mich wie auch für die ExpertInnen, konkreter und greifbarer. Eine Bewertung war damit leichter und nachvollziehbarer.

Die ExpertInnenbefragungen als qualitative Querschnittanalysen waren durchwegs aufschlussreich und haben neue Denkanstöße gegeben. Die Ermittlung entsprechender ExpertInnen half dabei, wesentliche Erkenntnisse schon im Vorfeld zu gewinnen. Ebenso würden einige der (in-)offiziellen Kommentare Potenzial für weiterführende wissenschaftliche Arbeiten bieten.

Die durchgeführten Feldexperimente haben gezeigt, dass potenzielle BwD und IT-SP thematisch einen Nutzen daraus ziehen könnten. Je nachdem wie intensiv sich das jeweilige Unternehmen bereits mit der Materie beschäftigt hat, ist das Spektrum des „Nutzens“ entsprechend hoch. Die Durchführung verlief dabei unkomplizierter als erwartet, was dabei weitestgehend den ExpertInnen zu verdanken war. Eine Verprobung als Feldexperiment mit inhaltlicher Bewertung des dokumentierten Wissens (z.B. Richtlinien, Prozesse), wäre äußerst interessant gewesen. Zu diesem Zweck hätten jedoch eine Vielzahl mehr an Dokumenten betrachtet werden müssen. Dazu kann festgehalten werden, dass spezifische Dokumente in den Unternehmen weitestgehend einem hohen Schutzbedarf unterliegen und deshalb keine Einsicht zugelassen wurde.

4.3 Ausblick

Da die NIS-Richtlinie – dem Charakter einer EU-Richtlinie entsprechend - in der vorliegenden Fassung in einigen Teilen äußerst vage gehalten ist, werden potenzielle (in-)direkt betroffene Unternehmen zeitnah Maßnahmen ergreifen müssen. Die in dieser Masterarbeit gewonnenen Erkenntnisse und Ergebnisse stellen eine fundierte Basis dar,

um Unternehmen in Österreich im Zusammenhang mit der NIS-Richtlinie eine Hilfestellung bieten zu können. Vor allem durch die Berücksichtigung internationaler Normen und Standards wie etwa ISO 27001 oder BSI IT-Grundschutz-Kataloge ist ein umfangreicher themenspezifischer Bereich abgedeckt worden. Mögliche Weiterentwicklungen von IT-Frameworks, -Standards oder -Normen sollten dabei auch weiterhin verfolgt und berücksichtigt werden, da diese oftmals den relevanten „Stand der Technik" behandeln bzw. repräsentieren, welcher auch in der NIS-Richtlinie ein zentrales Element ist.

Mit dem als Prototypen selbst entwickelten „Self Assessment für NIS-Readiness" ist ein standardisiertes und verhältnismäßig klar strukturiertes Werkzeug geschaffen worden. Mittels der darin erfassten Inhalte können relevante technische und organisatorische Maßnahmen aufgezeigt, sowie einer möglichen Bearbeitung zugeführt werden. Aufgrund des Umstandes, dass in Österreich das spezifische NISG im Betrachtungszeitraum der Masterarbeit noch ausstehend war, wäre zu gegebener Zeit (sobald die NISG umgesetzt wurde) eine Revision des „Self Assessment für NIS-Readiness" zweckmäßig. Wie in den ExpertInnenrückmeldungen oftmals angemerkt wurde, sind doch einige wesentliche Elemente erst mit der nationalen Gesetzgebung konkret ableitbar.

In Hinsicht auf die Kommentare der ExpertInnen könnten folgend einige inhaltlich und methodisch interessante Aspekte in das „Self Assessment für NIS-Readiness" integriert werden:

- Extraktion eines gesamtheitlichen Maßnahmenkatalogs für die Fachbereiche auf Basis der befüllten „NIS-Anforderungen"
- Betrachtung der Reifegrade als Risikowerte
- Spezifizierung des „Gesamtergebnis CMMI Ziel-Reifegrads" mit zwingender Berücksichtigung der entsprechenden NIS-Detailergebnisse
- Implementierung eines Trendverlaufs für tourliche Assessments

Der Prototyp des Self Assessments in Form eines Tabellenkalkulationsprogramms kann dabei als konservativ betrachtet werden. Eine Weiterentwicklung in Form einer online Ressource beispielsweise als eigene Website oder eingebettetem Webformular könnte die Bereitstellung und Nutzung zukünftig erleichtern. Dabei sollte bedacht werden, dass im Falle eines seriösen Self Assessment vom ausführenden Unternehmen vertrauliche und sensible Daten preisgegeben werden. Dementsprechend wären IT-Sicherheitsmaßnahmen zu implementieren, um Schaden in Form von Datenschutzverletzungen abzuwehren.

Eine zukünftige, reale Verprobung des „Self Assessment für NIS-Readiness", bei einem potenziellen BwD auf Basis des tatsächlichen österreichischen NISG wäre ein wünschenswertes Ziel bzw. krönender Abschluss dieser Masterarbeit!

„*Wichtig ist, dass man nicht aufhört zu fragen.*"
(Albert Einstein, 1879 - 1955)

Literaturverzeichnis

Adelmeyer, Michael, Christopher Petrick und Frank Teuteberg. 2017. IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes. Wiesbaden, Deutschland: Springer Fachmedien.

Allianz Global Corporate & Specialty SE. 2017. Allianz Risk Barometer - Die 10 wichtigsten Geschäftsrisiken 2017. München, Deutschland.

Amt für Veröffentlichungen der Europäischen Union. 2010. Strategie für die innere Sicherheit der Europäischen Union: Auf dem Weg zu einem europäischen Sicherheitsmodell. Luxemburg.

Amtsblatt der Europäischen Union. 2008. RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

Amtsblatt der Europäischen Union. 2016. RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

A-SIT Plus GmbH. 2017. Cloud Computing - Eine Orientierungshilfe für Cloud-Service-Kunden. Wien, Österreich: A-SIT Plus GmbH.

A-SIT Zentrum für sichere Informationstechnologie – Austria. 2017. *ISO/IEC 27001 - Anforderungen an Informationssicherheits-Managementsysteme*. Abgerufen am 10. Mai 2018 von https://onlinesicherheit.gv.at/experteninformation/normen_und_standards/iso-iec_27000/71520.html

Atug, Manuel, Kai Mettke-Pick und Dennis Pohl. 2017. *Erweiterte Sicherheitszone*. Von https://heise.de/ix/heft/Erweiterte-Sicherheitszone-3754488.html

Bartsch, Michael und Stefanie Frey. 2017. Cyberstrategien für Unternehmen und Behörden - Maßnahmen zur Erhöhung der Cyberresilienz. Wiesbaden, Deutschland: Springer Verlag.

Bedner, Mark und Tobias Ackermann. 2010. Schutzziele der IT-Sicherheit. DuD • Datenschutz und Datensicherheit.

Black Hat. 2017. *The 2017 Black Hat Europe Survey - The Cyberthreat in Europe.* Abgerufen am 12. März 2018 von https://blackhat.com/docs/eu-17/Black-Hat-Attendee-Survey.pdf

BSI Group. s.a.. ISO/IEC 27017 - Extending ISO/IEC 27001 into the Cloud. BSI Group.

Buber, Renate und Hartmut Holzmüller. 2007. *Qualitative Marktforschung.* Wiesbaden: Gabler Verlag.

Bundesamt für Sicherheit in der Informationstechnik. 2016. *Branchenspezifische Sicherheitsstandards.* Abgerufen am 12. Mai 2018 von https://bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/B3S/b3s_node.html

Bundesamt für Sicherheit in der Informationstechnik. 2016. *Meldepflicht*. Abgerufen am 10. Mai 2018 von https://bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht.html

Bundesamt für Sicherheit in der Informationstechnik. 2017a. *Gesetz zur Umsetzung der NIS-Richtlinie - Mehr Aufgaben und Befugnisse für das BSI.* Abgerufen am 12. Mai 2018 von https://bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS-Richtlinie.html

Bundesamt für Sicherheit in der Informationstechnik. 2017b. Die Lage der IT-Sicherheit in Deutschland 2017. Bonn, Deutschland: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. 2017c. Anforderungskatalog Cloud Computing (C5). Bonn, Deutschland: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. 2017d. Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG. Bonn, Deutschland: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. 2018. *"Stand der Technik" umsetzen.* Abgerufen am 10. Mai 2018 von https://bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/stand_der_technik.html

Bundesamt für Sicherheit in der Informationstechnik. s.a.. Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz. Bundesamt für Sicherheit in der Informationstechnik.

Bundesgesetzblatt. 2015. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. Bonn: Bundesanzeiger Verlag.

Bundeskanzleramt Österreich. 2015. Österreichisches Programm zum Schutz kritischer Infrastrukturen. Wien, Österreich: Bundeskanzleramt Österreich.

Bundeskanzleramt Österreich. 2016. Schutz kritischer Infrastrukturen APCIP. Österreich.

Bundeskanzleramt Österreich. 2017. Bundesgesetz über die Grundsätze der Deregulierung (Deregulierungsgrundsätzegesetz). Wien, Österreich: Bundeskanzleramt Österreich.

Bundeskanzleramt Österreich. s.a.. Österreichische Strategie für Cyber Sicherheit (ÖSCS) - Umsetzungsbericht 2015. Österreich: Bundeskanzleramt Österreich.

Bundesministerium der Justiz. 2008. Bekanntmachung des Handbuchs der Rechtsförmlichkeit. Köln, Deutschland: Bundesanzeiger Verlagsges.mbH.

Bundesministerium der Justiz und für Verbraucherschutz. 2017. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG). Deutschland: Bundesministerium der Justiz und für Verbraucherschutz.

Bundesministerium des Innern. 2011. Cyber-Sicherheitsstrategie für Deutschland. Berlin, Deutschland: Bundesministerium des Innern.

Bundesministerium des Innern. (2016). Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin: Bundesministerium des Innern.

Bundesministerium für Inneres. 2017. MEHR FREIHEIT.MEHR SICHERHEIT. Sicherheitsdoktrin des BMI für Österreich 2017 - 2020. Wien, Wien, Österreich: Bundesministerium für Inneres.

Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz. 2018. Regierungsvorlage - Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert

werden (Strafprozessrechtsänderungsgesetz 2018). Wien, Österreich: Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz.

CERT.at. 2017. BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2016. Wien, Österreich: nic.at GmbH, Computer Emergency Response Team Austria.

CERT.at. 2018. *Austrian Energy CERT*. Abgerufen am 2. Mai 2018 von https://cert.at/about/aec/content.html

CMMI Product Team. 2010a. CMMI® for Acquisition, Version 1.3. Carnegie Mellon University.

CMMI Product Team. 2010b. CMMI® for Services, Version 1.3. Carnegie Mellon University.

CMMI Product Team. 2011. CMMI® für Entwicklung, Version 1.3 (TECHNICAL REPORT). Carnegie Mellon University.

Council of the EU. 2017. EU stärkt die Cybersicherheit. Brüssel, Belgien: General Secretariat of the Council.

Cyber Security Austria. 2012. *Innenministerium plant IT-Sicherheitsgesetz*. Abgerufen am 2. Mai 2018 von https://www.cybersecurityaustria.at/index.php/blog/2012/86-deu-innenministerium-plant-it-sicherheitsgesetz

Cybersecurity Ventures. 2017. 2017 Cybercrime Report. Kalifornien, USA: Cybersecurity Ventures.

DIN-Normenausschuss Informationstechnik und Anwendungen. 2015. DIN ISO/IEC 27001:2013. DIN-Normenausschuss Informationstechnik und Anwendungen.

E-Control. 2014. Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft. E-Control.

ENISA. 2015. Definition of Cybersecurity - Gaps and overlaps in standardisation. Athen, Griechenland: European Union Agency for Network and Information Security.

ENISA. 2016a. Stocktaking, Analysis and Recommendations on the Protection of CIIs. Athen, Griechenland: ENISA.

ENISA. 2016b. Strategies for Incident Response and Cyber Crisis Cooperation. Athen, Griechenland: European Union Agency For Network And Information Security.

ENISA. 2016c. NCSS Good Practice Guide - Designing and Implementing National Cyber Security Strategies. Athen, Griechenland: European Union Agency For Network And Information Security.

ENISA. 2017a. Incident notification for DSPs in the context of the NIS Directive. Athen, Griechenland: ENISA.

ENISA. 2017b. *WannaCry Ransomware Outburst*. Abgerufen am 2. Mai 2018 von https://enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

ENISA. 2018. ENISA Threat Landscape Report 2017 - 15 Top Cyber-Threats and Trends. Athen, Griechenland: European Union Agency for Network and Information Security.

EUROPÄISCHE KOMMISSION. 2013. Cybersicherheitsstrategie der Europäischen Union - ein offener, sicherer und geschützter Cyberraum .

EUROPÄISCHE KOMMISSION. 2015a. Digitaler Binnenmarkt – Länderinformationen DE. EUROPÄISCHE KOMMISSION.

EUROPÄISCHE KOMMISSION. 2015b. Digitaler Binnenmarkt – Länderinformationen AT. EUROPÄISCHE KOMMISSION.

EUROPÄISCHE KOMMISSION. 2015c. Die Europäische Sicherheitsagenda.

EUROPÄISCHE KOMMISSION. 2017. Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen. Brüssel, Belgien: EUROPÄISCHE KOMMISSION.

EUROPÄISCHE KOMMISSION. 2017. Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. Brüssel, Belgien: EUROPÄISCHE KOMMISSION.

EUROPÄISCHE KOMMISSION. s.a.. *Policies about Cybersecurity*. Abgerufen am 7. Mai 2018 von https://ec.europa.eu/digital-single-market/en/policies/75984/3587

European Union. 2016. Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa. European Union.

Felser, Rudolf. 2015. *Österreich: Neuer Vorstoß in Richtung Vorratsdatenspeicherung*. Abgerufen am 12. Mai 2018 von https://computerwelt.at/news/osterreich-neuer-vorstos-in-richtung-vorratsdatenspeicherung/

Grobauer, Bernd, Peter Kossakowski und Thomas Schreck. 2016. *DuD • Datenschutz und Datensicherheit - Klassifikation von IT-Sicherheitsvorfällen.* Wiesbaden: Springer Verlag.

Heinrich, Lutz Jürgen, Armin Heinzl und René Riedl. 2011. *Wirtschaftsinformatik: Einführung und Grundlegung. 4. Auflage.* Berlin Heidelberg: Springer Verlag.

Kipker, Dennis-Kenji. 2016. Die NIS-RL der EU im Vergleich zum deutschen IT-Sicherheitsgesetz. ZD FOKUS.

Kipker, Dennis-Kenji. 2017. Der BMI-Referentenentwurf zur Umsetzung der NIS-RL. München, Deutschland: Verlag C. H. Beck.

KIRAS Sicherheitsforschung. 2017. *GENESIS - Guideline für Behörden und KMU-Anbieter strategischer Services zur risiko-orientierten Implementierung der NIS-Richtlinie*. Abgerufen am 12. Mai 2018 von http://kiras.at/gefoerderte-projekte/detail/d/genesis-guideline-fuer-behoerden-und-kmu-anbieter-strategischer-services-zur-risiko-orientierten-im/

KSÖ – Kuratorium Sicheres Österreich. 2016. KSÖ Rechts- und Technologiedialog Whitepaper. Wien, Österreich: KSÖ – Kuratorium Sicheres Österreich.

KSÖ – Kuratorium Sicheres Österreich. s.a.. *Cyber Security*. Abgerufen am 2. Mai 2018 von https://kuratorium-sicheres-oesterreich.at/allgemein/cyber-security/

Mayer, Sylvia und Gregor Schmied. 2017. NIS-RL und ihre Umsetzung in Österreich. Wien, Wien, Österreich.

Menold, Natalja und Kathrin Bogner. 2015. *Gestaltung von Ratingskalen in Fragebögen.* Mannheim: GESIS – Leibniz-Institut für Sozialwissenschaften (SDM Survey Guidelines). Abgerufen am 12. Mai 2018 von https://www.gesis.org/fileadmin/upload/SDMwiki/Archiv/Ratingskalen_MenoldBogner_012015_1.0.pdf

Michaelis, Patrick. 2016. *DuD • Datenschutz und Datensicherheit - Der „Stand der Technik" im Kontext regulatorischer Anforderungen.* Springer Verlag.

Pomberger, Gustav und Wolfgang Pree. 2004. *Software Engineering: Architektur-Design und Prozessorientierung. 3. Auflage*. München: Carl Hanser Verlag.

Republik Österreich - Parlamentsdirektion. s.a.. Der Weg eines Bundesgesetzes. Österreich: Abgerufen am 12. April 2018 von https://parlament.gv.at/ZUSD/PDF/Weg_der_Bundesgesetzgebung.pdf.

Schmid, Fabian. 2018. *Cybersicherheitsgesetz nicht fertig: Österreich verpasst EU-Frist - derstandard.at/2000079522231/Cybersicherheitsgesetz-nicht-fertig-Oesterreich-verpasst-EU-Frist*. Abgerufen am 12. Mai 2018 von https://derstandard.at/2000079522231/Cybersicherheitsgesetz-nicht-fertig-Oesterreich-verpasst-EU-Frist

Schnider, Alexander. 2017. *Status der NIS Richtlinie in den EU-Mitgliedstaaten*. Abgerufen am 12. Mai 2018 von https://geistwert.at/status-der-nis-richtlinie-in-den-eu-mitgliedstaaten/

Schulzki-Haddouti, Christiane. 2017. *„Mit so einem Virus können Sie ganz Europa lahmlegen"*. Abgerufen am 2. Mai 2018 von https://vdi-nachrichten.com/Gesellschaft/Mit-so-Virus-koennen-Sie-Europa-lahmlegen

Sulzbacher, Markus. 2018. *Regierung: Wenn Kriminelle IT-Lücken nutzen, soll das auch der Staat tun*. Abgerufen am 2. Mai 2018 von https://derstandard.at/2000077415932/Regierung-Wenn-Kriminelle-IT-Luecken-nutzen-soll-das-auch-der

TeleTrusT – Bundesverband IT-Sicherheit e.V. 2010. *EU-Kommission: Stärkung der ENISA*. Abgerufen am 12. Mai 2018 von https://teletrust.de/startseite/news/?tx_ttnews%5Btt_news%5D=230&cHash=211bed2ee4a3cf3b6ab58686d9500fa9

Tschohl, Christof, Walter Hötzendorfer, Gerald Quirchmayr, Edith Huber und Otto Hellwig. 2017. DIE NIS-RICHTLINIE UND DER RECHTLICHE RAHMEN VON CERTS. ResearchGate.

Universität Augsburg. s.a.. *Etappe 2 der Dokumentation*. Abgerufen am 2. Mai 2018 von https://onlinekurslabor.phil.uni-augsburg.de/course/text/3618/3567

Universität Passau. s.a.. *NIS-Richtlinie*. Abgerufen am 2. Mai 2018 von https://www.baywidi.de/wiki/gesetzliche-grundlagen/gesetzliche-grundlagen-fuer-betreiber-kritischer-infrastrukturen/nis-richtlinie/

Wikipedia. 2018. *Rechtskreis*. Abgerufen am 10. Mai 2018 von https://de.wikipedia.org/wiki/Rechtskreis

Wilde, Thomas und Thomas Hess. 2006. *Methodenspektrum der Wirtschaftsinformatik: - Überblick und Portfoliobildung*. Abgerufen am 2. Mai 2018 von https://epub.ub.uni-muenchen.de/14146/1/hess_14146.pdf

Wimmer, Barbara. 2017. *Staatstrojaner: Überwachung umfangreicher als gedacht*. Abgerufen am 2. Mai 2018 von https://futurezone.at/netzpolitik/staatstrojaner-ueberwachung-umfangreicher-als-gedacht/274.332.667

Winter, Robert und Richard Baskerville. 2010. *WIRTSCHAFTSINFORMATIK (2010) 52: 257*. Abgerufen am 2. Mai 2018 von https://doi.org/10.1007/s11576-010-0242-2

Wischmeyer, Thomas. 2016. IT-Sicherheitsgesetz und NIS-Richtlinie als Elemente eines Ordnungsrechts für die Informationsgesellschaft. Freiburg: Die Verwaltung.

xmera e.K. 2017. IT-SICHERHEITSGESETZ ENERGIEVERSORGER & NEUREGELUNG. Gelsenkirchen, Deutschland: xmera e.K.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACI	Austrian Critical Infrastructure (Österreichische Kritische Infrastruktur)
AdD	Anbieter digitaler Dienste
APCIP	Austrian Program for Critical Infrastructure Protection (Österreichisches Programm zum Schutz kritischer Infrastrukturen)
AtG	Atomgesetz
B3S	Branchenspezifische Sicherheitsstandards
BAK	Branchenarbeitskreis
BbesG	Bundesbesoldungsgesetz
BBK	Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management (Betriebliches Kontinuitätsmanagement)
BGebGEG	Gesetz zur Strukturreform des Gebührenrechts des Bundes
BKA	Bundeskanzleramt
BKAG	Bundeskriminalamtgesetz
BMFWJ	Bundesministerium für Familie, Wirtschaft und Jugend
BMI	Bundesministerium für Inneres
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BwD	Betreiber wesentlicher Dienste
bzw.	beziehungsweise
ca.	circa
CERT	Computer Emergency Response Team (Computersicherheits-Ereignis- und Reaktionsteam)
CISO	Chief Information Security Officer
CIWIN	Critical Infrastructure Warning and Information Network
CKM	Cyber Krisen Management
CMMI	Capability Maturity Model Integration
CMMI-ACQ	CMMI for Acquisition (CMMI für Beschaffung)
CMMI-DEV	CMMI for Development (CMMI für Entwicklung)
CMMI-SVC	CMMI for Services (CMMI für Dienstleistungen)
CSIRT	Computer Security Incident Response Team
DIN	Deutsches Institut für Normung
DSGVO	Datenschutz-Grundverordnung
EKI	Europäische kritische Infrastrukturen
ENISA	European Union Agency for Network and Information Security (Europäische Agentur für Netz- und Informationssicherheit)
EnWG	Energiewirtschaftsgesetz
EPCIP	European Program for Critical Infrastructure Protection (Europäisches Programm zum Schutz kritischer Infrastrukturen)
etc.	et cetera
EU	Europäische Union
f	folgende (Originalzitat geht über maximal zwei Seiten)
ff	fortfolgende (Originalzitat geht über mehr als zwei Seiten)
IKT	Informations- und Kommunikationstechnologien

inkl.	inklusive
KIRAS	Österreichisches Sicherheitsforschungsprogramm
ISMS	Information Security Management System (Informationssicherheits Managementsystem)
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnologie
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
IT-SP	IT-Service Provider
KG	Kooperationsgruppe
KI	Kritische Infrastrukturen (Österreich)
KMU	kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen (Deutschland)
KSÖ	Kuratorium Sicheres Österreich
MIRT	Mobile Incident Response Team
N.N.	nomen nescio (kein/e AutorIn)
N/A	Not Applicable (Nicht Anwendbar)
NACE	Nomenclature générale des activités économiques dans les communautés européennes
NCSS	National Cyber Security Strategies (Nationale Cyber Sicherheits Strategien)
NIS	Netz- und Informationssysteme
NISG	Netz- und Informationssystemsicherheitsgesetz
NIS-Richtlinie	Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
NIS-Richtlinien-UG	Gesetz zur Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
ÖBB	Österreichische Bundesbahnen
ÖNACE	Österreichische Form von NACE
ÖSCS	Österreichische Strategie für Cyber Sicherheit
ÖSS	Österreichische Sicherheitsstrategie
PPP	Public-Private-Partnership
R-IT	Raiffeisen Informatik
s.a.	sine anno (keine Jahresangabe)
s.p.	sine pagina (keine Seitenangabe)
SGB V	Fünfte Buch des Sozialgesetzbuches
SKI	Schutz kritischer Infrastrukturen
SKKM	Staatliches Krisen- und Katastrophenschutzmanagement
SLA	Service Level Agreement
SPICE	Software Process Improvement and Capability Determination
SPOC	Single Point of Contact
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
UP	Umsetzungsplan
uvm.	und vieles mehr
vgl.	vergleiche
z.B.	zum Beispiel

Anhang A - „Self Assessment für NIS-Readiness“

In diesem Anhang A ist der komplette Prototyp des „Self Assessment für NIS-Readiness“ enthalten, welcher auf der (dieser Masterarbeit beiliegenden) CD unter folgenden Dateinamen zu finden ist.

- Prototyp-Self Assessment für NIS-Readiness.xlsx

Anhang B - Ergebnisse der ExpertInnenbefragungen

In Anhang B sind die Ergebnisse der sechs durchgeführten ExpertInnenbefragungen, die im Zusammenhang mit dem „Self Assessment für NIS-Readiness“ durchgeführt wurden, detailliert dokumentiert. Es wurden ausschließlich die freigegebenen Informationen als nicht veränderbare Inhalte übernommen.

Die einzelnen beantworteten Fragebögen der ExpertInnen sind auf der (dieser Masterarbeit beiliegenden) CD unter folgenden Dateinamen zu finden.

- Expertenbefragung-ExpertIn I-Originalübertrag+Gespräch.pdf
- Expertenbefragung-Experte II-Originalübertrag+Gespräch.pdf
- Expertenbefragung-Experte III-Originalübertrag+Gespräch.pdf
- Expertenbefragung-Experte IV-Originalübertrag+Gespräch.pdf
- Expertenbefragung-Experte V-Originalübertrag+Gespräch.pdf
- Expertenbefragung-Experte VI-Originalübertrag+Gespräch.pdf

Anhang C - Ergebnisse der Feldexperimente

In Anhang C sind die beiden durchgeführten Feldexperimente des „Self Assessment für NIS-Readiness“ im Detail dokumentiert. Diese sind auf der (dieser Masterarbeit beiliegenden) CD unter folgenden Dateinamen zu finden.

- ÖBB-Self Assessment-NIS-Readiness.xlsx
- R-IT-Self Assessment-NIS-Readiness.xlsx