FERDINAND PORSCHE
FERNFH

Die Vereinbarkeit von Vertraulichkeit und Integrität mit der Hochverfügbarkeit von kritischen Systemen

Masterarbeit

Eingereicht von: **Peter Gneist, BA**

Matrikelnummer: 0052210612

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Christoph Jungbauer, BA MA MA

Zweitgutachten: Ing. Anna Völkl, BSc MSc

Brunn am Gebirge, September 2024

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.

Brunn am Gebirge, 4. September 2024 _____

Unterschrift

Kurzzusammenfassung:

Die Vereinbarkeit von Vertraulichkeit und Integrität mit der Hochverfügbarkeit von kritischen Systemen

Die Masterarbeit untersucht im Kontext von kritischen Systemen die Vereinbarkeit von hohen Anforderungen an Vertraulichkeit und Integrität einerseits mit einer hohen Verfügbarkeit andererseits. Dazu wurde die Design Science Methode angewendet und mittels Literaturstudie zunächst iterativ die Erwartungen an die umzusetzenden Sicherheitsmaßnahmen formuliert. Diese wurden schließlich mit Expert_innen-Interviews evaluiert, welche mit der qualitativen Inhaltsanalyse nach Mayring ausgewertet wurden.

Die Literaturstudie zeigte, dass zahlreiche Standards und Best Practices existieren, es jedoch schwierig ist die passenden auszuwählen. Daher wurde das österreichische Netz- und Informationssystemsicherheitsgesetz als Referenz verwendet, das konkrete Sicherheitsmaßnahmen für kritische Infrastrukturen definiert. Zusätzlich wurde das Security-by-Design Prinzip beleuchtet und es wurden Aspekte wie Risikomanagement, Hochverfügbarkeit, Systemkomplexität und Wirtschaftlichkeit untersucht.

Mithilfe von acht Expert_innen wurden die theoretischen Erwartungen schließlich evaluiert. Die Ergebnisse zeigen, dass keine allgemeingültige Aussage zur Vereinbarkeit hoher Vertraulichkeits- und Integritätsanforderungen mit hoher Verfügbarkeit möglich ist. Es gibt zwar Indizien, dass in bestimmten Fällen zugunsten der Verfügbarkeit auf zentrale Sicherheitsanforderungen verzichtet werden kann, aber eine allgemeingültige Regel lässt sich daraus nicht ableiten. Stattdessen wird die Kontextabhängigkeit der Sicherheitsanforderungen hervorgehoben und die Notwendigkeit eines subjektiven, risikobasierten Ansatzes betont.

Schlagwörter:

Sicherheit, Anforderungen, NIS, Verfügbarkeit, Vertraulichkeit, Integrität, Design Science

Abstract:

The compatibility of confidentiality and integrity with the high availability of critical systems

In the context of critical systems, the master's thesis examines the compatibility of high confidentiality and integrity requirements on the one hand and high availability on the other. To this end, the design science method was applied and the expectations of the security measures to be implemented were first iteratively formulated by means of a literature study. These were then evaluated using expert interviews, which were analysed using Mayring's qualitative content analysis.

The literature study showed that numerous standards and best practices exist, but that it is difficult to select the appropriate ones. The Austrian Network and Information System Security Act, which defines specific security measures for critical infrastructures, was therefore used as a reference. In addition, the security-by-design principle was examined and aspects such as risk management, high availability, system complexity and cost-effectiveness were investigated.

Finally, the theoretical expectations were evaluated with the help of eight experts. The results show that it is not possible to make a generally valid statement on the compatibility of high confidentiality and integrity requirements with high availability. Although there are indications that in certain cases central security requirements can be dispensed with in favour of availability, a generally valid rule cannot be derived from this. Instead, the context dependency of security requirements is emphasized and the need for a subjective, risk-based approach is stressed.

Keywords:

Security, Requirements, NIS, Availability, Confidentiality, Integrity, Design Science

Danksagung

An erster Stelle bedanke ich mich bei meinem Betreuer für die tolle Unterstützung. Danke Christoph für deine unbürokratische Art, dafür dass du auch spontan und unkompliziert für Termine bereitgestanden bist und du mich mit deinen lösungsorientierten Ideen zurück in die Spur gebracht hast. Du warst mir eine große Hilfe und ich bin froh dich als meinen Betreuer gehabt zu haben!

Ich bedanke mich auch vielmals bei meinen Interview-Partnern für ihre Bereitschaft mich bei meiner Arbeit zu unterstützen. Es ist alles andere als selbstverständlich, dass solche Key-Player und angesehene Fachexpert_innen sich die Zeit nehmen um bei einem Forschungsprojekt wie meinem mitzuwirken, und das rechne ich ihnen hoch an. Vielen Dank dafür! Ich fand es super spannend von euch zu lernen und eure Standpunkte zu erfahren!

Ich bedanke mich auch bei meinen Eltern und bei meinem Sohn für ihren laufenden Zuspruch und die aufmunternden Worte, die sie zwischendurch gefunden haben. Ihr habt mir so oft zugehört, wenn ich über die Arbeit gesprochen habe, und mich damit aufgemuntert, das hat mir viel bedeutet!

Ein gewaltiges Dankeschön gilt meinem früheren Studien-Kollegen und nunmehrigen engen Freund Thomas. Danke Thomas für die vielen, richtungsweisenden Gespräche die wir geführt haben, für die Zeit die du dir genommen hast, für deine unglaubliche Expertise und für deine immer offene und unterstützende Art! Du bist ein Wahnsinn!

Last but not least bedanke ich mich bei meiner Freundin Nicole, mit der ich unendlich viele Gespräche zu dieser Arbeit geführt habe und die mich mental unterstützt hat. Sie war aber nicht nur moralisch für mich da, sondern hat mir auch mit ihrer Cleverness und ihrer akademischen Erfahrung dabei geholfen die Arbeit greifbar zu machen und auf den Boden zu bekommen. Danke, dass du mich unterstützt und an mich geglaubt hast, du bist die Beste!

Vorwort

Auslöser und Ideengeber dieser Arbeit ist der sogenannte AT-Alert. Das ist eine österreichische Initiative die auf einer EU-Regulierung beruht, die zum Ziel hat im Katastrophenfall Warnmeldungen an die österreichische Bevölkerung zu senden, damit diese informiert ist und sich in Sicherheit bringen kann. Ich bin vonseiten eines der österreichischen Mobilfunkanbieter hauptverantwortlich für die Umsetzung des AT-Alert und begleite das Projekt in dieser Rolle seit mehr als zwei Jahren. Entsprechend habe ich viele der technischen Diskussionen rund um dessen Umsetzung miterlebt und habe die Evolutionsstufen des technischen Designs kommentiert und diskutiert. Und im Zuge dieser Design-Erstellung war ich überrascht, dass selbst über die Umsetzung von einfachen Sicherheitsmaßnahmen diskutiert wurde, die ich in meiner bisherigen beruflichen Erfahrung für indiskutabel wahrgenommen und als absolute Grund-Anforderungen an die IT-Sicherheit eingestuft hatte. Gleichzeitig wurden andere, für meine Begriffe überraschende Design-Entscheidungen getroffen, die ich in meiner beruflichen Laufbahn bis dahin weder als Software-Entwickler noch als Designer oder Architekt jemals zu Gesicht bekommen hatte. Als Hintergrund dieser Überlegungen stellten sich die hohen Anforderungen an die Verfügbarkeit des Systems heraus. Nachdem es sich bei dem AT-Alert um ein Alarmierungssystem handelt, das im Katastrophenfall eingesetzt werden soll um Gefahren für Leib und Leben abzuwenden, ist es schließlich nachvollziehbar, dass eine extrem hohe Verfügbarkeit gegeben sein muss und das System immer bereitstehen muss. Und das obwohl es gleichzeitig nur sehr selten, im Idealfall sogar niemals, benötigt wird.

Das brachte mich auf die Idee zu erforschen ob diese Überlegungen gerechtfertigt waren und wie denn wirklich der Zusammenhang von Anforderungen an die Vertraulichkeit und Integrität auf der einen Seite und einer hohen Verfügbarkeit auf der anderen Seite ist. Und so habe ich mir zum Ziel gesetzt in dieser Arbeit zu untersuchen ob es Situationen gibt, in denen es legitim ist selbst auf Basis-Anforderungen der IT-Sicherheit zu verzichten um damit eine höhere Verfügbarkeit zu erreichen.

Inhaltsverzeichnis

1 Einleitung 1

1.1 Ausgangslage 1

1.2 Ziel der Arbeit 3

1.3 Forschungsfrage 3

1.4 Methodik 4

1.4.1 Literaturstudie 5

1.4.2 Design Science 5

1.4.3 Qualitative Expert_innen-Interviews 7

2 Sicherheitsanforderungen 9

2.1 Standards, Referenz-Modelle und Best Practices 9

2.1.1 ITIL 9

2.1.2 COBIT 10

2.1.3 ISO/IEC 20000 10

2.1.4 ISO/IEC 27000 11

2.1.5 BSI IT-Grundschutz 12

2.1.6 NIST Cybersecurity Framework 13

2.1.7 CIS Controls 14

2.1.8 OWASP Top 10 14

2.1.9 Vielfalt und Vielschichtigkeit 15

2.1.10 Problematik 16

2.2 NIS-Richtlinie und Umsetzung in Österreich 17

2.2.1 NIS-Gesetz, NISG 18
2.2.2 NIS-Verordnung, NISV 18
2.2.3 NIS-Factsheets 23
2.2.4 Österreichisches Sicherheitshandbuch 24
2.2.5 ÖNORM A7700 24
2.2.6 IEC 62443 25
2.2.7 EN 50600 26
2.3 Security by Design 26
3 Umsetzung von Sicherheitsanforderungen 29
3.1 Risikomanagement 29
3.1.1 Risikoanalyse 29
3.1.2 Risikobehandlung 33
3.1.3 Kritik 34
3.2 Hochverfügbarkeit und Redundanzen 34
3.2.1 Definition von Verfügbarkeit 35
3.2.2 Redundanzen 37
3.2.3 Verfügbarkeitsberechnung 40
3.3 Komplexität 41
3.3.1 Microservices-Ansatz 42
3.3.2 Cloud-Computing 43
3.3.3 Weitere Dienste 44
3.4 Wirtschaftlichkeit 45
3.4.1 Return on Security Investment (ROSI) 47

4 Abgeleitete Erwartungen 49
4.1 Anforderungsquellen 49
4.2 Vertraulichkeit und Integrität 49
4.3 Verfügbarkeit 50
4.4 Wirtschaftlichkeit 50
5 Expert_innen-Interviews 51
5.1 Interview-Gestaltung 51
5.2 Durchführung der Interviews 53
5.3 Qualitative Inhaltsanalyse nach Mayring 56
6 Forschungsergebnisse 59
6.1 Anforderungsquellen 59
6.1.1 Österreichisches Sicherheitshandbuch 61
6.1.2 Ö-Normen 62
6.2 Vertraulichkeit und Integrität 62
6.3 Verfügbarkeit 64
6.3.1 Komplexität und externe Dienste 65
6.3.2 Security by Design 67
6.4 Testing von Sicherheitsanforderungen 68
6.5 Wirtschaftlichkeit 70
6.5.1 Return on Security Investment (ROSI) 72
6.6 Vertraulichkeit & Integrität vs. Verfügbarkeit 74
7 Diskussion 78
7.1 Zusammenfassung und Beantwortung der Forschungsfrage 78

7.1.1 Anforderungsquellen 78
7.1.2 Vertraulichkeit und Integrität 79
7.1.3 Verfügbarkeit 79
7.1.4 Wirtschaftlichkeit 80
7.1.5 Vereinbarkeit von Vertraulichkeit & Integrität mit Verfügbarkeit 81
7.2 Offenbarte Problemfelder 82
7.3 Gegenüberstellung der Forschungsergebnisse 83
7.3.1 Gegenüberstellung mit den Fallstudien zur IT-Sicherheit 83
7.3.2 Gegenüberstellung mit dem Themenband Resilienz 84
7.4 Reflexion der Methode 85
7.5 Forschungsausblick 86
7.6 Fazit 87
8 Literaturverzeichnis 89
9 Abbildungsverzeichnis 99
10 Tabellenverzeichnis 100
11 Abkürzungsverzeichnis 101
Anhang A – Interviewleitfaden 103
Anhang B – Soziodemografische Daten 108
Anhang C – Einwilligungserklärung 110
Anhang D – Codesystem 114

1 Einleitung

1.1 Ausgangslage

Informationssicherheit wird definiert als die "Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität" (Melanie Rainer, Thomas Neuroth-Pfeiffer, Martin Latzenhofer, & Christian Focke, 2022a), den sogenannten Schutzzielen, und um diese Schutzziele zu erreichen ist es nötig technische Maßnahmen umzusetzen. Dazu gehören etwa Maßnahmen wie Authentifizierung, also dem Feststellen der Identität, oder zur Autorisierung, dem Prüfen der Zugangsberechtigung. (Melanie Rainer et al., 2022a) Darüber hinaus ist für eine sichere Netzwerkarchitektur ebenso zu sorgen wie für die sichere Konfiguration aller System-Bausteine der einzelnen Anwendungen. (Bundesamt für Sicherheit in der Informationstechnik, 2023) Die Gewährleistung der Informationssicherheit bedingt also die Einführung zusätzlicher, technischer Komponenten. „IT-Sicherheitsmaßnahmen müssen eingeführt, Technologien ausgewählt und im Unternehmen implementiert werden und das Thema IT-Sicherheit muss in Strategien und der täglichen Agenda die notwendige Priorität erhalten." (Ulrike Lechner, Sebastian Dännart, Andreas Rieb, & Steffi Rudel, 2018)

Allerdings beeinflusst jede zusätzliche Komponente einer Anwendung auch deren Architektur und macht sie komplexer. Und dies hat in weiterer Folge Auswirkungen auf deren Ausfallswahrscheinlichkeit. Das liegt daran, dass jede Komponente ihre eigene Ausfallswahrscheinlichkeit besitzt und abhängig davon ob diese Komponenten in der Applikation seriell oder parallel geschaltet werden, beeinflusst dies entweder die Gesamtverfügbarkeit oder den Bedarf an zusätzlichen Redundanzen. (Andrea Held, 2015)

Durch die Umsetzung von Sicherheitsanforderungen steigt also die Komplexität des Gesamtsystems, und in Bezug auf die Verfügbarkeit von Systemen hat „die Geschichte der Informationssicherheit […] gezeigt, dass die Komplexität der Infrastrukturen schon immer Feind der Security war." (Rich Campagna, 2023) Der Themenband Resilienz drückt das noch direkter aus und meint: „Der ärgste Feind von Sicherheit ist Komplexität. Je komplexer ein System ist, desto unsicherer ist es."(Lunkeit & Zimmer, 2021, S. 112)

Diese Aussagen bestätigen Vorfälle bei denen ausgerechnet Probleme mit Sicherheitsmaßnahmen zu Systemausfällen geführt haben. Geschehen etwa aufgrund von abgelaufenen SSL Zertifikaten, die zu Verfügbarkeitseinbußen geführt haben. (Lea Toms, 2016) Auch sind bereits Root-Zertifikate von Certification Authorities (CAs) invalidiert

worden, was mit einem Schlag viele über sie ausgestellte SSL-Zertifikate ungültig gemacht hat. (Sectigo Limited, 2020) Aber auch die vom BSI empfohlene Mehr-Faktor-Authentisierung (Bundesamt für Sicherheit in der Informationstechnik, 2023a) erfordert, dass das für diesen Zweck häufig genutzte One-Time-Password auch wirklich stets bis zum Endanwender übertragen werden kann. (ComputerWeekly, 2023) Funktioniert das aus irgendeinem Grund nicht, ist - sofern es keine alternative Anmeldefunktion gibt - kein Login in die Anwendung mehr möglich. Und schließlich bestätigt auch ein aktueller Fall, in dem eine Cybersecurity-Software aufgrund eines fehlerhaften Software-Updates zu weltweiten IT-Ausfällen geführt hat, dass der Einsatz von Sicherheitsmaßnahmen die Verfügbarkeit von Anwendungen gefährden kann.(Bundesamt für Sicherheit in der Informationstechnik, 2024a; Weiß, 2024)

Nun gibt es aber Systeme bei denen die Verfügbarkeit der kritischste Faktor ist, wie das etwa bei den Warnungs- und Alarmierungssystemen des Krisen- und Katastrophenmanagements der Fall ist. Bei solchen Systemen geht es darum die Bevölkerung vor eingetretenen Katastrophensituationen zu warnen und in solchen Fällen ist es naturgemäß von entscheidender Bedeutung, dass auf Krisensituationen zeitnahe reagiert werden kann. (Bundesministerium für Inneres, 2023) Solche Systeme können auch nicht isoliert und völlig abgeschottet aufgebaut und betrieben werden, denn sie benötigen zum Funktionieren externe Schnittstellen, etwa zu den Landeswarnzentralen oder sogar zu den Mobilfunkbetreibern wie im Falle des sog. AT-Alerts. (Bundeskanzleramt, 2023) Und es stellt sich die Frage ob selbst bei Systemen dieser Kategorie die Umsetzung hoher Sicherheitsanforderungen möglich ist, ohne gleichzeitig Risiken in Bezug auf deren Verfügbarkeit einzugehen. Wobei die genannten Warnungs- und Alarmierungssysteme nur als veranschaulichendes Beispiel gedacht sind und sich die Untersuchung in dieser Arbeit nicht exklusiv darauf beziehen soll. Stattdessen soll sie sich auf kritische Systeme im Allgemeinen beziehen.

Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen zeigen mögliche Lösungen in ähnlichen Themengebieten (Ulrike Lechner et al., 2018) und der Themenband Resilienz behandelt unter anderem „Resiliente kritische und sensible Infrastrukturen im Kontext moderner Kommunikationssysteme“ (Volker Wittpahl, 2023). Diese werden in dieser Arbeit an mehreren Stellen herangezogen um die Frage zu beantworten wie bei kritischen Systemen mit der Wechselwirkung aus hohen Anforderungen and die Vertraulichkeit und Integrität einerseits und jenen an eine hohe Systemverfügbarkeit andererseits umgegangen werden kann. Es wird darin ermittelt ob es Voraussetzungen gibt in denen es nötig ist zugunsten einer hohen Systemverfügbarkeit auf die Umsetzung von

Sicherheitsmaßnahmen bewusst zu verzichten. Und um die Offenheit im Denken zu bewahren bezieht sich diese Arbeit auf kritische Systeme, deren Anforderungen frei definiert werden können und nicht bereits durch externe Normen strikt vorgegeben sind.

1.2 Ziel der Arbeit

Ziel der Arbeit ist es zu erforschen ob hohe Anforderungen an Vertraulichkeit und Integrität und eine hohe Systemverfügbarkeit miteinander vereinbar sind, und um dies zu beurteilen werden darin folgende Dimensionen berücksichtigt:

- *Die technische Machbarkeit*: In diesem Aspekt wird untersucht welche Sicherheitsanforderungen bestehen und welche technischen Mittel zur Verfügung stehen um diese zu erfüllen. Insbesondere die NIS-Richtlinie der Europäischen Union und die oben erwähnten Fallstudien werden hierfür als Referenz herangezogen.
- *Die wirtschaftlichen Auswirkungen*: In diesem Punkt wird berücksichtigt inwiefern wirtschaftliche Aspekte in der Umsetzung von Sicherheitsanforderungen miteinbezogen werden können.
- *Die Meinungen ausgewiesener Fachexpert_innen*: Diese Dimension erweitert die Forschung um den Aspekt der Praxistauglichkeit. Von Fachexperten wird darin erhoben wie sie die Umsetzbarkeit der Sicherheitsanforderungen gesamtheitlich einstufen und wie sie ggfs. bei vergleichbaren Aufgabenstellungen vorgegangen sind.

Auf diese Art wird die Umsetzbarkeit und Praxistauglichkeit der Anforderungen geprüft, und das konkret in Bezug auf die eingangs beschriebenen, kritischen Systeme.

1.3 Forschungsfrage

Die konkrete, wissenschaftliche Forschungsfrage lautet:

> Lassen sich in Bezug auf kritische Systeme mit externen Schnittstellen sowohl hohe Anforderungen im Bereich der Vertraulichkeit und Integrität als auch eine hohe Systemverfügbarkeit gleichzeitig umsetzen?

Diese dient der Prüfung folgender Hypothese:

Bei kritischen Systemen mit externen Schnittstellen stehen hohe Sicherheitsanforderungen im Bereich der Vertraulichkeit und Integrität und eine hohe Systemverfügbarkeit im Widerspruch zueinander.

1.4 Methodik

Um die Forschungsfrage zu beantworten folgt diese Arbeit der Methodik des empirischen, sozialwissenschaftlichen Forschungsprozesses, der in Abbildung 1 illustriert wird.(Gläser & Laudel, 2009, S. 33ff)

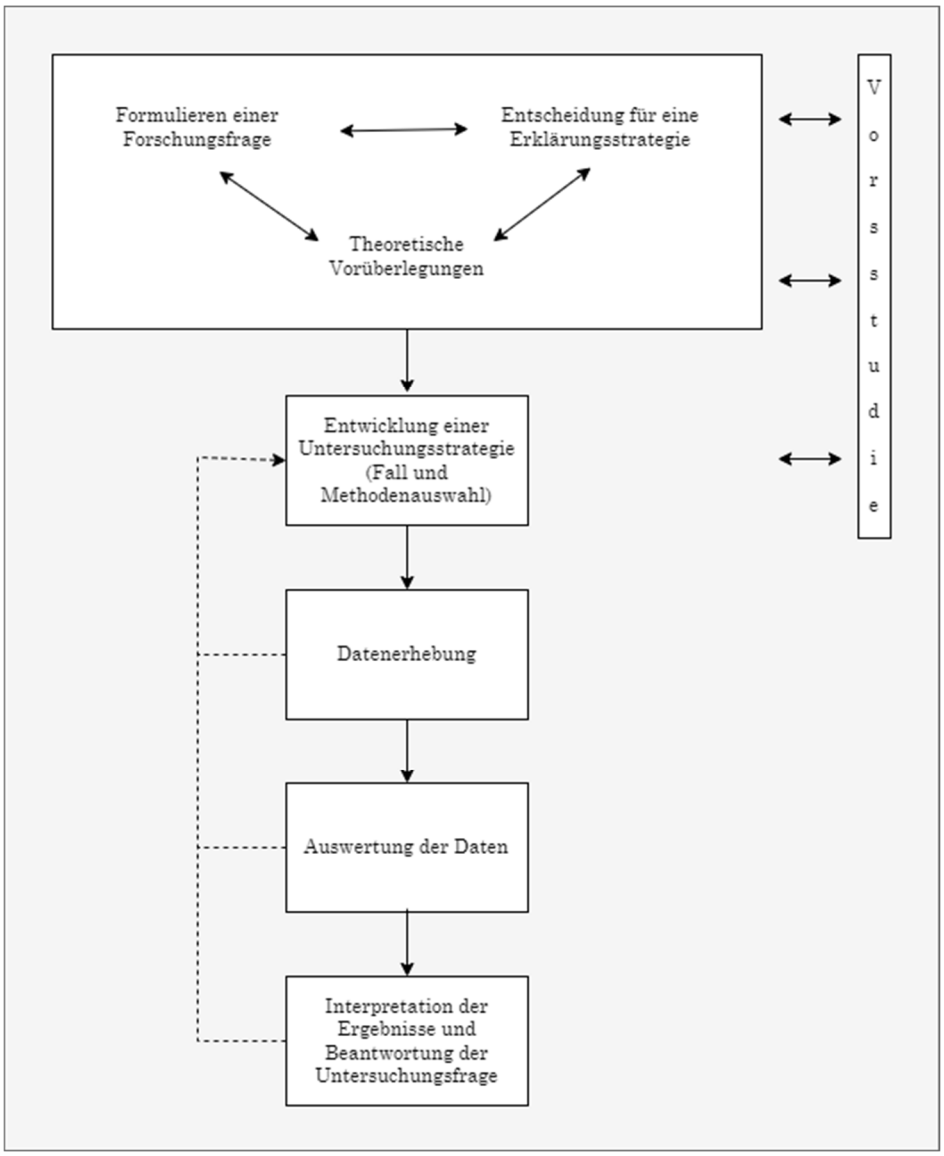

Abbildung 1: Empirischer, sozialwissenschaftlichen Forschungsprozess (nach Gläser & Laudel, 2009, S. 35)

Dabei wird als übergeordnete Untersuchungsstrategie der Design Science Ansatz gewählt. Für die Datenerhebung werden Literaturstudien und mehrere qualitative

Expert_innen-Interviews durchgeführt. Die Auswertung der Daten erfolgt schließlich mit der Qualitativen Inhaltsanalyse nach Mayring.

1.4.1 Literaturstudie

Die Literaturstudie dient der Ermittlung des aktuellen Stands von Forschung & Technik und ist somit die Grundlage für die wissenschaftliche Arbeit. (Ferdinand Porsche FernFH, 2023)

Folgende Quellen werden in dieser Arbeit bevorzugt herangezogen um Sicherheitsanforderungen zu bestimmen, wobei in den Kapiteln 2 und 3 erläutert wird warum genau diesen eine besondere Bedeutung beigemessen wird:

- Österreichische Umsetzung der NIS-Richtlinie
- Österreichisches Sicherheitshandbuch (Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)
- IT Grundschutz Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2023a)
- ISO/IEC 27000 (Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024a)
- Cybersecurity Framework des National Institute of Standards and Technology (NIST) (National Institute of Standards and Technology, 2024)

Zusätzlich dazu werden aus den eingangs angeführten, wissenschaftlichen Arbeiten weitere Anforderungen und Rahmenbedingungen abgeleitet.

1.4.2 Design Science

Design Science ist eine Methode, die es ermöglicht auf Basis von wissenschaftlichen und praktischen Kriterien ein (Design-)Artefakt zu erstellen. Die Erzeugung eines solchen Artefakts unterliegt dabei existierenden Kerntheorien, die anhand der Kreativität, Erfahrung, Intuition und Problemlösungsfähigkeit der Forscher_innen angewendet, getestet, modifiziert und erweitert werden. (Hevner, A.R.; March, S.T.; Park, J.; Ram, S., 2004)

Konkret wird für der Verwendung der Design Science Methode verlangt, dass folgende sieben Richtlinien eingehalten werden (Hevner, A.R.; March, S.T.; Park, J.; Ram, S., 2004, S. 83):

- *Design as an Artifact*: Diese Richtlinie besagt, dass ein realisierbares Artefakt in Form eines Konstrukts, Modells, einer Methode oder einer Instanziierung erzeugt werden soll.
- *Problem Relevance*: Diese Richtlinie verlangt, dass ausschließlich wichtige und betriebswirtschaftlich relevante Probleme behandelt werden sollen. Diese sollen mit einer technologiebasierten Lösung adressiert werden.
- *Design Evaluation*: Zur Evaluierung der Nutzbarkeit, Qualität und Wirksamkeit des Artefakts sollen bestimmte Evaluations-Methoden eingesetzt werden.
- *Research Contributions*: Die Forschung mit der Design-Science Methodik muss klare und nachprüfbare Beiträge in den Bereichen des Design-Artefakts, der Design Grundlagen und/oder der Design Methoden liefern.
- *Research Rigor*: Die Forschung mittels Design Science verlangt die Anwendung strikter Forschungsmethoden, also eine methodische Stringenz, sowohl in der Erzeugung als auch in der Evaluierung des Artefakts.
- *Design as a Search Process*: Diese Richtlinie besagt, dass auf der Suche nach einem wirksamen Artefakt alle verfügbaren Mittel genutzt werden sollen, um die gewünschten Ziele zu erreichen. Gleichzeitig müssen aber auch die Gesetze der jeweiligen Problemumgebung beachtet werden.
- *Communication of Research*: Diese Richtlinie verlangt schließlich, dass die Forschungsergebnisse sowohl einem technologie-orientierten als auch für management-orientierten Publikum präsentiert werden sollen.

In der Durchführung unterscheidet die Design Science Methode in zwei Teilprozesse: Den *Build*-Prozess, über den das Artefakt erzeugt wird, und den *Evaluate*-Prozess, mit dem die erzielten Ergebnisse geprüft und analysiert werden. Diese Prozesse können mehrmals im Wechselspiel durchgeführt werden bis das Ergebnis fertiggestellt ist, ein zyklischer Vorgang der in der Methode als *Design Cycle* bezeichnet wird. Unterstützt wird dieser durch zwei weitere Zyklen, die in der Methode als *Relevance Cycle* und *Rigor Cycle* bezeichnet werden. Die Aufgabe des *Relevance Cycle* ist es dabei den Praxisbezug sicherzustellen und dafür zu sorgen, dass das Artefakt nur wirklich relevante Problemstellungen adressiert. Der *Rigor Cycle* stellt hingegen den wissenschaftlichen Bezug sicher, und kümmert sich darum, dass das Artefakt methodisch korrekt erarbeitet und theoretisch fundiert ist. Alle drei Zyklen laufen prinzipiell parallel ab, beeinflussen sich aber wechselseitig. So steuern der *Relevance* und der *Rigor Cycle* den *Design Cycle*, in dem sie ihm zusätzliche Inputs geben, es können aber auch im *Relevance Cycle* neue

Fragestellungen aufgeworfen werden, die wiederum im *Rigor Cycle* behandelt werden. (Ferdinand Porsche FernFH, 2023b; Hevner, A.R.; March, S.T.; Park, J.; Ram, S., 2004)

Das nachfolgende Diagramm illustriert diese Zusammenhänge noch einmal.

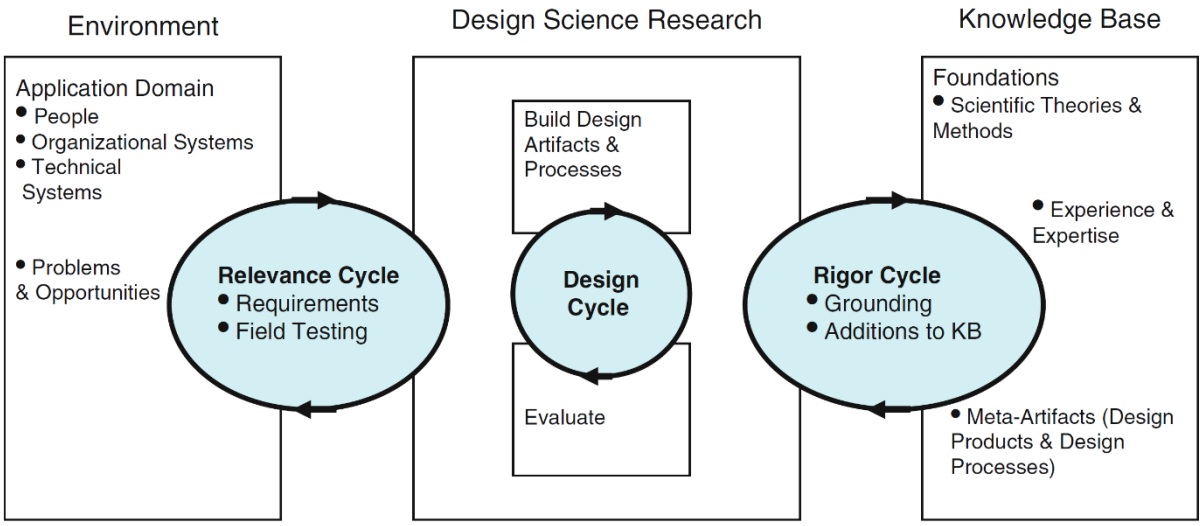

Abbildung 2: Design Sciene Zyklen (Hevner & Chatterjee, 2010)

Im Kontext dieser Arbeit wird die Design Science Methode angewendet um zunächst zu beschreiben welche Herangehensweise und welche Sicherheitsanforderungen bei der Umsetzung von kritischen Systemen erwartet werden können. Dies ist das im Prozess erstellte Artefakt und gleichzeitig die Grundlage für die Durchführung der nachfolgend beschriebenen, qualitativen Interviews mit denen es evaluiert wird. Der Praxisbezug der Problemstellung ergibt sich im Wesentlichen aus der einleitend beschriebenen Ausgangslage dieser Arbeit, die wissenschaftlich fundierte Abwicklung sowohl aus den Ergebnissen der Literaturstudie als auch durch die wissenschaftliche Methode in der Durchführung und Auswertung der Interviews.

1.4.3 Qualitative Expert_innen-Interviews

Ziel von qualitativen Expert_innen-Interviews ist es Wissen, Erfahrungen oder Sichtweisen von Akteuren in einem mündlichen Gespräch zu erheben, wobei der Gesprächsverlauf weniger vom Interviewer, sondern mehr vom Interviewten gesteuert und gestaltet wird. Damit sind tiefere und breitere Einblicke zum Forschungsthema möglich. (Jürgen Bortz & Nicola Döring, 1995)

Speziell interessant ist in diesem Zusammenhang die Gattung der *Experteninterviews*, in welcher die Befragten in ihrer Eigenschaft als Expert_innen, und weniger die Personen als Ganzes, im Zentrum stehen. (Hochschule Luzern, 2023)

Zusätzlich zu der Literaturrecherche und der Anforderungserhebung werden daher im Ergebnisteil dieser Arbeit qualitative Interviews mit Fachexpert_innen in der hier beschriebenen Materie durchgeführt. Diese dienen zwei Zwecken: Einerseits wird damit die Realisierbarkeit der Sicherheitsanforderungen untersucht, andererseits wird mit ihnen erhoben wie die Expert_innen in ihrem beruflichen Umfeld mit ähnlichen Anforderungen umgehen bzw. welche Anforderungen Ihnen darin begegnen. Beides dient in weiterer Folge dazu die Erwartungen an die Umsetzung von kritischen Systemen, methodisch also das im Design Science Prozess erstellte Artefakt, zu evaluieren. Seitens des Autors bestehen mehrere, persönliche Kontakte zu Personen die hierfür in Frage gekommen und um Unterstützung gebeten worden sind. Diese sind unter anderem Expert_innen im Aufbau von Einsatzleitstellensystemen, Spezialist_innen für Cybersecurity und Sicherheitsexperten in großen, österreichischen Konzernen. Wie bei der Auswahl der Personen vorgegangen wurde, welche Personen konkret interviewt wurden und wie die Ergebnisse verarbeitet wurden, wird im Kapitel 5 im Detail beschrieben und damit der Ergebnisteil dieser Arbeit eingeleitet.

Die Interviews wurden anschließend transkribiert und für deren Auswertung pseudonymisiert, sodass auf die interviewten Personen nicht mehr rückgeschlossen werden kann. Dies ermöglicht eine freie, unbefangene Meinungsäußerung.
Die inhaltliche Auswertung der Interviews folgt der *Qualitativen Inhaltsanalyse nach Mayring*, auf welche in Kapitel 5.1 noch im Detail eingegangen wird.(Franziska Pfeiffer, 2023)

2 Sicherheitsanforderungen

Um die Grundlagen für das Beantworten der Forschungsfrage zu schaffen in den nachfolgenden Kapiteln zunächst darauf eingegangen aus welchen Quellen Sicherheitsanforderungen bezogen werden können.

2.1 Standards, Referenz-Modelle und Best Practices

Typische Quellen für Sicherheitsanforderungen sind nationale und internationale Standards, Referenz-Modelle und Best Practices. Zu den bekanntesten zählen die nachfolgenden.

2.1.1 ITIL

Das *Information Technology Infrastructure Library*, kurz ITIL, wurde von der britischen Regierung in den 1980er Jahren initiiert um den Einsatz von IT-Mitteln effizient und effektiv zu gestalten. In der Zwischenzeit hat es sich als De-facto-Standard etabliert und definiert ein Rahmenwerk für die Gestaltung von IT-Prozessen. Ziel ist es ein Höchstmaß an Qualität und Kundenzufriedenheit zu erreichen, wofür die Strukturen und Prozesse der Unternehmen ganzheitlich betrachtet werden müssen und die IT schließlich als Werkzeug zur operativen Durchführung eben dieser Geschäftsprozesse dient. In seiner aktuellen Version, ITIL 4, wurde das Rahmenwerk modernisiert und neu ausgerichtet. Es soll nun insbesondere auch die agile Softwareentwicklung unterstützen und in modernen Konzepten wie DevOps eingesetzt werden können.(Axelos Ltd., o. J.; Melanie Rainer, Thomas Neuroth-Pfeiffer, Martin Latzenhofer, & Christian Focke, 2022b, S. 62; Olbrich, 2008)

Zusammenfassung:

- **Fokus:** IT-Service-Management
- **Kerninhalte:** Effiziente Bereitstellung und Unterstützung von IT-Services, Prozessoptimierung, Servicequalität.
- **Zielgruppe:** Management Ebene
- **Herausgeber**: AXELOS
- **Aktuelle Version**: ITIL 4, veröffentlicht 2019

2.1.2 COBIT

COBIT, dessen Name sich ursprünglich aus *Control Objectives for Information and Related Technology* herleitet, ist ein Rahmenwerk für die Governance und das Management von Unternehmensinformationen und -technologie und zwar in Bezug auf das Unternehmen als Ganzes und nicht bloß auf die IT-Abteilung bezogen. In der aktuellen Version, COBIT 2019, definiert es 40 Prozesse, die in Governance- und Managementprozesse unterteilt werden, wobei explizit darauf hingewiesen wird, dass diese Prozesse an die Bedürfnisse des Unternehmens angepasst werden müssen und dass COBIT weder eine vollständige Beschreibung der gesamten IT eines Unternehmens ist noch ein (IT-)technisches Rahmenwerk zur Verwaltung jedweder Technologie. Das Ziel ist es hingegen vielmehr eine optimale Abstimmung zwischen Business und IT sicherzustellen, den Wert der IT für das Unternehmen zu maximieren, der wirtschaftliche Einsatz von IT-Ressourcen und die Leistungsmessung.(ISACA, 2018a; ISACA, 2018b; Maxpert GmbH, 2024)

Zusammenfassung:

- **Fokus:** IT-Governance und Management
- **Kerninhalte:** Richtlinien und Prozesse zur Verwaltung und Steuerung der Unternehmens-IT, Risikomanagement, Compliance
- **Zielgruppe:** Management Ebene
- **Herausgeber**: ISACA
- **Aktuelle Version**: COBIT 2019, veröffentlicht 2018

2.1.3 ISO/IEC 20000

Die ISO/IEC 20000-Serie ist ein Standard für IT-Service-Management (ITSM) und definiert die Anforderungen an ein Service-Management-System. Sie ist inhaltlich also mit ITIL verwandt, orientiert sich an dessen Prozessbeschreibungen und erweitert diese. Der Standard untergliedert sich in 5 Sub-Standards ISO/IEC 20000-1 bis ISO/IEC TR 20000-5, die von den Anforderungen an ein ITSM bis zu dessen Prozessen und der Planung für seine Einführung reichen.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024b; ISO, 2018; TÜV AUSTRIA, 2024a)

Zusammenfassung:

- **Fokus:** IT-Service-Management
- **Kerninhalte:** Management von IT-Services, einschließlich ein Service-Management-System (SMS) zu etablieren, umzusetzen, zu warten und kontinuierlich zu verbessern
- **Zielgruppe:** Management Ebene
- **Herausgeber**: ISO/IEC
- **Aktuelle Version**:Edition 3, veröffentlicht 2018. Die Sub-Normen haben jeweils eine eigene Versionierung.

2.1.4 ISO/IEC 27000

Die ISO/IEC 27000-Normenreihe ist ein Set von Standards für die Umsetzung von Informationssicherheits-Managementsystemen (ISMS), das 2009 erstmals veröffentlicht und in der Zwischenzeit mehrfach novelliert worden ist. In seiner aktuellen Version besteht es aus über 10 Normen die von den Anforderungen an ISMS über allgemeine Leitfäden bis hin zu Sektor- und maßnahmenspezifischen Leitfäden reichen. Speziell hervorzuheben sind die Normen ISO/IEC 27001 und ISO/IEC 27002. Erste definiert die Anforderungen an ein ISMS, von der Planung bis zum Betrieb, sowie im sogenannten Annex A eine Aufstellung an technischen und organisatorischen Sicherheitsmaßnahmen. In der aktuell gültigen Fassung von 2022 sind das 93 Maßnahmen, die in die vier Gruppen Organisation, Personal, Infrastruktur und Technik untergliedert sind. Dieser Maßnahmenkatalog ist als erste Grundlage gedacht und versteht sich weder als vollständig noch als verpflichtend umzusetzen. Vielmehr soll jede Organisation die Maßnahmen an die eigenen Bedürfnisse anpassen. Damit das gelingt wird zunächst eine Risikoanalyse durchgeführt, welche aufzeigt in welchen Bereichen der Organisation welche Risiken bestehen, und diesen Risiken wird dann zielgerichtet und individuell mit entsprechenden Maßnahmen begegnet.(Brenner, Michael et al., 2022; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024a; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024a; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024c; ISO, 2024a; Kersten, Heinrich & Schröder, Klaus-Werner, 2023) Die ISO/IEC 27002 kann schließlich als Erweiterung des Annex A interpretiert werden, und enthält zusätzliche Empfehlungen und praxisorientierte Vorgehensweisen, welche allgemeiner Natur und auf alle Organisationen anwendbar sind.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024d)

Zusammenfassung:

- **Fokus:** Informationssicherheits-Management
- **Kerninhalte:** Aufbau und Betrieb eines ISMS, Risikobewertung, Umsetzung von Sicherheitsrichtlinien.
- **Zielgruppe:** Operative Ebene
- **Herausgeber**: ISO/IEC
- **Aktuelle Version**: Edition 5, veröffentlicht 2018. Die Sub-Normen haben jeweils eine eigene Versionierung.

2.1.5 BSI IT-Grundschutz

Der IT-Grundschutz wird vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und ist nicht nur eine Methode, sondern auch eine umfassende Anleitung, die Empfehlungen und praxisnahe Hilfestellungen zur Absicherung von Informationen bietet. Die Kernelemente bilden einerseits das BSI IT-Grundschutz Kompendium und andererseits die BSI-Standards. Sämtliche Elemente werden laufend vom BSI überarbeitet, damit das Framework den aktuellen Stand der Technik abbildet, die aktuelle Version ist die Edition 2023. Das Grundschutz Kompendium enthält neben allgemeinen Empfehlungen zur Informationssicherheit auch praktische Anleitungen, Beispiele und Checklisten, und ist in 111 Bausteine in den Kategorien Elementare Gefährdungen, Prozess-Bausteine und System-Bausteine unterteilt. Vom BSI werden zusätzlich vier Standards entwickelt und publiziert. Der Standard 200-1 definiert allgemeine Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) und ist vollständig kompatibel mit der im vorherigen Kapitel beschriebenen ISO/IEC 27001 und berücksichtigt auch die Empfehlungen der anderen ISO/IEC-Normen. Der Standard 200-2 fokussiert den praktischen Aufbau und den Betrieb eines ISMS und baut berücksichtigt ebenfalls die ISO/IEC 27001 sowie den 200-1 Standard. Der 200-3 widmet sich die Herangehensweise in der Risikoanalyse und dem Risiko-Management, und der 200-4 schließlich dem Business Continuity Management. Besonders am BSI IT-Grundschutz ist, dass im Gegensatz zu den vorgenannten Normen sämtliche Veröffentlichungen zum kostenfreien Download angeboten werden.(Bundesamt für Sicherheit in der Informationstechnik, 2023b; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024e)

Zusammenfassung:

- **Fokus:** IT-Sicherheitsmanagement
- **Kerninhalte:** Praktische Sicherheitsmaßnahmen, um grundlegende Sicherheitsanforderungen zu erfüllen. Aufbau eines ISMS, Risikomanagement und Business Continuity Management.
- **Zielgruppe:** Operative Ebene
- **Herausgeber**: BSI
- **Aktuelle Version**: Edition 2023, veröffentlicht 2023. Die Standards haben jeweils eine eigene Versionierung.

2.1.6 NIST Cybersecurity Framework

Das Cybersecurity Framework (CSF) ist ein speziell auf Cybersicherheit ausgelegtes Rahmenwerk, das von der NIST, dem US-amerikanischen National Institute of Standards and Technology, publiziert wird. In seiner aktuellen Version, dem CSF 2.0, unterscheidet es in die sechs Funktionen Steuern, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen, welche der Gruppierung der Cyberrisiken dienen. Das Framework selbst besteht wiederum aus dem CSF Core, den CSF Organizational Profiles und den den CSF Tiers. Ersteres dient dazu die einzelnen Cybersecurity-Risiken zu organisieren indem diese nach den Funktionen gegliedert und dort in Kategorien und Sub-Kategorien dargestellt werden. Zweitere werden verwendet um den Status-Quo der Organisation und das Delta zum idealen Schutzzustand zu bestimmen. Die CSF Tiers definieren schließlich das Sicherheitsniveau in dem sich die Organisation befindet. Sie reichen von der niedrigsten Stufe Tier 1: Teilweise (partial), über die Stufen Tier 2: Risikogesteuert (Risk Informed) und Tier 3: Wiederholbar (Repeatable) bis zur höchsten Stufe Tier 4: Anpassungsfähig (Adaptive), in der die Organisation sehr gut vorbereitet ist und sich an neue Bedrohungen schnell anpassen kann.(NIST, 2024a; NIST, 2024b)

Zusammenfassung:

- **Fokus:** Cybersicherheitsmanagement
- **Kerninhalte:** Identifizieren, Schützen, Erkennen von Cybersicherheitsrisiken, Reagieren und Wiederherstellen
- **Zielgruppe:** Operative Ebene
- **Herausgeber**: NIST
- **Aktuelle Version**: CSF 2.0, veröffentlicht 2024

2.1.7 CIS Controls

Die CIS Controls sind eine Sammlung von Best Practices zur Cybersecurity, die vom Center for Internet Security (CIS), einer gemeinnützigen, community-getriebenen Organisation, entwickelt und publiziert werden. In seiner aktuellen Version, der V8.1, werden 18 Steuerungselemente angeführt, die eine priorisierte Sammlung von Schutzmaßnahmen darstellen, um den am häufigsten vorkommenden Cyberangriffen zu begegnen. Die Maßnahmen selbst sind sehr konkret und entwicklungsnahe, sie können also unmittelbar umgesetzt werden. Dabei können die Maßnahmen in Form einer Excel-Tabelle heruntergeladen werden und werden darin, zur gezielteren Anwendung, auch noch in sogenannte Implementation Groups unterschieden. Diese reichen von IG1, die minimale technische Expertise erfordert und für Organisationen mit geringem Risikoprofil geeignet ist, über IG2, einer mittleren Stufe, bis zur IG3, für welches ein hohes Maß an technischer Expertise und Ressourcen erforderlich ist und die sich an Organisationen mit hohem Risikoprofil richten.(CIS, 2024a; CIS, 2024b; CIS, 2024c)

Zusammenfassung:

- **Fokus:** Praktische IT-Sicherheits-Steuerungselemente
- **Kerninhalte:** Konkrete, priorisierte Sicherheitsmaßnahmen zur Verteidigung gegen häufige Cyberangriffe
- **Zielgruppe:** Technische Ebene
- **Herausgeber**: CIS
- **Aktuelle Version:** V8.1, veröffentlicht 2024

2.1.8 OWASP Top 10

Die OWASP Top 10 sind eine Aufstellung der größten Gefährdungen für Web-Anwendungen, welche von dem Open Web Application Security Project, einer community-getriebenen Non-Profit-Organisation, zusammengestellt und veröffentlicht werden. Sie listet die 10 bedeutsamsten Risiken, jeweils nach ihrem Schweregrad sortiert, und beschreibt für jedes davon konkret umsetzbare Schutzmaßnahmen auf Softwareentwicklungs-Niveau. In der aktuellen Version 2021 sind das die Risiken:

1. **Broken Access Control**: Fehler in der Zugriffskontrolle
2. **Cryptographic Failures**: Schwachstellen in der Verschlüsselung von Daten und Datentransfers
3. **Injection**: Einschleusen und ausführen von schadhaftem Code

4. **Insecure Design**: Risiken im Zusammenhang mit Design- und Architekturfehlern.
5. **Security Misconfiguration**: Fehler bei der Konfiguration von Sicherheitsmaßnahmen
6. **Vulnerable and Outdated Components**: Unzureichendes Einspielen von Updates, Upgrades, Patches
7. **Identification and Authentication Failures**: Schwachstellen in Verbindung mit Anmeldungen und Authentifizierungen
8. **Software and Data Integrity Failures**: Verwenden von Code-Bestandteilen aus nicht vertrauenswürdigen Quellen
9. **Security Logging and Monitoring Failures**: Unzureichendes Logging & Montitoring und daher keine Möglichkeit Sicherheitsverletzung zu erkennen und darauf zu reagieren
10. **Server-Side Request Forgery (SSRF)**: Abrufen von entfernten Ressourcen ohne sie ausreichend zu validieren
    (Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024f; Myra Security GmbH, 2024; OWASP Foundation, o. J.; OWASP Foundation, 2024a; OWASP Foundation, 2024b)

Zusammenfassung:

- **Fokus:** Sicherheit von Webanwendungen
- **Kerninhalte:** Sicherheitsrichtlinien und Tools zur Erkennung und Vermeidung von Sicherheitslücken in Webanwendungen, spezifisch für Entwickler.
- **Zielgruppe:** Technische Ebene
- **Herausgeber**: OWASP
- **Aktuelle Version:** 2021

2.1.9 Vielfalt und Vielschichtigkeit

Die vorangegangenen Kapitel zeigen, dass es im Bereich der Informationssicherheit viele, unterschiedliche Standards, Referenz-Modelle und Best Practices gibt, und die hier angeführte Aufstellung ist auch lediglich exemplarisch zu sehen und bei weitem nicht vollständig. Neben den bereits erwähnten gibt es etwa von der ISO unter anderem mit der ISO 31000, die sich mit Risikomanagement beschäftigt, oder der ISO 22301, welche sich

um Business Continuity Management (BCM) dreht, noch einige weitere Normen, die Anforderungen an die Informationssicherheit stellen.(ISO, 2024b; ISO, 2024c)

Diese Vielfalt unterstreicht auch die Risk Management Standards Darstellung der European Union Agency for Cyber Security (ENISA), welche einige weitere Standards anführt die sich alle mit dem Thema Risikomanagement beschäftigen.(ENISA, 2022)

Daneben gibt es Sicherheits-Standards, die kombiniert werden können, wie das etwa bei der ISO/IEC 27001 der Fall ist, welche auch auf Basis des BSI IT-Grundschutzes zertifiziert werden kann.(Bundesamt für Sicherheit in der Informationstechnik, 2024b)

Und darüber hinaus gibt es etliche auf bestimmte Bereiche spezialisierte Normen, wie etwa das Hochverfügbarkeits-Kompendium des BSI, sowie viele branchenspezifische Standards, wie die umfangreiche Auflistung des österreichischen Bundeskanzleramts zu den Standards für Telekom-Betreiber belegt.(Bundesamt für Sicherheit in der Informationstechnik, 2024c; Bundeskanzleramt, 2024a)

Neben der bloßen Vielfalt an Normen und Standards sind diese auch vielschichtig in Bezug auf die Zielgruppen an die sie sich richten. Diese reichen vom Management-Level, welches von Standards wie ITIL und COBIT hauptsächlich adressiert wird, über das operative Level, welches von der ISO/IEC 27000, dem BSI IT-Grundschutz oder dem NIST Cybersecurity Framework angesprochen wird, bis hin zum technischen Level, an welches sich etwa die CIS Controls oder die OWASP Top 10 primär richten. Um zu entscheiden welche Normen für ein Thema herangezogen werden muss also auch nach der Zielgruppe unterschieden werden.

2.1.10 Problematik

Aufgrund der Fülle an Normen und Standards stellt sich für eine konkrete Aufgabenstellung die Frage auf welches der Modelle zurückgegriffen werden soll. Die meisten Standards bestehen aus einer Vielzahl von Anforderungen die auf mehreren Hundert Seiten beschrieben stehen, daher ist es schwierig festzustellen wo es zwischen den Normen Unterschiede, Überschneidungen oder auch Widersprüche gibt. Entsprechend kompliziert gestaltet es sich die einzelnen Standards und Modelle gegeneinander abzuwägen sowie die Übersicht zu bewahren und auf dem neuesten Stand zu bleiben.

Im Kontext dieser Arbeit ist es daher nicht möglich eine einfache, taxative Aufstellung an Sicherheitsanforderungen zu erstellen und diese dann zu überprüfen. Stattdessen braucht

es ein anderes Konzept und einen zusätzlichen Input um zu definieren welche Sicherheitsanforderungen für kritische Systeme erwartet werden können, und um diese Brücke zu schlagen wird die NIS Richtlinie, und deren österreichische Umsetzung, herangezogen.

2.2 NIS-Richtlinie und Umsetzung in Österreich

Die Richtlinie (EU) 2016/1148, die sogenannte NIS-Richtlinie, verfolgt das Ziel Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der gesamten Europäischen Union umzusetzen. Lt. Richtlinie ist dies nötig, da einerseits Netz- und Informationssysteme mit ihren zugehörigen Diensten eine zunehmend zentrale Rolle für die Gesellschaft und für das Funktionieren des Binnenmarktes spielen und andererseits die Tragweite, die Häufigkeit und die Auswirkungen von Sicherheitsvorfällen zunehmen. Die NIS-Richtlinie definiert daher unter anderem, dass jeder Mitgliedsstaat

- die in seinem Land angesiedelten Betreiber wesentlicher Dienste in bestimmten Sektoren identifizieren muss,
- sicherstellt, dass diese Betreiber wesentlicher Dienste geeignete technische und operative Maßnahmen umsetzen um die Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten
- definiert welche Sicherheitsanforderungen bestehen und wie Sicherheitsvorfälle gemeldet werden müssen
- Computer-Notfallteams etabliert, sogenannte Computer Security Incident Response Teams (CSIRTs), welche die nationalen Sicherheitsvorfälle überwachen, darauf entsprechend reagieren, sich mit den CSIRTS der anderen Mitgliedsstaaten zu einem Netzwerk zusammenschließen und mit ihnen kooperieren.

Die NIS-Richtlinie wurde schließlich am 6. Juli 2016 vom Europäischen Parlament und dem Europäischen Rat beschlossen, ist am 8. August 2016 in Kraft getreten und in weiterer Folge in einzelne, nationale Gesetze der Mitgliedsstaaten überführt.(Bundeskanzleramt, 2018; Europäisches Parlament & Europäische Kommission, 2016)

2.2.1 NIS-Gesetz, NISG

In Österreich wurde die NIS-Richtlinie mit 28. Dezember 2018 mit dem NIS-Gesetz (Netz- und Informationssystemsicherheitsgesetz, NISG) umgesetzt und somit in österreichisches Recht überführt.(Bundeskanzleramt & Bundesministerium für Inneres, 2024a)

Es erfüllt die Vorgaben der NIS-Richtlinie indem es unter anderem

- Die Sektoren benennt, in denen das NIS-Gesetz Anwendung findet
- Kriterien zur Bestimmung der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste definiert
- Computer-Notfallteams festlegt
- Meldepflichten für Sicherheitsvorfälle vorgibt
- Strafmaße bei Nicht-Einhaltung festsetzt

Konkrete Sicherheitsanforderungen definiert das NIS-Gesetz allerdings nicht. Im Paragraf §17, Absatz 1 definiert es diese lediglich auf allgemeine Art und Weise: „Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.“ (NISG, §17 (1))

2.2.2 NIS-Verordnung, NISV

Aufgrund der generischen Definition im NIS-Gesetz sind für eine technische Umsetzung von konkreten Maßnahmen zusätzliche, detailliertere Anforderungen erforderlich, und diese werden in der österreichischen Umsetzung der NIS-Richtlinie in der NIS-Verordnung (NISV) definiert, einer Verordnung des Bundesministers für EU, Kunst, Kultur und Medien. Diese präzisiert einerseits den Geltungsbereich des NIS-Gesetzes indem sie für jeden im Gesetz genannten Sektor die wesentlichen Dienste definiert. Im Sektor Digitale Infrastruktur sind das etwa ausschließlich Dienste, die mit dem Domain Name Service (DNS) zu tun haben. Konkret wird hier der Betrieb von DNS-Resolvern, von autoritativen DNS-Servern und von einer TLD-Name-Registry angeführt. Und im Sektor Gesundheitswesen wird etwa der Betrieb von Leitstellen zur Durchführung von Notfallrettungstransporten genannt, nicht aber der von Leitstellen im Bereich des

Katastrophenschutzes. (Bundeskanzleramt, 2024b; Bundeskanzleramt & Bundesministerium für Inneres, 2024a)

Zusätzlich zu der Präzisierung der wesentlichen Dienste enthält die NIS-Verordnung im 3. Abschnitt, §11 (1) andererseits eine Detaillierung der Sicherheitsvorkehrungen im Sinne des oben beschriebenen NISG, §17 (1) und geht auf diese in seiner Anlage 1 noch weiter ein. Konkret werden hier 11 Kategorien von Sicherheitsmaßnahmen genannt, die jeweils in 1-6 Sub-Kategorien untergliedert sind. Die Tabelle unterhalb stellt diese dar.(Bundeskanzleramt, 2024b)

Sicherheitsmaßnahmen	
1	**Governance und Risikomanagement**
1.1	Risikoanalyse: Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.
1.2	Sicherheitsrichtlinie: Eine Sicherheitsrichtlinie ist zu erstellen und periodisch zu aktualisieren.
1.3	Überprüfungsplan der Netz- und Informationssysteme: Die Durchführung der periodischen Überprüfung der Netz- und Informationssystemsicherheit ist zu planen und festzulegen.
1.4	Ressourcenmanagement: Alle Ressourcen, die erforderlich sind, um die Funktionsfähigkeit der Netz- und Informationssysteme zu gewährleisten, sind im Hinblick auf kurz-, mittel- und langfristige Kapazitätsanforderungen einzuplanen und sicherzustellen.
1.5	Informationssicherheitsmanagementsystemprüfung: Die periodische Überprüfung des Informationssicherheitsmanagementsystems ist festzulegen und durchzuführen.
1.6	Personalwesen: Sicherheitsrelevante Aspekte sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen

2	**Umgang mit Dienstleistern, Lieferanten und Dritten**
2.1	Beziehungen mit Dienstleistern, Lieferanten und Dritten: Anforderungen an Dienstleistern, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.
2.2	Leistungsvereinbarungen mit Dienstleistern und Lieferanten: Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.
3	**Sicherheitsarchitektur**
3.1	Systemkonfiguration: Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguratoin ist strukturiert zu dokumentieren. Die Dokumentation ist aktuell zu halten.
3.2	Vermögenswerte: Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, sind strukturiert zu analysieren und zu dokumentieren.
3.3	Netzwerksegmentierung: Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.
3.4	Netzwerksicherheit: Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten.
3.5	Kryptographie: Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.
4	**Systemadministration**
4.1	Administrative Zugangsrechte: Administrative Zugangsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.

4.2	Systeme und Anwendungen zur Systemadministration: Systeme und Anwendungen zur Systemadministration sind ausschließlich für Tätigkeiten zum Zweck der Systemadministration zu verwenden. Die Sicherheit dieser Systeme und Anwendungen ist zu gewährleisten.
5	**Identitäts- und Zugriffsmanagement**
5.1	Identifikation und Authentifikation: Es sind Verfahren umzusetzen und Technologien einzusetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten
5.2	Autorisierung: Es sind Verfahren umzusetzen und Technologien einzusetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden.
6	**Systemwartung und Betrieb**
6.1	Systemwartung und Betrieb: Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen
6.2	Fernzugriff: Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.
7	**Physische Sicherheit**
7.1	Physische Sicherheit: Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.
8	**Erkennung von Vorfällen**
8.1	Erkennung: Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.
8.2	Protokollierung und Monitoring: Mechanismen zu Protokollierung und Monitoring, insbesondere von für die

	Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.
8.3	Korrelation und Analyse: Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen.
9	**Bewältigung von Vorfällen**
9.1	Vorfallsreaktion: Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.
9.2	Vorfallsmeldung: Prozesse zur internen und externen Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.
9.3	Vorfallsanalyse: Prozesse zur Analyse und Bewertung von Vorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.
10	**Betriebskontinuität**
10.1	Betriebskontinuitätsmanagement: Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.
10.2	Notfallmanagement: Notfallpläne sind zu erstellen, anzuwenden, regelmäßig zu bewerten und zu erproben.
11	**Krisenmanagement**
11.1	Krisenmanagement: Rahmenbedingungen und Prozessabläufe des Krisenmanagements sind für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen und zu erproben.

Tabelle 1: Anlage 1 der NIS-Verordnung (Bundeskanzleramt, 2024b)

In Bezug auf die Aufgabenstellung dieser Arbeit sind aus diesem Katalog allen voran die Kategorien 3 - 7 besonders relevant, aber auch die anderen enthalten wichtige Aspekte wie die periodischen Überprüfungen und Vorbereiten auf etwaige Ausnahmesituationen.

2.2.3 NIS-Factsheets

Das österreichische Bundeskanzleramt hat gemeinsam mit dem Bundesministerium für Inneres mit der *Anlaufstelle Netz- und Informationssicherheitsgesetz (NISG)* ein eigenes Online-Portal eingerichtet um über die Inhalte des NIS-Gesetzes zu informieren, Fragen dazu zu beantworten und es mit zusätzlichen Inhalten klarer zu gestalten. Neben FAQs, Verlinkungen zu den Gesetzestexten und weiteren Informationen finden sich darauf auch eigens zum besseren Verständnis des NIS-Gesetzes und der NIS-Verordnung entwickelte Fact Sheets. So enthält dieses Portal auch ein eigenes Fact Sheet in Bezug auf die oberhalb beschriebene Anlage 1 zur NIS-Verordnung, das Fact Sheet 9/2022. Dieses Dokument mit dem Titel *Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste* hat zum Ziel die Sicherheitsmaßnahmen dieser Anlage 1 näher zu erläutern, um Betreiber wesentlicher Dienste dabei zu unterstützen sie umzusetzen.(Bundeskanzleramt & Bundesministerium für Inneres, 2024b; Bundeskanzleramt & Bundesministerium für Inneres, 2022)

In dem NIS Fact Sheet 9/2022 wird jede der 11 Kategorien mitsamt ihrer Sub-Kategorien konkretisiert und genauer abgegrenzt. Insbesondere werden darin jeweils auch nationale und internationale Informationssicherheitsstandards referenziert, welche als Beispiel für die konkrete, technische Umsetzung herangezogen werden können. Auf zwei der angegebenen Standards und Best Practices ist oberhalb bereits kurz eingegangen worden, und zwar auf die ISO/IEC 27000 und auf die CIS Controls. Das Fact Sheet referenziert aber auch weitere, auf die in den nachfolgenden Kapiteln kurz eingegangen wird. Diese sind:

- Das österreichische Sicherheitshandbuch
- Die ÖNORM A7700
- Die IEC 62443 und
- Die EN 50600

2.2.4 Österreichisches Sicherheitshandbuch

Das österreichische Sicherheitshandbuch wird vom österreichischen Bundeskanzleramt (BKA) und dem Zentrum für sichere Informationstechnologie - Austria (A-SIT) entwickelt und positioniert sich nach eigenen Angaben zwischen der ISO/IEC 27001/270002 und dem BSI IT-Grundschutz und dessen Bausteinen. In seiner aktuellen Version, der Version 4.4, wurde diesem Umstand speziell Rechnung getragen indem die Struktur des Dokuments nach jener der ISO/IEC 27001 und 27002 ausgerichtet wurde um die Integration mit ISMS, die nach diesen Standards aufgebaut sind, zu vereinfachen. Inhaltlich gliedert sich das Sicherheitshandbuch in 18 Abschnitte, wobei die Abschnitte 4-18 konkrete Sicherheitsmaßnahmen inklusive ihrer Umsetzung beschreiben. Darüber hinaus enthält es mehrere Anhänge, die sich jeweils speziellen Aspekten der Informationssicherheit im Detail widmen. Hauptzielgruppe des Dokuments sind Großunternehmen und Behörden, das Sicherheitshandbuch ist aber auch für kleine und mittlere Unternehmen (KMU), Ein-Personen-Unternehmen (EPU) und sogar für Privatpersonen konzipiert. In Kapitel 1.3.3.1 wird hierfür ein Überblick gegeben und dargestellt welcher der Abschnitte und Anhänge für welche Zielgruppe tauglich ist. Besonders an dem Sicherheitshandbuch ist, dass sowohl als PDF-Version als auch als eigene Webseite existiert und beides frei zugänglich ist.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023b)

Zusammenfassung:

- **Fokus:** IT-Sicherheitsmanagement
- **Kerninhalte:** Praktische Sicherheitsmaßnahmen, um grundlegende Sicherheitsanforderungen zu erfüllen.
- **Zielgruppe:** Operative Ebene
- **Herausgeber**: BKA und A-SIT
- **Aktuelle Version**: Version 4.4, veröffentlicht 2023

2.2.5 ÖNORM A7700

Die ÖNORM A7700 Sichere Webapplikationen wird von der Austrian Standards International herausgegeben und definiert Anforderungen an die Sicherheit und den sicheren Betrieb von Webapplikationen. Sie wurde 2019 grundlegend überarbeitet und gliedert sich nun in folgende vier Teile:

- A 7700-1: Begriffe
- A 7700-2: Anforderungen durch Datenschutz
- A 7700-3: Sicherheitstechnische Anforderungen
- A 7700-4: Anforderungen an den sicheren Betrieb

Die ÖNORM richtet sich inhaltlich sowohl an Programmierer als auch an Software-Einkäufer und soll für diese als Leitfaden dienen.(Austrian Standards International, 2024; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2024g)

Zusammenfassung:

- **Fokus:** Sicherheit von Webanwendungen
- **Kerninhalte:** Sicherheitsanforderungen für Entwicklung und Betrieb von Webapplikationen
- **Zielgruppe:** Operative/Technische Ebene
- **Herausgeber**: Austrian Standards International
- **Aktuelle Version**: A 7700:2019, veröffentlicht 2019

2.2.6 IEC 62443

Die IEC 62443 ist eine Normenreihe für Cybersecurity in der Industrieautomatisierung die von der International Eletrotechnical Commission (IEC) herausgegeben wird. Die Serie besteht aus vier Teilen, die ihrerseits wiederum aus neun Standards, technischen Reports (TR) und technischen Spezifikationen (TS) besteht. Fokus der Normenreihe ist die Absicherung von sogenannten *Industrial Automation and Control Systems* (IACS), also von Steuerungssystemen in der Industrie, wobei diese in einer breiten Anzahl von Sektoren vorkommen. Maschinen- und Anlagenbau sind hier also ebenso adressiert wie zum Beispiel die Energieversorgung. Die IEC 62443 ist themenverwandt mit der ISO/IEC 27000 Serie, während die ISO/IEC 27000 aber auf IT-Systeme abzielt setzt die IEC 62443 hingegen einen Schwerpunkt auf Operational Technology (OT-)Systeme. Dies ist nicht zwangsläufig ein Widerspruch, aber für OT-Systeme gelten unterschiedliche Rahmenbedingungen wie andere Performance- oder Verfügbarkeitsanforderungen, längere Lebenszyklen oder das Zusammenspiel mit physikalischen Prozessen, und darauf nimmt die IEC 62443 Rücksicht.(International Eletrotechnical Commission, 2024; TÜV AUSTRIA, 2024b; VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., 2024)

Zusammenfassung:

- **Fokus:** Cybersecurity in der Industrieautomatisierung
- **Kerninhalte:** Cybersicherheit von Industrial Automation and Control Systems, Risikoanalyse und -management
- **Zielgruppe:** Operative /Technische Ebene
- **Herausgeber**: IEC
- **Aktuelle Version**: Unterschiedlich je Teil

2.2.7 EN 50600

Die EN 50600 ist eine Europäische Norm die vom *European Electrotechnical Committee for Standardization* (CENELEC) herausgegeben wird und sich mit dem sicheren Aufbau von Rechenzentren befasst. Die Norm ist in vier Teile unterteilt, wobei der erste Teil die allgemeinen Konzepte beschreibt, der zweite das Design von Rechenzentren, der dritte den Betrieb von Rechenzentren und der vierte messbare Kenngrößen (KPIs). Inhaltlich deckt die Norm ein breites Spektrum ab und reicht von der physischen Gebäudekonstruktion über die Stromversorgung und Energieeffizienz bis zur Definition von Verfügbarkeitsklassen und den Prozessen zum Management und Betrieb von Rechenzentren.(TÜV SÜD AG, 2024; VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., 2019)

Zusammenfassung:

- **Fokus:** Sicherer Aufbau von Rechenzentren
- **Kerninhalte:** Anforderungen und Empfehlungen für Planung, Bau und Betrieb von Rechenzentren
- **Zielgruppe:** Operative /Technische Ebene
- **Herausgeber**: CENELEC
- **Aktuelle Version**: Unterschiedlich je Teil

2.3 Security by Design

In den vorangegangenen Kapiteln wurde das Augenmerk auf konkrete, bereits ausdefinierte Sicherheitsmaßnahmen gelegt die in verschiedenen Standards und Best Practices beschrieben sind. Allerdings besteht beim ausschließlichen Verlassen auf bekannte Maßnahmen das Risiko neuen Bedrohungen immer ein Stück hinterher zu sein. Das liegt daran, dass laufend neue Bedrohungen entstehen, die dann wiederum neuer

Maßnahmen bedürfen, die erst umgesetzt werden müssen um die Bedrohungen abzuwenden. Ein Problem das in den Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen mit dem Spiel von Hase und Igel verglichen wird und um diesem entgegen zu wirken empfehlen sie die Umsetzung eines zusätzlichen Paradigmas, dem sogenannten *Security by Design*.(Ulrike Lechner et al., 2018, S. 220ff)

Unter Security by Design wird der methodische Ansatz verstanden die Anforderungen der Informationssicherheit von Anfang an in der Konzeption von Produkten und Systemen mit zu berücksichtigen anstatt sich zunächst nur auf funktionale Aspekte zu konzentrieren und Security erst im Nachgang umzusetzen. Dabei kann man Security by Design im engeren und im weiteren Sinne interpretieren. Im engeren Sinn bezeichnet es das Antizipieren und Behandeln von Sicherheitsrisiken im Zuge des Softwareentwicklungsprozesses, also deren Berücksichtigung in der technischen Entwicklung. Im weiter gefassten Sinn bedeutet es die Sicherheitsaspekte in der gesamten Organisation und ihren Prozessen zu verankern und im gesamten Lebenszyklus der Systeme zu berücksichtigen. Damit soll das Ziel erreicht werden Sicherheitslücken zu vermeiden oder zumindest zu reduzieren, sowie die Systeme widerstandsfähiger und robuster zu machen.(Lunkeit & Zimmer, 2021, S. 8; Waidner, Backes & Müller-Quade, 2013, S. 4)

Beispiele aus der Vergangenheit in denen Security by Design nicht umgesetzt wurde und die in diesem Kontext daher gerne als Anti-Beispiele herangezogen werden sind etwa

- die alten Internetprotokolle aus den Frühzeiten des Internets, bei deren Entwurf Sicherheitsaspekte nicht bedacht und somit vernachlässigt wurden und die teilweise immer noch verwendet werden, oder
- Produkte im IoT-Bereich, bei denen Sicherheitsanforderungen häufig in den ersten Versionen ausgeklammert und erst nachträglich ergänzt wurden.

Zweiteres passierte etwa aus Kostengründen oder um eine rasche Markteinführung zu erreichen. Besonders häufig waren hiervon Überwachungskameras betroffen, aber auch Router, Smart Home Geräte und viele mehr. Diese Probleme haben unter anderem dazu geführt, dass mit der ETSI EN 303 645 in der Zwischenzeit auch eine eigene Europäische Norm für Cyber Security im Consumer IoT Bereich entwickelt wurde. (Bundesamt für Sicherheit in der Informationstechnik, 2017a; Bundesamt für Sicherheit in der Informationstechnik, 2024d; F-Secure Deutschland, 2019)

Die Maßnahmen zur Umsetzung von Security by Design sind vielseitig und reichen von technischen bis zu organisatorischen. Zu den technischen zählt etwa die Härtung der Systeme, der Einsatz kryptografischer Verfahren, die Implementierung sicherer Default-Werte oder eine vollständige Mediation, bei der jeder Objektzugriff auf Zulässigkeit geprüft wird. Zu den organisatorischen zählt unter anderem die Vergabe von minimalen Privilegien und minimalen Autorisierungen, das Auditieren von Zugriffen aber auch das kontinuierliche Testing der Sicherheit.(Luber & Schmitz, 2021; Lunkeit & Zimmer, 2021)

Security by Design fordert also die Berücksichtigung von Sicherheitsaspekten von der initialen Konzeption weg. Der Themenband Resilienz greift nun dieses Konzept auf, geht einen Schritt weiter und führt es zu dem Ansatz der sogenannten *Resilience by Design*, für welchen die Ansätze des Security by Design eine Voraussetzung sind. In diesem Ansatz geht um die Fähigkeit zur Regeneration oder Selbstheilung. Es geht also darum Systeme so zu entwerfen, dass sie Ausnahmesituationen wie Angriffe oder (Teil-)Ausfälle aushalten, sich davon erholen und sich anpassen können. Um das zu erreichen müssen mögliche Probleme im Vorfeld antizipiert und bereits von der Konzeption an in das Design der Systeme einfließen, anstatt nur auf Probleme zu reagieren, wenn sie auftreten. Der Themenband schließt schließlich damit und weist darauf hin, dass Resilienz ein gesamtsystemisches Denken, Planen und Handeln bedeutet, aber Resilienz bedeutet auch neben technischen und organisatorischen Aspekten auch gesellschaftliche Fragen zu berücksichtigen.(Volker Wittpahl, 2023)

3 Umsetzung von Sicherheitsanforderungen

Im vorangegangenen Kapitel wurde beleuchtet aus welchen Quellen und Ansätzen Sicherheitsanforderungen abgeleitet werden können und welche Problemstellungen aufgrund deren Vielzahl entstehen. Dieses Kapitel baut nun darauf auf und ist jenen Aspekten und Fragestellungen gewidmet, die sich während der praktischen Umsetzung ergeben.

3.1 Risikomanagement

Der Umsetzung von Sicherheitsmaßnahmen liegt häufig ein Risikomanagement zugrunde, welches sich in die Bereiche Risikoanalyse und Risikobehandlung unterteilt. Erstere dient dazu die Risiken zu identifizieren, zweitere sie strukturiert zu mitigieren.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)

3.1.1 Risikoanalyse

Der oben bereits zitierte §17 des NIS-Gesetzes hält fest, dass die umzusetzenden Sicherheitsvorkehrungen nicht nur dem Stand der Technik entsprechen, sondern auch dem festgestellten Risiko angemessen sein müssen. Es wird also ein risikobasierter Ansatz verlangt. Die NIS-Vorordnung verfeinert diese Definition und ergänzt in §11 (2), dass eine sog. Risikoanalyse durchgeführt werden muss, so wie sie in Punkt 1.1 ihres Anhang 1 beschrieben ist. Zu dieser wiederum detailliert das NIS-Factsheet, dass damit einerseits erhoben werden soll, welche Netz- und Informationssysteme für die wesentlichen Dienste des Betreibers nötig sind und andererseits welchen Risiken diese ausgesetzt sind. Für die Umsetzung empfiehlt es an oberster Stelle die Risikoanalyse nach der im österreichischen Sicherheitshandbuch beschriebenen Methode durchzuführen.(Bundeskanzleramt, 2024c; Bundeskanzleramt, 2024b; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, o. J.)

Das österreichische Sicherheitshandbuch beschreibt die Risikoanalyse in Kapitel 5.1 und hält dazu einleitend fest, dass es diese aus dem oben beschrieben BSI IT-Grundschutz, konkret dem BSI Standard 200-2, übernommen hat. Dieser unterscheidet 3 Arten von Risikoanalyse:

1. Grundschutzansatz
2. Detaillierte Risikoanalyse

3. Kombinierter Ansatz

Die erste Methode beschreibt eine einfache, leichtgewichtige Risikoanalyse die den Vorteil hat, dass sie ressourcenschonender und entsprechend einfacher umsetzbar ist. Die zweite definiert eine detaillierte Risikoanalyse, die präziser und zielgerichteter ist, aber wesentlich mehr Zeit und Ressourcen benötigt. Die dritte ist eine Mischung der ersten beiden. Mit ihr wird zunächst über einen Kriterienkatalog festgestellt welche Anwendungen welchen Schutzbedarf haben und definiert schließlich, dass Anwendungen mit niedrigem bis mittleren bzw. normalem Schutzbedarf mit dem Grundschutzansatz analysiert werden und jene mit hohem bis sehr hohem mit der detaillierten Risikoanalyse. Für kritische Systeme empfiehlt es entsprechend eine detaillierte Risikoanalyse.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)

Den Prozess zur Durchführung einer detaillierten Risikoanalyse definiert das Sicherheitshandbuch wie nachfolgend in Abbildung 3 dargestellt:

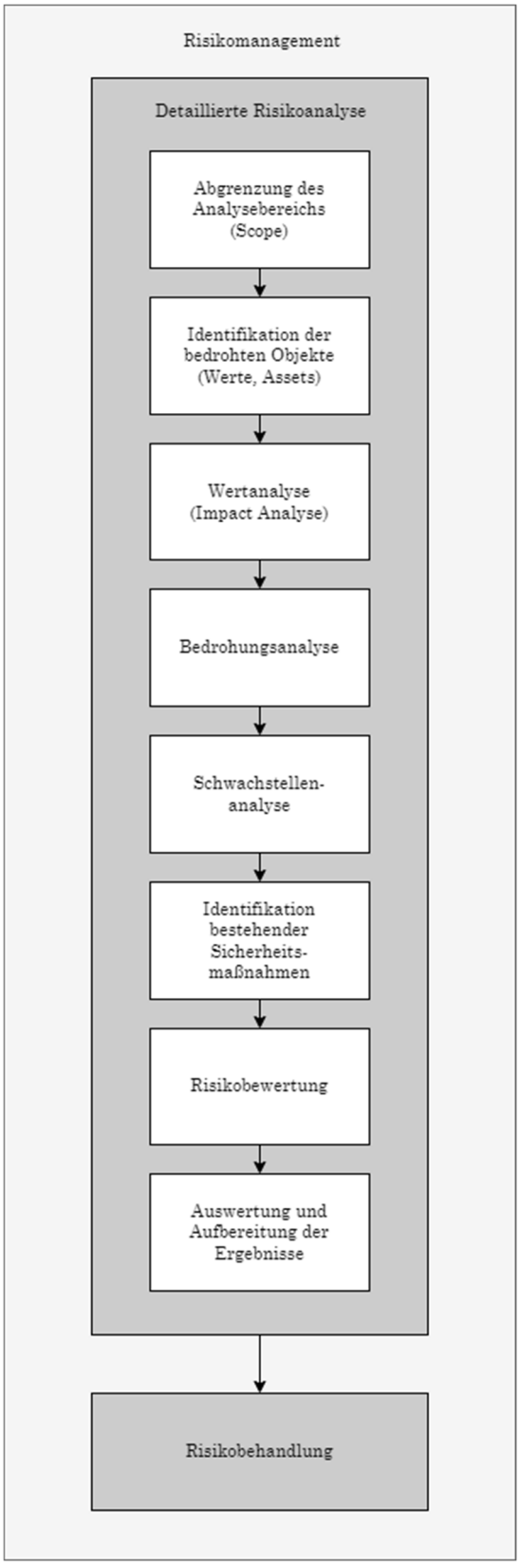

Abbildung 3: Detaillierte Risikoanalyse lt. österreichischem Sicherheitshandbuch (angelehnt an Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)

Es sieht also vor zunächst den Geltungsbereich der Analyse abzugrenzen und festzustellen welche bedrohten Objekte es darin gibt sowie welchen Wert diese besitzen.

Danach wird festgestellt welchen Bedrohungen diese Objekte ausgesetzt sind und über welche Schwachstellen sie schlagend werden könnten. Abschließend wird unter Beachtung der bereits umgesetzten Schutzmaßnahmen festgestellt welche Risiken für die Objekte bestehen und diese Ergebnisse ausgewertet und aufbereitet.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)

Für die so identifizierten Risiken kann schließlich die erwartete Schadenshöhe berechnet werden, welche dem Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe entspricht. Risiken mit höherer erwarteter Schadenshöhe sind demnach dringender zu behandeln als jene mit geringerer.(Bundesamt für Sicherheit in der Informationstechnik, 2017b, S. 44)

Alternativ können die Risiken auch in Form einer Risikomatrix veranschaulicht und gruppiert werden. Hierzu werden die Risiken in Eintrittshäufigkeit und Schadenshöhe bemessen und in Matrixform dargestellt, wobei das BSI für die Bewertung von Häufigkeiten und Schadensauswirkungen empfiehlt auf folgende Klassifikationen zurückzugreifen (Bundesamt für Sicherheit in der Informationstechnik, 2024e):

Häufigkeiten:

- Selten: Höchstens alle 5 Jahre
- Mittel: Alle 5 Jahre bis einmal pro Jahr
- Häufig: Einmal pro Jahr bis einmal pro Monat
- Sehr häufig: Mehrmals pro Monat

Schadensauswirkungen:

- Vernachlässigbar: Geringe Auswirkungen die vernachlässigt werden können
- Begrenzt: Auswirkungen sind überschaubar
- Beträchtlich: Auswirkungen können beträchtlich sein
- Existenzbedrohend: Auswirkungen können katastrophal oder gar existenzbedrohend sein

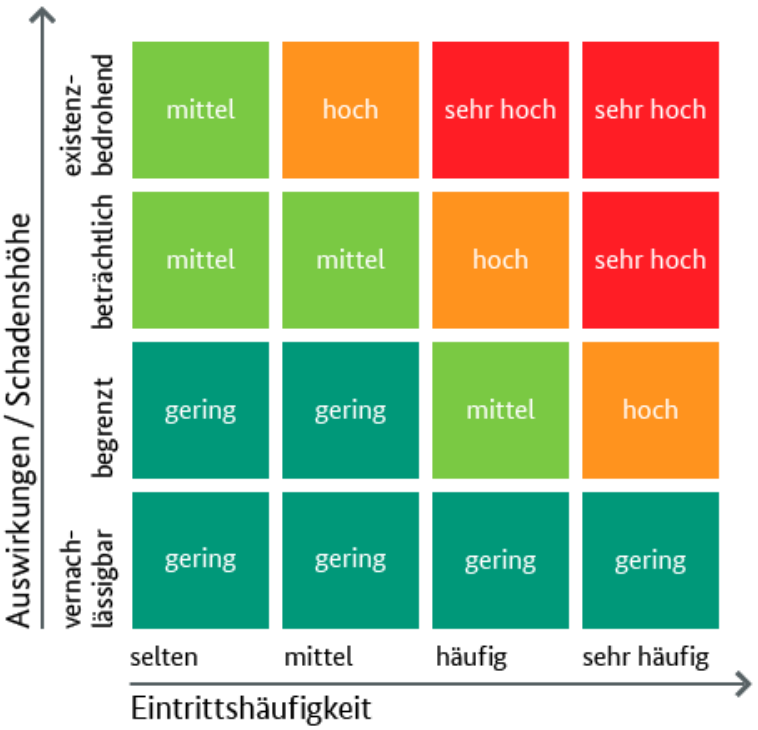

Abbildung 4: Risikomatrix nach BSI 200-3 (Bundesamt für Sicherheit in der Informationstechnik, 2024e)

3.1.2 Risikobehandlung

In der Behandlung von Risiken orientiert sich das österreichische Sicherheitshandbuch erneut am BSI IT-Grundschutz, konkret am BSI-Standard 200-3, sowie an der ISO/IEC 27005. Darin werden folgende vier grundsätzliche Strategien für den Umgang mit Risiken angeführt:

- Risikovermeidung: Etwas wird am Objekt verändert sodass das Risiko nicht mehr besteht
- Risikominimierung: Eine technische und/oder organisatorische Maßnahme wird ergriffen um die Auswirkung des Risikos zu reduzieren
- Risikotransfer: Das Risiko wird auf einen Dritten übertragen
- Risikoakzeptanz: Das Risiko wird in Kauf genommen

In den ersten beiden Strategien werden konkrete Maßnahmen umgesetzt, um den Risiken zu begegnen, und diese untergliedert das Sicherheitshandbuch in:

- Präventive Maßnahmen: Das Risiko tritt nicht/seltener ein
- Detektierende Maßnahmen: Der Eintritt eines Risikos wird erkannt
- Korrigierende Maßnahmen: Die Auswirkungen eines eingetretenen Risikos werden reduziert

Für die auf diese Art festgelegten Maßnahmen wird schließlich die Umsetzung geplant und durchgeführt bzw. werden durch das Management etwaige, transparent gemachte Restrisiken bewusst akzeptiert.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)

3.1.3 Kritik

Obwohl der Risikomanagement-Ansatz sehr strukturiert und gut durchdacht ist darf nicht außer Acht gelassen werden, dass einige der Faktoren auf Meinungen und Schätzungen basieren und demnach subjektiv sind. In Bezug auf die Einstufung der Schadenshöhe hält das Sicherheitshandbuch etwa fest: „Mit Ausnahme der Festsetzung von Zeit- oder Wiederbeschaffungswert wird die Bewertung von bedrohten Objekten in der Regel sehr subjektiv sein.“(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a)

Auch eine Einordnung in bestimmte Klassifizierungen, wie sie das BSI empfiehlt, ist häufig nur eine Einstufung aufgrund von Expertenmeinungen und nicht quantitativ. Dieselben Probleme gelten auch für die Einschätzung und Bewertung der Eintrittswahrscheinlichkeiten, denn auch hier handelt es sich im Regelfall um Expertenschätzungen und nicht um quantitativ messbare Größen. Und nachdem sich die Gewichtung von Risiken aus dem Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe errechnet, muss, wenn beides nur Schätzwerte sind, deren Aussagekraft kritisch hinterfragt werden. So kann diese Risikobewertung auch nur als eine Art „Wette“ auf die Zukunft und die Risikomatrix nur als Placebo-Analyse gesehen werden.(Lunkeit & Zimmer, 2021, S. 381ff)

Einen zusätzlichen Weichmacher in Bezug auf die Umsetzung stellt der Verweis auf den „vernünftigen“ Aufwand dar, der lt. NIS-Gesetz für die Durchführung der Risikoanalyse investiert werden soll, denn in keiner der NIS-Quellen wird erläutert wie sich ein solcher Aufwand bemisst.(Bundeskanzleramt, 2024c) Entsprechend muss dieser Aufwand selbst definiert und gegebenenfalls gegenüber Dritten mit Argumentationen glaubhaft gemacht werden.

3.2 Hochverfügbarkeit und Redundanzen

Ein Kernelement dieser Arbeit ist eine hohe Systemverfügbarkeit und ein wesentliches Prinzip um in IT-Systemen eine hohe Verfügbarkeit zu erreichen ist die sogenannte Redundanz. Daher wird in diesem Kapitel darauf eingegangen auf welchen Ebenen

Redundanzen vorgesehen werden können, welche Verfügbarkeiten damit erreicht werden und wie diese klassifiziert werden können.(Bundesamt für Sicherheit in der Informationstechnik, 2013a, S. 6) Zunächst wird aber erläutert welche Arten von Verfügbarkeiten es gibt und wie diese gemessen werden können. Das österreichische NIS-Gesetz kann in diesem Fall aber nicht als wesentliche Bezugsquelle herangezogen werden, da darin das Thema Verfügbarkeit nur eine untergeordnete Bedeutung hat. Teilaspekte davon kommen zwar in den Sicherheitsmaßnahmen der Anlage 1 indirekt vor, insbesondere in den Bereichen der Betriebskontinuität und des Krisenmanagements, explizit ist darin aber weder eine Hochverfügbarkeit noch eine bestimmte Umsetzung von Redundanzen gefordert. Für den bezugnehmenden Sektor Digitale Infrastruktur hält die NIS-Verordnung zwar fest, dass ein Sicherheitsvorfall vorliegt, wenn der betroffene Dienst für mehr als 12 Stunden ausfällt, im Kontext von Hoch- oder Höchstverfügbarkeit werden aber wesentlich kürzere, maximale Ausfallszeiträume verlangt, sodass bei deren Erreichung die angeführten 12h nie erreicht werden würden. Als eine der wesentlichen Input-Quellen wird in diesem Kapitel daher das Hochverfügbarkeitskompendium des deutschen BSI herangezogen.(Bundeskanzleramt, 2024c; Bundeskanzleramt, 2024b; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, o. J.)

3.2.1 Definition von Verfügbarkeit

Für die Definition und Messung von Verfügbarkeiten werden häufig folgende Begriffe verwendet:

- Meantime between failures (MTBF): Misst die Zeitspanne zwischen aufgetretenen Fehlern.
- Meantime to repair (MTTR): Misst die Zeitspanne bis zur wiedererlangten Verfügbarkeit (inkl. Reaktionszeiten und Problemlösungszeiten)
- Meantime to failure (MTTF): Misst die prognostizierte Zeitspanne bis zum Auftreten des nächsten Fehlers.

Speziell die ersten beiden Kennzahlen werden in der Verfügbarkeitsplanung eingesetzt, daher kommt ihnen eine besondere Bedeutung zu. Zu Deutsch werden sie auch als Verfügbarkeitsdauer bzw. Verfügbarkeitszeit und Ausfalldauer bzw. Ausfallzeit bezeichnet. Eine gängige Herangehensweise ist es sie zu verwenden um die Verfügbarkeit von Systemen zu klassifizieren. Das BSI definiert etwa 6 Verfügbarkeitsklassen basierend auf diesen Werten, welche in der Tabelle unterhalb dargestellt sind.

Verfügbarkeits-klasse	Bezeichnung	Minimale Verfügbarkeit	Nicht-Verfügbarkeit	Ausfallzeit pro Monat	Ausfallzeit pro Jahr
VK 0	Standard-IT-System ohne Anforderungen an die Verfügbarkeit	~95%	~ 5%	1 Tag	Mehrere Tage
VK 1	Standard-Sicherheit nach IT-Grundschutz bei normalem Verfügbarkeitsbedarf	99,0%	1%	< 8 h	< 88 h
VK 2	Standard-Sicherheit nach IT-Grundschutz bei erhöhtem Verfügbarkeitsbedarf	99,9%	0,1%	< 44 min	< 9 h
VK 3	Hochverfügbar nach IT-Grundschutz für spezifische IT-Ressourcen;	99,99%	0,01%	< 5min	< 53 min
VK 4	Höchstverfügbar	99,999%	0,001%	< 26 s	< 6 min
VK5	Desaster-Tolerant	max. Verfügbarkeit	0	0	0

Tabelle 2: Typische Verfügbarkeitsklassen und ihre Ausfallzeiten lt. BSI (nach Bundesamt für Sicherheit in der Informationstechnik, 2013b)

Das BSI unterschiedet also in den höchsten Verfügbarkeitsstufen zwischen hochverfügbar, höchstverfügbar und desaster-tolerant, wobei diese Klassifizierung allgemeiner Natur ist und für die Bewertung von IT-Systemen aller Art eingesetzt werden kann. In Bezug auf die einleitenden Erläuterungen zum NIS-Gesetz würde das bedeuten, dass bei einem System, wenn es 12h und länger ausfällt, nicht von hoch- oder gar höchstverfügbar gesprochen werden kann, zumindest nicht nach dieser Skala. Ein solches System würde nach dieser Definition in die Verfügbarkeitsklasse 0 fallen, also in die Kategorie jener Systeme ohne Anforderungen an die Verfügbarkeit.(Bundesamt für Sicherheit in der Informationstechnik, 2013b)

Speziell in Bezug auf die Verfügbarkeit von Rechenzentren hat sich aber noch eine weitere Definition eingebürgert, nämlich die sog. Tier-Levels. Diese wurden Anfang der 90er-Jahre durch das amerikanische Uptime Institute definiert und sind bis heute weit

verbreitet. Sie klassifizieren die Verfügbarkeiten in Tiers, zu Deutsch Stufen, die im nachfolgenden Diagramm dargestellt sind.(Uptime Institute, LLC, 2024)

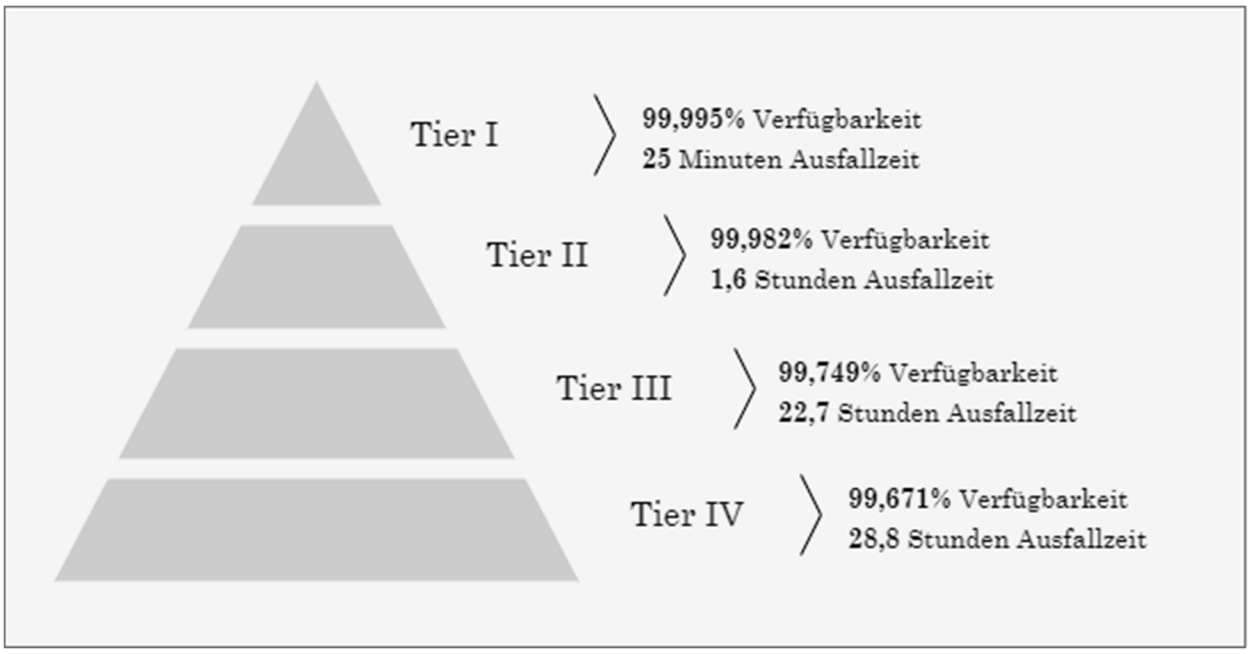

Abbildung 5: Verfügbarkeiten in Tiers (nach G-Core Labs S.A., 2021)

Demzufolge liegt die maximal erreichbare Verfügbarkeit eines einzelnen Rechenzentrums bei 99,995%, und das bereits bei maximaler Redundanz. Um eine Höchstverfügbarkeit, also eine Verfügbarkeit von 99,999% (auch Five-Nine-Availibility genannt), zu erreichen, wie sie etwa für besonders kritische Systeme verlangt wird, braucht es daher mindestens 2 geographisch getrennte Rechenzentren. Auf diese Redundanz-Aspekte wird nun im nächsten Kapitel eingegangen.(G-Core Labs S.A., 2021)

3.2.2 Redundanzen

Allgemein formuliert bezeichnet Redundanz das mehrfache Vorhandensein von gleichartigen Objekten. Im Speziellen wird damit die mehrfache Ausführung von technischen Komponenten, Services und Informationen gemeint, sowie das Vorhandensein von mehreren, ähnlich qualifizierten Personen im Personalstamm.(Bundesamt für Sicherheit in der Informationstechnik, 2013b)

Wie oben bereits kurz erläutert müssen sämtliche Komponenten eines Systems redundant ausgelegt sein um eine hohe Verfügbarkeit zu gewährleisten. Entsprechend obiger Definition bedeutet das, dass diese Komponenten mehrfach vorliegen müssen, sodass der Ausfall einer einzelnen Komponente durch die andere(n) kompensiert werden kann. Und diese Kompensation muss möglichst ohne zeitlichen Abstand geschehen, d.h. sobald eine

ausfällt übernimmt die andere vollautomatisch ohne weitere Verzögerung. Schließlich würde eine zeitliche Verzögerung in einem solchen Fall zu einem Systemausfall führen.

Das BSI unterteilt die Redundanz in ihre Merkmale und ihre Aktivierung. Mit ersterem meint das BSI die Eigenschaften, welche die Redundanz ausmachen, mit zweiterem die Art und Weise wie die Redundanz in der Architektur und im Betrieb des IT-Systems umgesetzt ist. Diese Zusammenhänge sind in untenstehendem Diagramm veranschaulicht.

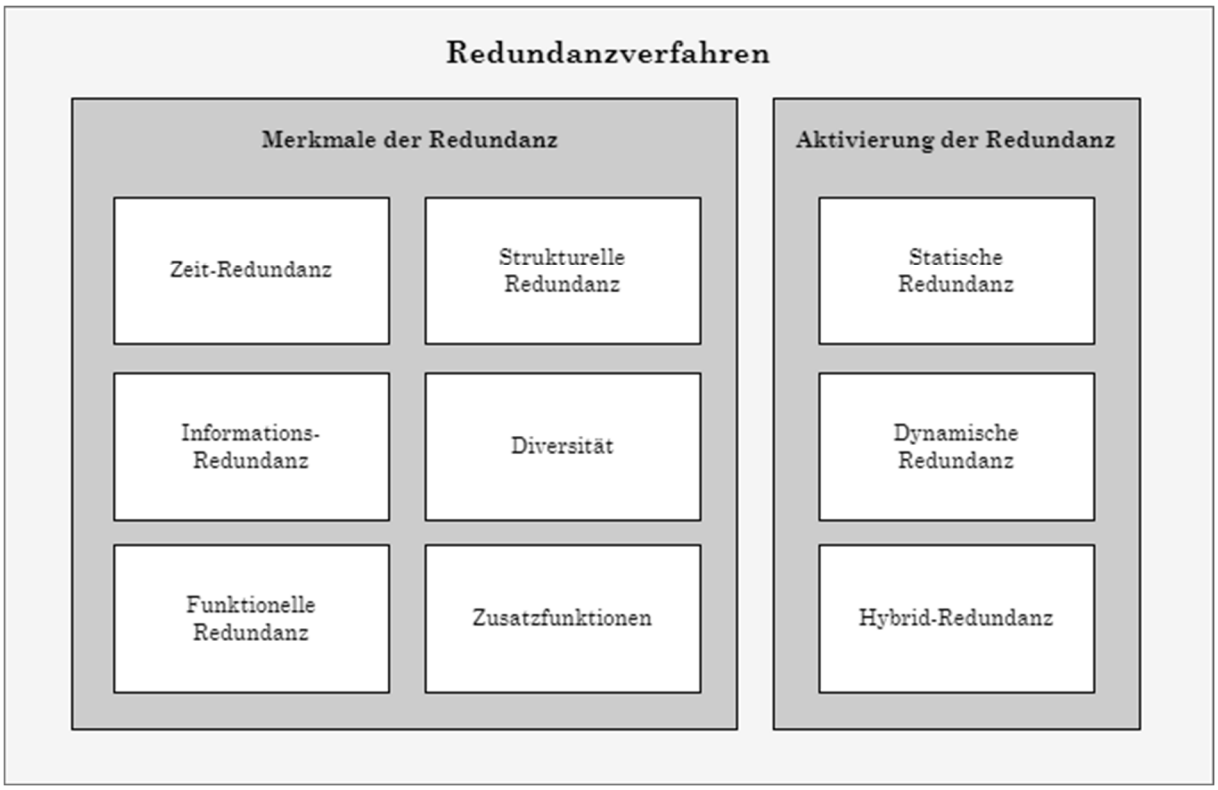

Abbildung 6: Redundanzverfahren lt. BSI (nach Bundesamt für Sicherheit in der Informationstechnik, 2013a)

Die Merkmale der Redundanz sind lt. BSI (Bundesamt für Sicherheit in der Informationstechnik, 2013a):

- Strukturelle Redundanz: Die schlichte, mehrfache Ausprägung von Ressourcen und Komponenten
- Funktionelle Redundanz: Eigens entwickelte Funktionen um die Redundanz in der Software zu erreichen. Etwa Fehlertoleranz-Funktionen.
- Zusatzfunktionen: Eine Unterart der funktionellen Redundanz, die nur existiert um die Redundanz zu ermöglichen. Etwa Steuerungskomponenten für Cluster Software.

- Informationsredundanz: Spezielle, zum Zweck der Redundanz generierte Informationen, etwa für die Fehlererkennung
- Zeitredundanz: Die zur Erbringung der funktionellen Redundanz zur Verfügung stehende Verarbeitungszeit.
- Diversität: Eine Erweiterung der strukturellen Redundanz in der die Redundanz nicht mit baugleichen Komponenten umgesetzt wird, sondern nur durch funktional äquivalente, die aber unterschiedlich implementiert sind. Solche Komponenten können von unterschiedlichen Lieferanten stammen, andere Technologien nutzen etc.

In Bezug auf die Aktivierung der Redundanz unterscheidet das BSI in (Bundesamt für Sicherheit in der Informationstechnik, 2013a):

- Statische Redundanz: Die redundanten Komponenten sind ständig aktiv und können jederzeit verwendet werden.
- Dynamische Redundanz: Die redundanten Komponenten liegen zwar vor, sind aber deaktiviert und müssen für deren Verwendung erst aktiviert werden.
- Hybrid-Redundanz: Sind Mischformen bzw. Spezialvarianten aus den oben genannten.

Zusätzlich zu den oben genannten nennt das BSI weitere, in der Praxis besonders bedeutsame Spezialvarianten der Redundanz, nämlich die Pfadredundanz und die Geographische Redundanz. Von Pfad-Redundanz wird gesprochen, wenn nicht nur die Komponenten selbst redundant ausgelegt sind, sondern auch die Verbindungen und Verbindungswege zwischen ihnen. Geographische Redundanz bezeichnet wiederum eine räumliche Verteilung der Redundanzen, etwa eine Aufteilung auf mehrere Unternehmensstandorte oder Rechenzentren.(Bundesamt für Sicherheit in der Informationstechnik, 2013a) Zu letzterem definiert das BSI auch einen eigenen Kriterienkatalog der definiert welche Eigenschaften bei der Auswahl von Rechenzentren-Standorten zu prüfen sind bzw. welche Gefahren für solche Standorte bestehen.(Bundesamt für Sicherheit in der Informationstechnik, 2019)

Auf die Komponenten-Ebene bezogen betont das BSI, dass Redundanzen sowohl auf der Hardware- als auch auf Software-Ebene vollständig umgesetzt werden müssen um eine hochverfügbare Architektur zu erzielen. Auf der Hardware-Ebene betrifft das jedwede Bauteile, wie CPU, Netzteile, Festplatten oder Arbeitsspeicher, auf Software-Ebene jede Software-Komponente. Bei letzterer wird speziell eine Software-Diversität

hervorgehoben, durch welche dieselbe Software-Komponente in unterschiedlicher, technischer Realisierung bereitgestellt wird. Die Komponente könnte etwa in unterschiedlichen Programmiersprachen entwickelt oder von unterschiedlichen Herstellern bezogen werden um eine Abhängigkeit zu einer bestimmten Software-Komponente zu vermeiden.(Bundesamt für Sicherheit in der Informationstechnik, 2013a)

Letztlich wird noch darauf hingewiesen, dass die Redundanzen sich nicht nur auf technische Komponenten beschränken, sondern sich auch auf IT-Dienstleistungen und das Personal beziehen. Beides muss in der Redundanz-Planung berücksichtigt werden.(Bundesamt für Sicherheit in der Informationstechnik, 2013a)

3.2.3 Verfügbarkeitsberechnung

Die Verfügbarkeit eines Systems wird berechnet durch das Verhältnis aus Downtime und Uptime eines Systems (Andrea Held, 2015):

Verfügbarkeit = Uptime / (Downtime + Uptime)

Das Ergebnis dieser Berechnung ist ein Prozentsatz der die Verfügbarkeit des Systems im betrachteten Zeitraum angibt. Entsprechend dem Ergebnis kann das System anschließend in eine der oben genannten Verfügbarkeitsklassen eingeordnet werden.

Gleichermaßen komplexer als auch realistischer wird es, wenn man berücksichtigt, dass diese Berechnung nur für ein einzelnes System gilt, bzw. innerhalb des Systems auch nur für eine einzelne Komponente. Will man aber ein System entwerfen, das rechnerisch als Ganzes eine hohe Verfügbarkeit aufweist, muss man die Verfügbarkeit von allen Einzelkomponenten berechnen und miteinander kombinieren, und dafür wiederum ist es entscheidend ob die einzelnen Komponenten seriell oder parallel miteinander verbunden sind. Wobei seriell bedeutet, dass die Komponenten einzeln vorkommen und alle verfügbar sein müssen damit das Gesamtsystem funktioniert. Parallel bedeutet hingegen, dass die einzelnen Komponenten mehrfach, redundant vorkommen, sodass wenn eine ausfällt immer noch die andere das System verfügbar hält.(Bundesamt für Sicherheit in der Informationstechnik, 2013c, S. 21ff)

Bei seriellen Schaltungen ist die Gesamtverfügbarkeit das Produkt der Einzelverfügbarkeiten, d.h. die Verfügbarkeiten multiplizieren sich. Die Verfügbarkeit A berechnet sich im Fall von zwei Komponenten demnach mit:

$$A_{seriell} = A_a * A_b$$

Hat man also etwa ein System mit zwei seriell geschalteten Komponenten, von denen jede eine Einzelverfügbarkeit von 99%, also Verfügbarkeitsklasse 1, hat, so hat das Gesamtsystem eine Verfügbarkeit von ~98%, und somit Verfügbarkeitsklasse 0.

Anders verhält es sich hingegen bei parallelen Schaltungen. Hier berechnet sich die Verfügbarkeit A, wiederum für den Fall von zwei Komponenten, nach der Formel:

$$A_{parallel} = 1 - (1 - A_a) * (1 - A_b)$$

Werden die Komponenten aus demselben Beispiel wie oben statt seriell nun parallel geschaltet ergibt das also eine Gesamtverfügbarkeit von 99,99%, und somit Verfügbarkeitsklasse 3.(Bundesamt für Sicherheit in der Informationstechnik, 2013c, S. 21ff)

3.3 Komplexität

Die Komplexität von Systemen wächst im selben Ausmaß wie die Anzahl seiner Komponenten und ihrer Verbindungen untereinander sowie mit ihrer Funktionalität. Unterschieden wird hierbei in eine strukturelle und eine funktionale Komplexität. Mit einer strukturellen Komplexität ist gemeint, dass das System und seine Komponenten eine komplexe Struktur aufweisen in der viele bzw. vielfältige Komponenten eingesetzt werden die wiederum stark miteinander vernetzt sind. Auch die Art der Vernetzung selbst kann eine hohe Komplexität aufweisen. Mit der funktionellen Komplexität ist im Gegensatz dazu das Verhalten der Komponenten gemeint. Diese können komplexe Funktionen ausführen oder sich aufgrund einer Vielzahl von Input-Parametern völlig unterschiedlich verhalten.(Lunkeit & Zimmer, 2021)

In Bezug auf Informationssysteme bedeutet eine hohe Komplexität auch eine Vervielfältigung möglicher Sicherheitslücken. Bei struktureller Komplexität steigen sie aufgrund der hohen Anzahl an Komponenten und Verbindungen, denn je mehr davon existieren und je unterschiedlicher sie sind, desto größer ist die Chance von Ausfällen, von der Notwendigkeit kritischer Patches, oder von Fehlern in der Einrichtung der Verbindungen. Bei funktioneller Komplexität steigt mit der Komplexität die Wahrscheinlichkeit von eigenen Programmierfehlern, von welchen die in den verwendeten Programm-Bibliotheken enthalten sind, und von fehlerhaften Software-Konfigurationen. Und mit der steigenden Vernetzung der Systeme untereinander steigt dadurch auch das Risiko erfolgreicher Cyberangriffe.(Lunkeit & Zimmer, 2021)

In den folgenden Kapiteln werden moderne Trends vorgestellt die in diesem Kontext eine Rolle spielen und die Komplexität zusätzlich erhöhen.

3.3.1 Microservices-Ansatz

Unter dem Begriff *Microservices* wird ein moderner Ansatz in der Softwarearchitektur verstanden, der vor allem darauf abzielt die Entwicklungsgeschwindigkeit zu erhöhen und entsprechend die Time-to-Market zu verkürzen. Dies wird dadurch erreicht, dass Applikationen in kleine, nur lose miteinander gekoppelte und unabhängig voneinander entwickelbare Software-Teile zerlegt werden, die über APIs (Application Programming Interfaces) miteinander kommunizieren. Dadurch verteilen sich die Anwendungen auf voreinander unabhängige Teilkomponenten, die entsprechend durch unterschiedliche Teams oder Organisationen entwickelt, mit unterschiedlichen Programmiersprachen und Technologien umgesetzt und die auch unabhängig voneinander betrieben werden können. Letzteres hat auch den Effekt der unterschiedlichen Skalierbarkeit der Microservices, denn dadurch, dass diese Services unabhängig und jeweils auf einer eigenständigen Architektur betrieben werden können, kann auch für jedes dieser Services selbst definiert werden, in welcher Anzahl es vorhanden sein muss. Es kann also unabhängig von der restlichen Anwendung wachsen oder schrumpfen.(Amazon.com, 2024; Atlassian, 2024a; IBM Deutschland GmbH, 2024)

Die Aufteilung der Services passiert dabei in erster Linie vertikal, also entsprechend ihres funktionalen Aufgabenbereichs. So kann es etwa ein Microservices für die Authentifizierung geben, ein zweites für der Erfassen von Kundendaten und ein drittes für die Abwicklung von Bestellungen. Aufgrund dieser Unterteilung wird der Micoservices-Ansatz häufig als Gegenspieler der sogenannten *Monolithischen Architektur* bezeichnet, in welcher die Software horizontal geschnitten wird. In einer solchen Unterteilung wird etwa zwischen Frontend, Middleware und Backend unterschieden, und somit nicht nach ihrer Funktion sondern nach ihrer Technologie.(Tremp, 2021)

Häufig wird auch angeführt, dass der Microservices-Ansatz ein Teil einer sogenannten *cloudnativen Architektur* ist. Damit ist gemeint, dass dieser durch seine Aufteilung der Anwendungen in viele, unabhängige Teil-Komponenten sich speziell für einen Betrieb in einer Cloud eignet, einem weiteren Trend auf den im nächsten Kapitel eigegangen wird.(Amazon.com, 2024; Atlassian, 2024a)

Der Microservices-Ansatz bringt aber nicht nur Vorteile mit sich. Der Softwareanbieter Atlassian nennt hierzu etwa explizit (Atlassian, 2024b):

- Erhöhte Komplexität
- Herausforderungen bei Deployment und Versionierung
- Komplexität bei Tests
- Schwierigkeiten bei der Fehlerbehebung
- Herausforderungen beim Datenmanagement

Hinzu kommen weitere Risiken die mit diesem Ansatz verknüpft sind, wie die möglichen Abhängigkeiten von einzelnen Anbietern und der geringe Einfluss auf deren Entwicklungszyklen.(Iserlohn & Schulte-Coerne, 2017)

3.3.2 Cloud-Computing

Mit Cloud-Computing wird das Konzept bezeichnet IT-Dienste dynamisch über ein Netz zu beziehen anstatt sie selbst zu betreiben. Diese IT-Dienste können Anwendungen sein (sog. Software-as-a-Service, SaaS), ganze Plattformen (sog. Platform-as-a-Service, PaaS), reine Infrastruktur (sog. Infrastructure-as-a-Service, IaaS) und weitere. Für die Entwicklung und den Betrieb von Individual-Software, wie sie im Kontext dieser Arbeit angenommen wird, wird in erster Linie IaaS eingesetzt, da es damit möglich ist die darunterliegende Hardware zu optimieren und besser auszunutzen. Technisch basiert dies auf der sogenannten Hardware-Virtualisierung, welche es erlaubt die physischen Hardwarekomponenten zu abstrahieren und auf virtuelle Hardware-Komponenten zu übersetzen. Auf diese Weise können jene Hardware-Ressourcen, die die Anwendung sieht, von den tatsächlich existierenden, physischen Hardware-Ressourcen getrennt werden und das kann schließlich genutzt werden um die physische Hardware effizienter zu nutzen.(Bundesamt für Sicherheit in der Informationstechnik, 2022; Zeiß & Jorns, 2022)

Zum Hauptnutzen von Cloud-Computing zählen im Kontext der in dieser Arbeit untersuchten Systeme die gewonnene Flexibilität, im Sinne der einfachen Skalierbarkeit der bezogenen Dienste, und die Effizient in Bezug auf die Nutzung der Infrastruktur, die Anschaffungs- und die Betriebskosten. Gleichzeitig birgt es aber auch die Risiken, wie eine mögliche Anbieterabhängigkeit, der Kontrollverlust über Daten und Prozesse, die Intransparenz über die Aktivitäten beim Cloud-Anbieter sowie Risiken im Bereich des Datenschutzes und er IT-Sicherheit.(Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2017) Um diesen Aspekten Rechnung zu tragen hat das BSI mit dem *Kritierienkatalog C5* ein eigene Spezifikation mit Mindestanforderungen

an ein sicheres Cloud-Computing erstellt, das sich an Cloud-Anbieter und -Kunden sowie deren Prüfer richtet.(Bundesamt für Sicherheit in der Informationstechnik, 2024f) Und auch die österreichische A-SIT, das Zentrum für sichere Informationstechnologie Austria, stellt mit dem *Cloud Computing Kompass* ein eigenes Dokument mit vielen Kriterien und zusätzlichen Aspekten rund um den Einsatz von Cloud-Computing zur Verfügung.(A-SIT Zentrum für sichere Informationstechnologie – Austria, 2017)

In Bezug auf die oben beschriebene Komplexität bedeutet der Einsatz von Cloud-Computing, dass durch die zusätzliche Cloud-Schicht, die zwischen der Anwendung und der Hardware eingezogen wird, auch zusätzliche Komponenten erforderlich sind, was die Gesamtkomplexität des Systems entsprechend erhöht.

3.3.3 Weitere Dienste

Neben den oben genannten Microservices und Cloud-Computing gibt es vor allem im Bereich der Authentifizierung und Autorisierung weitere, moderne Konzepte, die aufgrund ihrer Bedeutung hier kurz vorgestellt werden.

OAuth ist ein von der Internet Engineering Task Force (IETF) publizierter Standard, der aktuell in der Version 2.0 vorliegt, und beschreibt ein Framework für die Autorisierung von Zugriffen auf die Daten und Objekte eines Dritten. OAuth ermöglicht also eine dienstübergreifende Autorisierung und stellt sicher, dass nur ein Zugriff auf die Daten und Objekte nur mit Zustimmung des Eigentümers dieser Daten und Objekte möglich ist.(IETF, 2012) Mit OAuth technisch verwandt und darauf basierend ist der Standard *OpenID Connect* der OpenID Foundation, welcher zur Authentifizierung verwendet werden kann.(OpenID Foundation, 2023)

Die *Active Directory Domain Services* bezeichnen einen von Microsoft entwickelten Verzeichnisdienst, der zentral im Netzwerk aufgebaut und für die Verwaltung von Benutzerkonten und deren Berechtigungen verwendet wird. Er kann mit Anwendungen integriert werden, etwa über das Lightweight Directory Access Protocol (LDAP), und ermöglicht es so, dass Benutzerzugänge nur an einem einzigen, zentralen Ort gespeichert sein müssen.(Microsoft, 2023)

Public Key Infrastructures (PKI) bezeichnen schließlich Systeme zur Verwaltung von digitalen Zertifikaten, die zur Authentifizierung herangezogen werden können. Ihre Kernaufgaben sind (Bundesamt für Sicherheit in der Informationstechnik, 2002):

- Anträge auf Zertifikate entgegennehmen und prüfen
- Zertifikate ausstellen
- Ausgestellte Zertifikate durchsuchen
- Zertifikate zurückziehen

Diesen Diensten ist gemein, dass sie an zentralen Stellen Daten für die Authentifizierung und Autorisierung verwalten und mit den jeweiligen Anwendungen integriert werden. Auch durch Ihre Verwendung kommen also in Bezug auf die Komplexität der Anwendungen zusätzliche Komponenten hinzu, die für den ordnungsgemäßen Betrieb verfügbar sein müssen. Beim Einsatz von PKI braucht es zur unmittelbaren Zertifikatsvalidierung zwar keine aktive Verbindung zur Zertifizierungsstelle, es braucht diese aber um zu prüfen ob das Zertifikat widerrufen wurde. Auch für den Umgang mit den Zertifikaten werden in der Implementierung zumeist zusätzliche Programm-Bibliotheken benötigt und somit die funktionelle Komplexität erhöht.

3.4 Wirtschaftlichkeit

Ob Sicherheitsanforderungen umgesetzt werden oder nicht ist häufig nicht nur eine technische Frage, sondern auch eine wirtschaftliche, auch wenn gerade im Kontext von kritischen Anwendungen die Kosten nicht immer das ausschlaggebende Argument sein dürfen. Vor allem in Bezug auf kritische Systeme wäre eine beweisbare Sicherheit über alle Komponenten des Systems hinweg ideal, weil sich Sicherheitsvorfälle in diesem Bereich so gravierend auswirken können. Vom wirtschaftlichen Standpunkt aus gesehen gilt das insbesondere auch in Anbetracht dessen, dass eine Fehlerbehebung umso teurer wird je später ein Fehler gefunden wird. Untersuchungen in diesem Bereich haben gezeigt, dass die mittleren Kosten für die Korrektur kritischer Fehler um ein Vielfaches höher sind, wenn sie erst sehr spät entdeckt werden. Je nach Untersuchung wird hier von einem Faktor 30 bis zu einem Faktor größer als 100 ausgegangen, im Vergleich dazu, wenn diese Fehler bereits in einer frühen Phase gefunden werden. Hinzu kommt, dass aufgrund von Wettbewerbsdruck und Time-to-Market der Funktionalität von Produkten und Technologien häufig ein höherer Stellenwert beigemessen wird als deren Sicherheit und Zuverlässigkeit. Allerdings ist aufgrund der Komplexität und des Umfangs von kritischen Systemen eine vollständig beweisbare Sicherheit zumindest zurzeit nicht

umsetzbar und solche Beweise können sich maximal auf absolut zentrale Komponenten begrenzen.(Lunkeit & Zimmer, 2021; Volker Wittpahl, 2023; Waidner et al., 2013)

Auch eine vollständig redundante Auslegung aller Komponenten ist angesichts der hohen Komplexität und der umfangreichen Vernetzung kaum mehr zu erreichen oder zumindest sehr teuer. Die Redundanz erfordert schließlich eine Vervielfachung sämtlicher Ressourcen, sie erhöht aber auch die Kosten in der Entwicklung und im Betrieb bzw. erhöht sie die Komplexität des Systems.(Volker Wittpahl, 2023, S. 173)

Es braucht daher eine Methode um die Umsetzung von Sicherheitsanforderungen auch wirtschaftlich zu beurteilen. Das NIS-Gesetz spricht in diesem Zusammenhang im oben bereits erwähnten §17 (1) davon, dass die zu treffenden Vorkehrungen verhältnismäßig sein sollen und auch die Risikoanalyse mit vernünftigem Aufwand durchzuführen ist. Diese Einschränkungen zielen darauf ab bei der Umsetzung der Sicherheitsanforderungen auch deren Kosten und entsprechend deren Wirtschaftlichkeit zu berücksichtigen. Was das NIS-Gesetz allerdings nicht festlegt ist wie die Begriffe „verhältnismäßig“ und „vernünftig“ konkret zu bemessen sind. Auch in der NIS-Verordnung findet sich dafür keine Definition. Zwar wird dort näher erläutert welches die Sicherheitsvorkehrungen sind, die in Betracht gezogen werden sollen, nicht aber was in diesem Kontext als verhältnismäßig angesehen werden kann. In §11 (2) der NIS-Verordnung wird sogar noch weiter verunsichert, indem hier auch die Risikoanalyse nur noch „soweit möglich“ durchzuführen ist. Und schließlich bietet auch das NIS-Factsheet keine konkretere Definition an und referenziert bei der Durchführung der Risikoanalyse wiederum den „vernünftigen“ Aufwand. Das NIS-Gesetz berücksichtigt in gewisser Weise also Aspekte der Wirtschaftlichkeit, definiert aber gleichzeitig keine zwingenden und konkreten Maßstäbe oder monetäre Bezugsgrößen.(Bundeskanzleramt, 2024c; Bundeskanzleramt, 2024b; Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, o. J.; Volker Wittpahl, 2023)

In der deutschen Umsetzung der NIS-Richtlinie besteht eine ähnliche Problematik in Bezug auf die Angemessenheit der Maßnahmen. Auch hier wurde seitens des Gesetzgebers zwar definiert, dass bei der Auswahl der Schutzmaßnahmen unter anderem auch wirtschaftliche Aspekte zu berücksichtigen sind, gleichzeitig klammert der deutsche Bundesverband IT-Sicherheit in seiner Beurteilung der Umsetzbarkeit der technischen und organisatorischen Maßnahmen die Wirtschaftlichkeitsprüfung aus, weil eine solche Beurteilung seiner Meinung nach nur individuell erfolgen kann.(TeleTrusT, 2023)

Im nächsten Kapitel wir daher ein Ansatz vorgestellt um die Wirtschaftlichkeit von Sicherheitsanforderungen individuell zu bemessen, der sogenannte *Return on Security Investment* (ROSI).

3.4.1 Return on Security Investment (ROSI)

Der Return on Security Investment ist angelehnt an die verbreitete, finanzwirtschaftliche Rentabilitätskennzahl des *Return on Investment* (ROI), mit dem berechnet wird ob eine Investition ökonomisch sinnvoll ist. Dieser ROI wird mit folgender Formel berechnet:

$$ROI = \frac{Gain\ from\ Investment - Cost\ of\ Investment}{Cost\ of\ Investment}$$

Er setzt also den Ertrag und die Kosten einer Investition in Relation berechnet so den Prozentsatz des durch die Investition erzielten Gewinns.(ENISA, 2012; Geißler & Schmitz, 2020)

Für Sicherheitsinvestitionen kann dieser Ansatz nicht 1:1 verwendet werden da mit solchen Investitionen kein unmittelbarer Profit erwirtschaftet, sondern ein möglicher Schaden abgewendet wird. Um den Wert einer solchen Investition zu berechnen muss also nicht der zusätzliche Ertrag, sondern der verhinderte Schaden in die Kalkulation einfließen. Um dies zu tun beruht die Berechnung des ROSI auf folgenden vier Parametern:

- Single Loss Expectancy, SLE: Dies ist der erwartete Verlust, wenn das Risiko ein einziges Mal schlagend wird. Gemeint ist hier die Summe aller Kosten, materiell wie immateriell, die durch den Schaden verursacht werden.
- Annualized Rate of Occurrence, ARO: Mit diesem Parameter wird geschätzt wie häufig das Risiko in einem Jahr schlagend wird.
- Annualized Loss Expectancy, ALE: Dies ist das Produkt aus SLE und ARO und drück aus mit welchem Schadensausmaß pro Jahr gerechnet werden muss.
- Mitigation Ratio: Mit diesem Wert wird geschätzt um welchen Prozentsatz sich die Schadensauswirkung durch die Investition reduziert.

Mit diesen Parametern berechnet sich der ROSI schließlich wie folgt:

$$ROSI = \frac{ALE * Mitigation\ Ratio - Cost\ of\ Investment}{Cost\ of\ Investment}$$

Er setzt also den Wert der Risikominderung in Relation zu den Kosten der Investition und berechnet so den Prozentsatz des durch die Investition erzielten, finanziellen Nutzens.(ENISA, 2012; Geißler & Schmitz, 2020)

Die Berechnung des Return on Security Investment ermöglicht es also den Nutzen einer Investition in eine Sicherheitsmaßnahme finanziell zu bemessen und somit anschaulicher zu machen. Er beruht aber auf mehreren Schätzgrößen, daher gelten auch bei ihm schlussendlich dieselben Limitierungen und Kritikpunkte die bereits oberhalb im Bezug auf das Risikomanagement genannt worden sind.

4 Abgeleitete Erwartungen

Basierend auf den Erkenntnissen der vorangegangenen Kapitel werden in diesem nun Erwartungen aufgestellt, wie die in dieser Arbeit beschriebenen, kritischen Anwendungen durch österreichische Sicherheitsexpert_innen umgesetzt werden würden. Diese Erwartungshaltung entspricht dem im Rahmen der Design Science Methode erstellten Artefakt und ist dementsprechend der Ausgangspunkt für die qualitativen Experteninterviews, mit denen es evaluiert wird.

4.1 Anforderungsquellen

Es wird erwartet, dass österreichische Sicherheitsexpert_innen für den Aufbau eines allgemeinen, kritischen Systems eine vergleichbare Herangehensweise wählen würden, wie jene die für die wesentlichen Dienste der kritischen Infrastruktur durch die NIS-Richtlinie vorgeschrieben ist. Entsprechend wird davon ausgegangen, dass für die Umsetzung ein risikobasierter Ansatz gewählt werden würde und dass ähnliche Sicherheitsmaßnahmen umgesetzt würden, wie jene, die in der Anlage 1 der NIS-Verordnung beschrieben sind.

Weiters wird erwartet, dass die Anforderungsquellen die für die österreichische Umsetzung der NIS-Richtlinie in den NIS-Factsheets vorgeschlagen werden bekannt sind und für die Umsetzung zumindest in Betracht gezogen werden würden. Das gilt insbesondere für das österreichische Sicherheitshandbuch. Es wird aber auch erwartet, dass die Sicherheitsexpert_innen mindestens 1-2 weitere Referenz-Modelle und Best Practices heranziehen würden um die Sicherheitsmaßnahmen zu bestimmen.

4.2 Vertraulichkeit und Integrität

Es wird erwartet, dass sich die Anforderungen im Bereich der Vertraulichkeit und der Integrität ähnlich gestalten würden wie jene der Kategorien 3 - 7 der Anlage 1 der NIS-Verordnung. Insbesondere wird davon ausgegangen, dass den Themen Verschlüsselung, Authentifizierung & Autorisierung und Maßnahmen zur Absicherung der externen Schnittstellen ein besonders hoher Stellenwert zukommen würde und darauf keinesfalls verzichtet werden würde.

4.3 Verfügbarkeit

Es wird erwartet, dass österreichische Sicherheitsexpert_innen in der Umsetzung von kritischen Systemen versuchen würden die Komplexität der Systeme so gering als möglich zu halten und nur jene Sicherheitsmaßnahmen umzusetzen die für unentbehrlich gehalten werden und nicht mehr. Er wird also erwartet, dass die Sicherheitsmaßnahmen einer kritischen Bedarfsanalyse unterzogen werden.

Weiters wird erwartet, dass modernen Trends wie dem Microservices-Ansatz und dem Cloud-Computing bei kritischen Systemen skeptisch begegnet wird und diese nicht oder wenn, dann nur sehr vorsichtig eingesetzt werden würden, um die Komplexität zu reduzieren bzw. auch um volle Transparenz über alle Systemkomponenten zu haben.

Darüber hinaus wird erwartet, dass die Expert_innen angesichts der Erkenntnisse in der Verfügbarkeitsberechnung auf eine vollständige Redundanz auf allen Ebenen setzen würden. Für besonders kritische Komponenten, insbesondere für welche bei denen Abhängigkeiten zu Dritten bestehen, wird erwartet, dass zusätzlich zur physischen Redundanz auch auf eine Redundanz durch Diversität geachtet werden würde.

Abschließend wird erwartet, dass das Security by Design Paradigma durch die Expert_innen forciert und dessen Umsetzung verlangt wird.

4.4 Wirtschaftlichkeit

In Bezug auf die Wirtschaftlichkeit wird erwartet, dass für die Umsetzung der Sicherheitsmaßnahmen eine Kosten-Nutzen-Analyse durchgeführt oder sogar ein konkreter Return on Security Investment berechnet werden würde. Es wird erwartet, dass nicht nur die Maßnahmen an sich, sondern insbesondere auch die Redundanzen der einzelnen Komponenten wirtschaftlich gerechtfertigt sein müssen um sie umzusetzen.

5 Expert_innen-Interviews

Wie in der Einleitung beschrieben wurden Interviews mit Fachexpert_innen durchgeführt um die Erkenntnisse aus dem theoretischen Teil und die daraus abgeleiteten Erwartungen im Rahmen der Design Science Methode zu evaluieren. Dieses Kapitel geht nun im Detail darauf ein wie die Interviews genau durchgeführt und ausgewertet wurden.

5.1 Interview-Gestaltung

Für die Durchführung der Interviews wurde der Ansatz eines sogenannten leitfadengestützten Interviews gewählt. Das bedeutet, basierend auf der Forschungsfrage und anhand der während der Literaturstudie identifizierten, relevanten Themenbereiche wurden im Vorfeld mehrere Fragen überlegt, um die Meinung der befragten Personen zu dem Forschungsthema möglichst zielgerichtet und ohne Vorbehalte in Erfahrung zu bringen. Dabei wurde speziell darauf Wert gelegt, dass die Fragen offen, erzählgenerierend und hörer_innenorientiert formuliert wurden, denn der Interviewer soll bei den Befragungen in den Hintergrund treten und lediglich moderierend und steuernd eingreifen, während die Inhalte möglichst unbeeinflusst von den Expert_innen selbst kommen sollen. Allerdings wurde im Zuge der Leitfadenerstellung auch der Ablauf der Interviews, und insbesondere die Interviewsituation, mental durchgespielt, um auf diese Weise bestimmte Gesprächsverläufe zu antizipieren, um darauf vorbereitet zu sein. Insbesondere wurden Situationen überlegt in denen der Gesprächsablauf ins Stocken geraten könnte oder in denen es seitens des Interviewpartners Unklarheiten geben könnte und entsprechend wurden bereits im Vorfeld sogenannte Aufrechterhaltungs- und Nachfragen formuliert, um beim Eintritt solcher Situationen flüssig reagieren zu können. Und schließlich wurden die Interview-Verläufe im Nachgang jeweils kritisch reflektiert, um so den Leitfaden und die Formulierung der Fragen bei Bedarf zu schärfen und im nächsten Durchgang noch besser vorbereitet zu sein.(Ferdinand Porsche FernFH, 2024a; Ferdinand Porsche FernFH, 2024b; Vogt & Werner, 2014)

Auf diese Weise wurde schließlich der Interviewleitfaden im Anhang A entwickelt, der als Grundlage für die Interviews zum Einsatz gekommen ist. Eine der Fragen, konkret die Frage No.5, wurde dabei im Zuge der Interviews aufgrund der Rückmeldungen der Interviewpartner überarbeitet und präzisiert, was schließlich zu weniger Rückfragen in den restlichen Interviews geführt hat. Ebenfalls wurde für jede Frage die Dauer für deren Beantwortung grob geschätzt um ein Gefühl dafür zu entwickeln wie lange das Interview in Summe dauern wird. Diese Dauer diente aber nur der Terminvorbereitung und wurde

nicht für ein Timeboxing verwendet. Im Gegenteil, jede Frage wurde so lange behandelt wie es neue Inputs gegeben hat, unabhängig von der Zeit die dafür benötigt wurde.

Abgerundet wurde der Leitfaden schließlich mit einer im Vorfeld überlegten Gesprächseinleitung und einer entsprechenden Verabschiedung. Beides diente aber nur der Orientierung und der Aufrechterhaltung des Redeflusses und wurde nicht vorgelesen, sondern frei interpretiert. In der Einleitung wurde aber insbesondere stets darauf Wert gelegt, dass nicht nur die Eckpfeiler der Arbeit selbst noch einmal vorgestellt wurden, sondern auch der Ablauf des Interviews sowie die Möglichkeit dieses zu jeder Zeit und ohne Angabe von Gründen abbrechen zu können.

Nach Abschluss des inhaltlichen Interviews wurden schließlich zusätzlich noch ein paar wenige, im Kontext dieser Arbeit aber speziell für relevant befundenen, soziodemografische Daten zur Person des Interviewten erhoben. Diese umfassten vor allem das Alter, die Ausbildung, das Geschlecht und die aktuelle Berufstätigkeit. Diese Fragen wurden in Form jenes eigenen, vom restlichen Interview unabhängigen Fragebogens gestellt, der sich in Anhang B befindet. Die Interviewten wurden dabei darauf hingewiesen, dass die Beantwortung dieser Fragen optional und unabhängig vom restlichen Interview sind um ihnen nicht das Gefühl zu geben zu deren Beantwortung gedrängt zu werden. Dies wurde zusätzlich durch die Auslagerung der Fragen in ein eigenes Dokument unterstrichen, und den Interviewten wurde es selbst überlassen ob sie dieses unmittelbar, also im Anschluss an das Interview gemeinsam ausfüllen, oder ob sie es sich im Nachgang ansehen wollten.

Für die generelle Einverständnis zur Teilnahme an der Forschung sowie zur Verwendung der erhobenen Daten wurde ebenfalls ein eigenes Dokument aufgesetzt. Diese Einverständniserklärung klärte die Interviewten über den Zweck des Interviews auf, gab ihnen eine Kurzbeschreibung des Forschungsgegenstands, wies darauf hin, dass die Teilnahme freiwillig ist und jederzeit abgebrochen werden kann und ging speziell auf die Verwendung der erhobenen Daten ein. Diesbezüglich wurde explizit darauf hingewiesen, dass die Daten vertraulich behandelt, nicht an Dritte weitergegeben und ausschließlich in anonymisierter Form verwendet werden, sowie dass sämtliche Aspekte der Datenschutzgrundverordnung eingehalten und die daraus abgeleiteten Ansprüche erfüllt werden. Die konkrete Ausformulierung der Einwilligungserklärung basierte auf dem Muster der Ferdinand Porsche FernFH, welches in deren sogenannten Qualitorial zur Verfügung gestellt wurde. Dieses Muster wurde als Ausgangspunkt verwendet und an den

Zweck dieser Arbeit angepasst. Das fertige Dokument findet sich in Anhang C.(Ferdinand Porsche FernFH, 2024c)

5.2 Durchführung der Interviews

Die oben beschriebenen Interviews wurden als sogenannte Expert_innen-Interviews durchgeführt, einer anwendungsfeldbezogenen Variante von Leitfadeninterviews. Das bedeutet sie wurden mit Personen durchgeführt die in Bezug auf die Fragestellungen dieser Arbeit aufgrund ihrer Ausbildung, Erfahrung und ihrer beruflichen Tätigkeit als Expert_innen angesehen sind. Hierbei ist aber hervorzuheben, dass nicht die einzelnen Personen im Fokus stehen, sondern diese als Repräsentanten für die Handlungs- und Sichtweisen der ganzen Expert_innengruppe angesehen werden.(Ferdinand Porsche FernFH, 2024a)

Insgesamt wurden im Rahmen dieser Arbeit Interviews mit acht Personen aus sieben unterschiedlichen Organisationen geführt, wobei die Interviews größtenteils mit den Expert_innen alleine durchgeführt wurden. Nur eines der Interviews wurde mit zwei Expert_innen derselben Organisation gemeinsam durchgeführt, um dadurch den gegenseitigen Austausch und ein dynamisches Gespräch zu begünstigen.

Die interviewten Expert_innen stammen einerseits aus dem persönlichen Netzwerk des Autors und wurden andererseits über erweiterte, persönliche Beziehungen sowie ihre berufliche Verbindung zur Ferdinand Porsche FernFH kontaktiert und konnten so für die Teilnahme an dieser Forschungsarbeit gewonnen werden. Nach der persönlichen Kontaktaufnahme und einer ersten Schilderung des Forschungsprojekts und dessen Zielsetzungen wurde allen Expert_innen bereits im Vorfeld des Interviews die Einwilligungserklärung per E-Mail übermittelt, von Ihnen inhaltlich geprüft und anschließend digital signiert zurückgesendet. Diese wurden schließlich durch den Autor digital gegengezeichnet und somit beidseitig unterschrieben, und diese finale Version wurde auch den Interviewpartner_innen abschließend übermittelt. Für die Signierung wurde jeweils das Zertifikat der ID Austria verwendet, wobei unter anderem das Tool der A-Trust für die Signierung von PDF-Dokumenten zum Einsatz gekommen ist.(A-Trust GmbH, 2024; Bundeskanzleramt, 2024d)

Durchgeführt wurden die Interviews schließlich in einer Videokonferenz, die mittels der Microsoft Teams Umgebung der FernFH technisch abgewickelt wurde. Mit Einwilligung der Interviewpartner_innen wurden die Termine durch Microsoft Teams aufgenommen und auch initial transkribiert, wobei parallel dazu ein digitales Aufnahmegerät als

Backup eingesetzt wurde. Auf dieses musste in weiterer Folge auch zurückgegriffen werden da eine der durchgeführten Aufzeichnungen auf der Office 365-Plattform verloren ging und auch durch die Administratoren der FernFH nicht mehr wiederhergestellt werden konnte. Für dieses Interview musste also auf die Aufzeichnung des digitalen Aufnahmegeräts zurückgegriffen werden. Auch das Transkript von Microsoft Teams wurde nur für drei der Interviews als Ausgangsbasis herangezogen. Die restlichen Interviews wurden mit der Analyse-Software MAXQDA initial transkribiert, welche für die Durchführung der unterhalb beschriebenen, qualitativen Inhaltsanalyse bereits angeschafft wurde und für das Dafürhalten des Autors wesentlich bessere, allerdings auch kostenpflichte Transkriptionsergebnisse geliefert hat. Trotz software-gestützter, initialer Transkription mussten die Transkripte aber dennoch jeweils in mehreren Durchläufen im Detail durchgegangen, korrigiert und vervollständigt werden. Die von Microsoft Teams und MAXQDA erstellten, automatischen Transkripte konnten somit lediglich als Ausgangsbasis herangezogen werden.

Für die Transkription selbst wurde die sogenannte *Wörtliche Transkription mit Übertragung ins Schriftdeutsche* verwendet. Fülllaute und non-verbale Elemente wurden entsprechend ebenso wenig im Transkript berücksichtigt wie Betonungen, Akzentuierungen, Lautstärkeänderungen oder Pausen. Zusätzlich wurden Aussagen im Dialekt geglättet und in die Schriftsprache überführt.(Vogt & Werner, 2014)

Konkret wurden folgende Personen interviewt, die nachfolgend auf anonymisierte Weise kurz beschrieben sind.

- **P1**: Ist sowohl selbstständig als auch unselbstständig tätig und seit knapp 30 Jahren berufstätig. Er hat mehrere Studienabschlüsse in technischen Fachrichtungen, unterrichtet selbst auch an einer Hochschule im Umfeld der Informationssicherheit und beschäftigt sich seit 10-15 Jahren intensiv mit dem Aufbau von kritischen Systemen im Bereich von Behörden und Organisationen mit Sicherheitsaufgaben.(P1, 2024, l. 7–12)
- **P2**: Arbeitet seit vielen Jahren im Team der Information Security eines österreichischen Telekom-Konzern und ist dort spezialisiert auf die formaleren Aspekte des Bereichs, wie Normen, speziell die ISO 27001, und Anforderungen bzw. Vorgaben von Regulierungsbehörden.
- **P3**: Ist der Leiter des oben genannten Information Security Teams eines österreichischen Telekom-Konzerns. Er ist seit über 10 Jahren intensiv mit

kritischen Systemen beschäftigt, hauptsächlich in der Telekommunikations-Branche.(P2 & P3, 2024, l. 7–10)

- **P4**: Ist seit über 20 Jahren sowohl selbstständig als auch unselbstständig im Bereich des Informationssicherheits-Managements tätig. In seiner Unselbstständigkeit ist er Chief Security Officer eines großen, österreichischen Konzerns, in seiner Selbstständigkeit Prüfer und Auditor, auch von Unternehmen die kritische Infrastrukturen nach dem NIS-Gesetz betreiben. Parallel ist er auch Dozent an einer Hochschule und leitet dort mehrere Lehrveranstaltungen.(P4, 2024, l. 8–11)
- **P5**: Arbeit seit dem Jahr 2000 in unterschiedlichen Positionen im Bereich der Informationssicherheit, die von Security Management, über IT-Audits bis zu IT Service- und Risiko-Management reichen. Aktuell arbeitet er eng mit Forschungsorganisationen und Bundesministerien im Bereich des Katastrophenmanagements und von resilienten IT-Strukturen zusammen bzw. ist er Berater im Bereich der Netz- und Informationssicherheit nach NIS-1 und NIS-2. Daneben war er einige Zeit als externer Lektor an einer Hochschule beschäftigt.(P5, 2024, l. 2)
- **P6**: Arbeitet seit über 15 Jahren im Security Bereich und ist aktuell Leiter von zwei Teams in der österreichischen Tochter eines internationalen Technologie-Konzerns. Zu seinen Tätigkeiten gehört es ebenso sichere Architekturen beim Kunden zu designen als auch diese zu implementieren. Zu seinen Kunden zählen zahlreiche Unternehmen im Bereich der kritischen Infrastruktur. Gleichzeitig arbeitet er als Lektor an einer Hochschule.(P6, 2024, l. 2)
- **P7**: Ist Eigentümer und Geschäftsführer eines Security Beratungsunternehmens das hauptsächlich Security Assessments durchführt. Der Schwerpunkt des Unternehmens liegt auf Unternehmen im Bereich Automatisierungstechnik, von OT und von kritischen Infrastrukturen. Parallel engagiert er sich in einem österreichischen, technisch-wissenschaftlichen Verband, speziell im Bereich der Security in der industriellen Automatisierungstechnik.(P7, 2024, l. 2)
- **P8**: Arbeitet seit über 15 Jahren im Security Bereich und ist aktuell in einer international tätigen Bankengruppe Teamleiter und dort in seiner Rolle für die technischen Security-Lösungen der gesamten Gruppe zuständig. Zu seinen Aufgaben gehört es auch im Fall von Security Incidents deren Abwicklung über mehrere Units der Gruppe hinweg zu koordinieren.(P8, 2024, l. 2)

5.3 Qualitative Inhaltsanalyse nach Mayring

Die qualitative Inhaltsanalyse, die im deutschsprachigen Raum vor allem durch Philipp Mayring entwickelt wurde, ist eine Methode zur strukturierten Auswertung eines in Textform vorliegenden Datenmaterials. In der vorliegenden Arbeit sind das die Transkripte der durchgeführten Expert_innen-Interviews. Die strukturierende Auswertung hat dabei zum Ziel aus dem vorliegenden Datenmaterial, das typischerweise sehr umfangreich ist, nur jene Inhalte zu extrahieren, die für die Beantwortung der Forschungsfrage relevant sind. Das in die Forschung einfließende Datenmaterial wird also sukzessive reduziert indem irrelevante Teile entfernt werden. Das verbleibende, relevante Datenmaterial wird schließlich analysiert und interpretiert.(Gläser & Laudel, 2009) Das nachfolgende Diagramm veranschaulicht diesen schrittweisen Prozess.

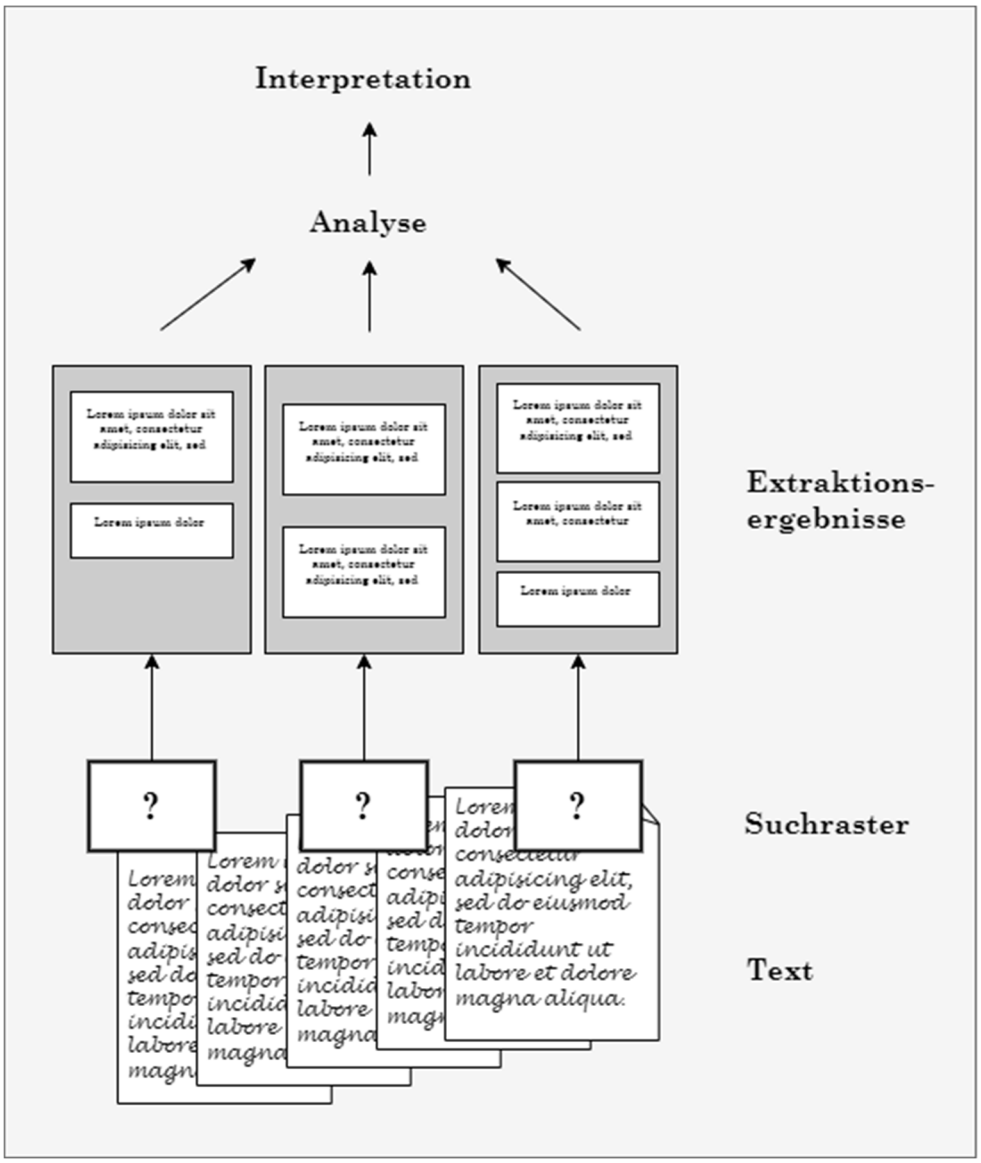

Abbildung 7: : Qualitative Inhaltsanalyse (nach Gläser & Laudel, 2009, S. 200)

Der Prozess der qualitativen Inhaltsanalyse ist in der Literatur vielfach beschrieben, unter anderem bei Flick (Flick, 2020, S. 143ff), Kotthaus (Kotthaus, 2020, S. 184ff), Vogt & Werner (Vogt & Werner, 2014) und Gläser & Laudel (Gläser & Laudel, 2009, S. 197ff). Da die Beschreibungen sich sehr ähneln orientiert sich die die Prozessbeschreibung in diesem Kapitel erster Linie an Gläser & Laudel.

Die Durchführung der qualitativen Inhaltsanalyse gestaltet sich so, dass das Datenmaterial sukzessive durchgearbeitet wird und die darin als relevant befundenen Passagen gekennzeichnet werden. D.h. es werden jene Daten markiert, die für relevant gehalten werden. Diese Markierung erfolgt allerdings nicht nur binär, im Sinne einer Ja-Nein-Entscheidung, sondern die Daten werden im selben Schritt auch gleich kategorisiert. Wird also eine relevante Text-Passage gefunden, wird geprüft ob bereits eine Kategorie existiert, zu der diese Text-Passage passt. Existiert diese, wird die Text-Passage dieser Kategorie zugewiesen. Existiert sie noch nicht, wird eine neue Kategorie erzeugt und die Text-Passage danach dieser neuen Kategorie zugewiesen. Der Vorgang um Daten einer Kategorie zuzuweisen wird als *Codieren* bezeichnet und mehrfach durchgeführt. D.h. es wird mehrmals über die Daten iteriert und mit jeder Iteration können sowohl die Kategorien verfeinert als auch die Daten neu zugeordnet werden. Das wird so lange durchgeführt bis schlussendlich alle relevanten Daten identifiziert und entsprechenden Kategorien zugewiesen worden sind.(Gläser & Laudel, 2009, S. 199f)

Welche Kategorien es gibt kann entweder im Vorfeld festgelegt werden (= deduktives Verfahren) oder dynamisch anhand der gefundenen Daten definiert werden (= induktives Verfahren). Häufig anzutreffen, und auch im Rahmen dieser Arbeit angewendet, ist aber das Deduktive-/Induktive-Wechselspiel, also eine Mischform aus beidem. Hier wird zunächst anhand des Forschungsgegenstands und des entsprechend aufgebauten Interview-Leitfadens bereits ein initiales Kategoriensystem deduktiv abgeleitet, denn schließlich ist aufgrund des Forschungsgegenstands bereits bekannt was den Forschenden an den zur Verfügung stehenden Daten interessiert. Ergeben sich während der Analyse aber neue Aspekte so werden diese nicht verworfen, sondern zusätzliche Kategorien dynamisch angelegt und in das Kategoriensystem eingeordnet. Diese Vorgangsweise ermöglicht es aus den erhobenen Daten zu lernen und zusätzliche Aspekte zu berücksichtigen, die im Vorfeld nicht sichtbar waren.(Gläser & Laudel, 2009, S. 201)

Die Auswertung erfolgt schließlich kategorienbasiert. D.h. jede Kategorie wird einzeln betrachtet und es werden sämtliche ihr zugeordnete Text-Passagen analysiert und kritisch beurteilt. In diesem Schritt kann das Kategoriensystem auch erneut verfeinert

werden, d.h. es können Kategorien bei Bedarf in mehrere Kategorien aufgesplittet oder mehrere Kategorien zu einer verdichtet werden. Auch können Ober- und Unterkategorien gebildet und so eine Hierarchie von Kategorien erzeugt werden. Das Ende dieses Prozesses ist erreicht, sobald bei einer neuerlichen Betrachtung aller Kategorien und der ihr zugewiesenen Daten keine weitere Verfeinerung mehr sinnvoll erscheint. Den Abschluss der qualitativen Inhaltsanalyse bildet die Interpretation der Ergebnisse im Kontext der Forschungsfrage. Hier werden die gefundenen Ergebnisse dargestellt, zusammenfassend diskutiert und mit anderen Theorien in Bezug gesetzt.(Gläser & Laudel, 2009, S. 246ff)

6 Forschungsergebnisse

In diesem Kapitel werden die Ergebnisse der Expert_innen-Interviews dargestellt, die mithilfe der Software MAXQDA 2024 ausgewertet wurden. Die Unterkapitel entsprechen dabei exakt jenem Codesystem, das im Zuge der qualitativen Inhaltsanalyse nach Mayring sukzessive generiert wurde. Die meisten Codes wurden aus dem Forschungsgegenstand und dem Interviewleitfaden deduktiv abgeleitet. Es wurden aber auch zusätzliche Aspekte mit aufgenommen, einzelne Codes in Sub-Codes unterteilt und neu strukturiert sowie mit dem Bereich des Testens von Sicherheitsanforderungen überhaupt eine komplett neue Kategorie induktiv identifiziert.

6.1 Anforderungsquellen

In dieser Kategorie wird darauf eingegangen wie die Expert_innen in ihrem beruflichen Kontext vorgehen um die Sicherheitsanforderungen von kritischen Systemen zu bestimmen. Insbesondere wird hier ermittelt, welche primären Quellen sie dafür heranziehen.

Die Kernaussagen in dieser Kategorie sind folgende:

P1: Er setzt in erster Linie auf BSI-Standards und nennt insbesondere auch das Hochverfügbarkeitskompendium des BSI als Referenz. Zusätzlich nennt aber auch die Veröffentlichungen der ENISA als wesentliche Quelle. Besonders streicht er aber hervor, dass in seinem Bereich, in dem er vor allem mit Umgang mit Gesundheitsdaten zu tun hat, die gesetzlichen Vorgaben von großer Bedeutung sind.

P2/P3: Sie arbeiten hierfür mit einem Vorgabenkatalog aus dem Konzern, der vor allem auf der langjährigen Erfahrung und dem gelernten Expert_innenenwissen zusammengetragen worden ist. Welche Standards und Frameworks bei der Erstellung und der Aktualisierung dieses Katalogs zusätzlich eingesetzt werden ist für die beiden Expert_innen nicht transparent.

P4: Verwendet CRISAM von der Fa. Calpana. Dieses basiert auf der BSI-Methodik, integriert aber auch diverse andere, internationale Standards, insbesondere auch ISO/IEC 27000, ITIL und Cobit.

P5: Er hält Cobit für am umfassendsten anwendbar, aber auch ITIL findet er sehr pragmatisch. Die ISO/IEC 27000 berücksichtigt er ebenso wie die ISO 31000, findet diese

aber eher akademisch. Generell findet er die Standards auch sehr überlappend. Auf der technischen Ebene findet er speziell die CIS Top 18 auch sehr gut. Um all diese Anforderungen einfließen zu lassen wurde in seinem Unternehmen selbst ein sogenanntes *Meta-ISMS* entwickelt, das all diese Standards adressiert, und nach Cobit strukturiert wurde.

P6: Definiert die Anforderungen je nach Fokus der Anwendung, wobei diese Anforderungen auch nur organisatorische sein können. Für die Anforderungen an die Hochverfügbarkeit setzt er auf einen Risikomanagement-Ansatz und versucht im Austausch mit den Kunden die Anforderungen zu bestimmen. Bezüglich der Standards orientiert er sich sonst vor allem an der NIST und dem BSI, er erwähnt aber auch die ISO/IEC 27000 sowie auch als einziger der Expert_innen auch direkt das österreichische Sicherheitshandbuch. Er hebt aber auch den Wert der eigenen Erfahrung hervor und ergänzt, dass er sich grundsätzlich auch dem *Zero-Trust* Prinzip der NIST orientiert.

P7: Sieht vor allem spezialisierte Dritthersteller-Tools wie CRISAM von der Fa. Calpana und risk2values von der Fa. avedos im Einsatz. Er sieht sonst auch häufig die ISO/IEC 27000 in Verwendung, insbesondere bei den Unternehmen im Energiesektor, und auch den BSI-Grundschutz. Er bevorzugt generell eine risikobasierte Vorgehensweise und hält kein Kapitel für per se wichtiger als das andere, aber im spezifischen Kontext kann durchaus das eine einen wesentlich höheren Stellenwert haben als das andere.

P8: Seine Organisation setzt in erster Linie auf eine selbst entwickelte *Threat Modeling Software* zur automatischen Bestimmung von Sicherheitsanforderungen auf Basis von internen Sicherheitsvorgaben. Verschiedene Normen und Standards fließen in den Anforderungskatalog dieses Tools ein. Daneben haben vor allem ISO-Standards und das NIST Cybersecurity Framework eine besondere Bedeutung für ihn.

Fazit:

Die Experten_innen greifen auf eine breite Palette an Standards, Frameworks und Tools zurück, um Sicherheitsanforderungen für kritische Systeme zu bestimmen. Die häufigsten Referenzen sind BSI-Standards, ISO/IEC 27000, ITIL, Cobit, und das NIST Cybersecurity Framework. Einige Organisationen verwenden oder entwickeln auch eigene Systeme und Tools, die auf diesen Standards basieren, um die Sicherheitsanforderungen zu definieren und umzusetzen. Erfahrungen und Expertenwissen spielen ebenfalls eine wichtige Rolle, insbesondere bei der Anpassung und Implementierung dieser Standards in spezifischen Kontexten.

6.1.1 Österreichisches Sicherheitshandbuch

In diese Kategorie werden die Meinungen der Expert_innen zum österreichischen Sicherheitshandbuch dargestellt und den Stellenwert, dass dieses in ihrem beruflichen Kontext hat.

Die Kernaussagen in diesem Bereich sind:

P1: Das Sicherheitshandbuch ist bekannt aber wenig präsent. Es wird seiner Ansicht nach eher regierungsintern verwendet. Er weiß aber, dass es sich am BSI-Grundschutz und an der ISO/IEC 27000 orientiert und für NIS-Audits herangezogen wird.

P2/P3: Das Sicherheitshandbuch läuft ihnen von Zeit zu Zeit über den Weg und wird dann von ihnen überflogen, bislang wurde aber kein entscheidender Mehrwert darin gesehen.

P5: Hält das Sicherheitshandbuch für abgeschrieben und es hat seiner Ansicht nach gar keine Auswirkung.

P6: Kennt das Sicherheitshandbuch und findet es prinzipiell auch ganz gut gelungen. Er hält es aber für sehr ähnlich zu anderen Standards.

P7: Findet es ist nur für den Behördenbereich gedacht und sieht es wenn, dann nur im Umfeld von Leitstellen wirklich im Einsatz.

P8: Das Sicherheitshandbuch hat in seinem Unternehmen keinen Einfluss. Die Sicherheitsanforderungen werden bei ihm in erster Linie international bestimmt und diese werden ohnehin für strenger gehalten als österreichische Empfehlungen.

Fazit:

Das österreichische Sicherheitshandbuch spielt unter den befragten Expert_innen eine untergeordnete Rolle obwohl es allen bekannt ist und teilweise für gut gelungen gehalten wird. Dennoch sehen die meisten Expert_innen keinen signifikanten Mehrwert darin, insbesondere im Vergleich zu internationalen Standards wie BSI-Grundschutz oder der ISO/IEC 27000. Es wird hauptsächlich als regierungsinternes oder behördenorientiertes Dokument wahrgenommen und findet in der privaten Wirtschaft nur begrenzt Anwendung. Die Kritikpunkte reichen von geringer Relevanz und Aktualität bis hin zur Redundanz mit bereits etablierten internationalen Standards.

6.1.2 Ö-Normen

In dieser Sektion wird die Bedeutung von Ö-Normen, wie sie im NIS Factsheet erwähnt werden, analysiert und welchen Einfluss diese in ihrem beruflichen Alltag haben.

Die Kernaussagen dazu lauten:

P1: Haben für ihn keine Bedeutung

P2/3: Haben für sie keine Bedeutung

P4: Haben für ihn eine untergeordnete Bedeutung, er weist aber auf die Ö-Norm Variante der ISO 27000 hin.

P5: Verwendet jetzt keine im Speziellen, gibt aber zu bedenken, dass die ISO 31000 ursprünglich von einer Ö-Norm abstammt.

P6: Finden bei ihm keine Anwendung

P7: Verwendet jetzt keine im Speziellen, gibt aber zu bedenken, dass die ISO 27000 auch als Ö-Norm existiert.

P8: Finden bei ihm keine Anwendung

Fazit:
Ö-Normen finden bei keinem der befragten Expert_innen eine Anwendung, auch wenn manche wissen, dass diese an internationale Standards angelehnt oder diese sogar maßgeblich beeinflusst haben.

6.2 Vertraulichkeit und Integrität

In diesem Punkt werden die Aussagen der Expert_innen zu ihrem Umgang mit Anforderungen an Vertraulichkeit und Integrität zusammengefasst.

Die wichtigsten Aussagen in diesem Bereich sind:

P1: Als die wichtigen Anforderungen nennt er eine Ende-zu-Ende Verschlüsselung, die Isolation der Systeme und ausreichende Redundanzen. Letztere beziehen sich sowohl auf Geo-Redundanzen als auch auf Technologie-Redundanzen. Zusätzlich dazu sollten mehrere Sicherheitsstufen umgesetzt werden, die alle durch Angreifer überwunden werden müssten.

P2/3: Unterscheiden in den Anforderungen danach ob Vertraulichkeit oder Verfügbarkeit der wichtigere Aspekt ist, nach dem Motto „Fail safe or fail secure."(P2 & P3, 2024, l. 26) Verschlüsselung ist einer der wichtigsten Faktoren. Weiters ist das Prinzip der Datenminimierung und der Serviceminimierung einzuhalten, es sollen keine „eierlegenden Wollmilchsau"-Schnittstellen entwickelt werden. Zusätzlich sollten die *Least Privileges* und die *Minimum Rights* Prinzipien umgesetzt werden und neue Zugänge sollten auch nur nach einer sicheren Verifizierung eingerichtet werden. Speziell sollte auch auf Wartungs- und administrative Zugänge wertgelegt werden, aber auch auf etwaige physische Zugänge durch unbefugte Dritte, die Schlupflöcher öffnen könnten („Putzfrau").

P4: Nennt Identity und Access Management als die wichtigsten Kriterien. Weiters ist es entscheidend die Angriffsfläche zu minimieren und nur das extern erreichbar zu machen was unbedingt erreichbar sein muss. Weiters ist die Protokollierung von allen Transaktionen extrem wichtig. Zusätzliche Aspekte auf die Wert gelegt werden muss sind Verschlüsselung, sichere Löschungen, und in Bezug auf Cloud der Umgang mit etwaigen *Super-Tenants*.

P5: Setzt in erster Linie auf ein sauberes Asset-Management als Grundvoraussetzung. Man muss zunächst seine Topografie genau kennen, also welche Systeme, Schnittstellen Protokolle, Ports etc. in Verwendung sind, und darauf dann ein entsprechendes Update- und Patch-Management aufsetzen. Am Zweit-Wichtigste stuft er den Change-Management-Prozess ein um Kontrolle und Transparenz darüber zu schaffen was am System passiert. Auch ein umfangreiches Monitoring spielt eine entscheidende Rolle.

P6: Versucht einerseits die Angriffsfläche von kritischen Anwendungen möglichst gering zu halten und setzt parallel dazu auf das *Least-Privileges* und das *Need-to-Know*-Prinzip.

P7: Man sucht sich ein Framework aus und schaut dann was relevant ist. Insbesondere nennt er den Annex A der ISO 27.000 und auch die 11 Kategorien der NIS-Verordnung. Er weist aber auch darauf hin, dass keine Anforderung per se wichtiger ist als eine andere, vielmehr muss im jeweiligen Kontext entschieden werden, was wichtig ist.

P8: Für ihn ist eine sogenannte *Basishygiene* entscheidend. Damit meint er allen voran ein sauberes Identity- und Access Management. Er hält etwa eine Verschlüsselung der Festplatte oder auf DB-Ebene für nutzlos, wenn die Schnittstelle nicht abgesichert ist, wenn unsichere Passwörter verwendet werden oder wenn sich jeder als Admin anmeldet. Er verwendet den Ansatz Zugriffe auf die Daten entsprechend dem *Need-to-Know*-Prinzip

absichern. Zusätzlich nennt er als entscheidende Maßnahmen die Verschlüsselung, das Zugriffmanagement und die Authentifizierung, wobei letztere auch über Identity Provider oder Zertifikate erfolgen kann.

Fazit:

Die Expert_innen nennen eine Vielzahl von Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität in kritischen Systemen. Zentrale Themen sind die Ende-zu-Ende-Verschlüsselung, Minimierung der Angriffsfläche, Prinzipien wie *Least Privileges* und *Need-to-Know* sowie ein umfassendes *Identity und Access Management.* Weitere wichtige Maßnahmen umfassen die Protokollierung, eine sichere Löschung, ein umfangreiches Monitoring sowie ein effektives Asset- und Change-Management.

6.3 Verfügbarkeit

Diese Kategorie fasst die Aussagen zusammen in denen sich die Expert_innen auf die Erzeugung von Ausfallsicherheit beziehen.

Die wesentlichen Aussagen sind:

P1: Essenziell ist eine redundante Auslegung der Systeme, inkl. Standort- und Technologie-Redundanzen. Je nach Komponente können das auch deutlich mehr als nur 2-fache Redundanzen sein. Ein zweiter, dritter, vierter Weg als Backup sowie Umschalt-Mechanismen müssen von vornherein beachtet werden.

P2/3: Das Ziel ist es Single Points of Failure suchen und zu vermeiden. Es gibt keine allgemein gültige Formel dafür wie die Geo-Redundanz umgesetzt werden sollte, also wie viele Sites, welche Entfernung zwischen den Sites etc. Stattdessen ist die Strategie sehr abhängig vom System selbst und es muss individuell entschieden werden wie die Redundanz aufgebaut werden muss.

P4: Setzt auf Redundanzen so gut es irgendwie geht und dann auf Vulnerability und Penetration Tests. Zusätzlich setzt er auf mehrfache Netzwerkanbindungen, redundante Datenhaltung und Geo-Redundanz.

P5: Nennt explizit das *Availability Management* aus ITIL an dem er sich orientiert. Single Points of Failure müssen demnach mit Redundanzen begegnet werden. Die betrifft die Stromzufuhr, die Netzwerkverbindungen, etc. Er streicht aber auch heraus, dass Single Points of Failure auch Mitarbeiter sein können und auch solche Abhängigkeiten muss

man beachten und abbauen. Dasselbe gilt für die Supply Chain. Er setzt generell darauf bei zentralen Komponenten für eine Diversifikation zu sorgen.

P6: Er setzt darauf Redundanzen einbringen, aber nicht nur für die Systeme an sich, sondern auch für ihre Kommunikationswege. Es ist für eine mehrfache Stromversorgung, ebenso zu sorgen wie für geo-redundante Rechenzentren.

P7: Nennt wieder eine risikobasierte Vorgehensweise und empfiehlt entsprechende Maßnahmen setzen um das Risiko auf ein akzeptables Niveau zu reduzieren. Er empfiehlt darüber hinaus die Redundanzen auf allen Ebenen inkl. der Kommunikationswege, der Hardware und auch auf personeller Ebene umzusetzen. Er nennt ein Beispiel bei dem für die Kommunikation gleich drei unterschiedliche Leitungen verwendet wurden.

P8: Nennt Geo-Redundanz und einen gewissen Mindestabstand, der eingehalten werden muss. Dies betrifft sowohl die Cloud als auch On-Premise-Systeme. Essenziell ist ein entsprechendes Load-Balancing davor, wobei dessen Strategie, also Active-Active / Active-Passive, dann eine Detailfrage ist. Seiner Ansicht nach sollten Redundanzen auf allen Ebenen vorhanden sein, allerdings gibt hier auch technische Grenzen, die nicht überwunden werden können.

Fazit:

Die Experten heben die Bedeutung von Redundanzen für die Verfügbarkeit kritischer Systeme hervor. Zentral sind die Vermeidung von *Single Points of Failure*, die Implementierung von Geo-Redundanzen und die Sicherstellung mehrerer Strom- und Kommunikationswege. Auch Ansätze wie *Availability Management* aus ITIL und risikobasierte Strategien spielen eine wichtige Rolle. Es wird auch auf die Diversifikation bei zentralen Komponenten und die Berücksichtigung technischer Grenzen hingewiesen.

6.3.1 Komplexität und externe Dienste

In diesem Kapitel werden jene Interview-Abschnitte beschrieben in denen sich die Expert_innen auf die Komplexität von Systemen beziehen, sowie auf Einflüsse von externen Diensten/Komponenten und Microservices.

Die Kernaussagen sind:

P1: Aus seiner Sicht spricht überhaupt nichts dagegen externe Dienste zu verwenden solange sie redundant vorhanden sind. Und man muss sich im Vorfeld genau überlegen was man konkret macht, wenn mal ein solches Service nicht verfügbar ist.

P2/P3: Sehen den Trend zur vermehrten Nutzung von externen Diensten in erster Linie bei den Anwendungen für die breite Masse. Bei kritischen Systemen wird hingegen versucht die Abhängigkeiten zu Externen so gering als möglich zu halten und möglichst alles aus einer Hand zu machen.

P4: Sieht die Verwendung von externen Diensten in ihrem Unternehmen kritisch und meint: „Wir versuchen das zu vermeiden, dass wir von Externen abhängig sind. Also für die kritischen Anwendungen versuchen wir das alles im Haus zu halten."(P4, 2024, l. 60)

P5: Meint, dass die Verteilung auf mehrere Dienste auch Vorteile haben kann aufgrund der Diversifikation. Andererseits sorgen sie auch für eine hohe Komplexität, die vielleicht nicht mehr handhabbar ist. Kleinteilige Lösungen sind auch undurchschaubar und es sorgt auch für Probleme mit der Einhaltung von SLAs, wenn so viele Unternehmen im Spiel sind. Sie fördern auch ein „Hot-Potato"- oder „Geht mich nichts an"-Denken und schaffen zusätzliche Abhängigkeiten, nämlich durchaus auch auf Personen- und Skill-Ebene.

P6: Hat bei kritischen Systemen nur selten gesehen, dass diese Cloud Lösungen oder externe Dienste verwenden, und sieht das mehr als Trend in der Anwendungsentwicklung. Er sieht dort die Problematik, dass hier häufig ein anderer Schlag von Entwickler_innen eingesetzt wird und die nicht so den Security-Fokus haben. Security Teams würden dort häufig erst zu spät eingebunden werden. Wenn aber externe Dienste verwendet werden würden, dann müssten für diese auch entsprechende Backup-Wege vorgesehen werden.

P7: Sieht durch die Verwendung von Cloud Architekturen eine höhere Komplexität und eine entsprechend höhere Fehleranfälligkeit, auch aufgrund des hohen Bedarfs an Automatisierung. Er steht der Verwendung der Cloud aber dennoch offen gegenüber und meint, dass das nur eine Frage der Risikoanalyse ist. „Ich bin da generell sehr pragmatisch und bin der Meinung, Cloud ist nicht grundsätzlich gut oder auch nicht grundsätzlich böse. Ich muss mir halt einfach anschauen, was die Security, die relevanten Security-Aspekte sind und dann auch dort eine Risikoanalyse machen und die Risiken adressieren."(P7, 2024, l. 32)

P8: Aus seiner Sicht spricht nichts gegen die Verwendung der Cloud oder die Verwendung externer Dienste, allerdings „mit starken kryptographischen Protokollen, die Authentifizierung und Autorisierung, aber auch Vertraulichkeit und Integrität, dann sicherstellen".(P8, 2024, l. 24) Auch die Redundanz muss gegeben sein. Darüber hinaus

streicht er die Notwendigkeit einer zertifikats-basierten, dezentralen Identität heraus, da das User-Management mit vielen externen Einheiten nicht mehr zu managen ist.

Fazit:

Die Meinungen zur Nutzung externer Dienste und Cloud Infrastrukturen variieren stark. Während einige Experten keine grundsätzlichen Einwände gegen deren Nutzung haben, betonen andere die Notwendigkeit, Abhängigkeiten zu minimieren und alles intern zu halten. Die Komplexität, die durch die Nutzung externer Dienste entsteht, wird als potenzielles Problem erkannt, insbesondere auch in Bezug auf SLAs und Abhängigkeiten auf Personen- und Skill-Ebene. Eine sorgfältige Planung und Risikoanalyse sowie die Sicherstellung von Redundanz und starken Sicherheitsmaßnahmen sind jedenfalls eine Grundvoraussetzung für den Einsatz externer Dienste in kritischen Systemen.

6.3.2 Security by Design

Diese Kategorie bezieht sich auf die Aussagen der Expert_innen in Bezug auf die Bedeutung und Umsetzung des Security by Design Prinzips.

Die Kernaussagen dieser Kategorie können folgendermaßen zusammengefasst werden:

P1: Kennt das Prinzip und forciert es vor allem in Bezug auf Ausschreibungen. Gleichzeitig sieht er bei einigen Herstellern aber auch Mängel bei dessen Umsetzung.

P2/P3: Kennen das Prinzip und es wird in der eigenen Softwareentwicklung bereits ganz gut berücksichtigt. Sie siehen hier eine Verbesserung im Laufe der letzten Jahre, insbesondere wenn es darum geht zu beurteilen welche Daten kritisch sind, wo die gespeichert werden, in welchen Fällen man Systeme auftrennen oder zusammenführen sollte und welche Schnittstellen es zwischen ihnen gibt.

P4: Security by Design ist beim ihm noch nicht dort wo sie es gerne hätten. Er lebt es so, dass bei der Umsetzung von funktionalen Anforderungen auch die Umsetzung von Sicherheitsmaßnahmen mitberücksichtigt und eingeplant wird. Der Anteil von Sicherheitsmaßnahmen im Verhältnis zu funktionalen Anforderungen beträgt bei im etwa 10-15%.

P5: Sieht noch einige Luft nach oben in der Umsetzung und vermutet den Grund dafür in der Time-to-Market-Denkweise, die versucht die Services und Produkte so schnell als möglich auf den Markt zu bekommen. Und das führt dazu, dass die Security-Lösungen

wenig durchdacht und schlecht umgesetzt sind. Er sieht das auch in aktuellen Trends so und spottet: „Das S in IoT steht ja für Security“.(P5, 2024, l. 24)

P6: Nennt als einziger der Expert_innen Security by Design im Gesprächsverlauf. Er sieht einen Trend in diese Richtung und, dass mehr Hersteller das mitbedenken.

P7: Versucht Security by Design in seinen Beratungsprojekten umzusetzen und Systeme von Anfang an sicher zu bauen. Er setzt hier in erster Linie auf Ansätze wie *Least Privileges* und *Defense in Depth*.

P8: In seinem Unternehmen wird Security by Design gelebt und es proklamiert die Devise „Security ist die Verantwortung von jedem.“(P8, 2024, l. 30) Einerseits entstehen aus dem verpflichtenden Einsatz ihres *Threat Modeling Tools* automatisch Security-Anforderungen, für die auch automatisiert Tickets in deren Issue-Tracker JIRA angelegt und in der Projektumsetzung realisiert werden. Siehe dazu die Erläuterungen bei den Anforderungsquellen. Andererseits ist Security by Design auch in deren Entwicklungsorganisation umgesetzt worden. So gibt es in jedem Produktentwicklungsteam einen sogenannten *Security Champion*, der das Mitbedenken der Security im Designprozess und die Umsetzung der Sicherheitsanforderungen sicherstellt. Daneben gibt es sogenannte *Security Domain Experts*, deren Aufgabe es ist die Security-Aspekte in die breite Masse zu tragen.

Fazit:

In welcher Tiefe Security by Design in den Organisationen berücksichtigt wird variiert sehr stark. Einige haben das Prinzip bereits gut integriert und erleben Verbesserungen dadurch, andere sehen noch erheblichen Verbesserungsbedarf. Ansätze wie *Least Privileges* und *Defense in Depth* sind wichtige Elemente der Umsetzung. Erfolgreiche Implementierungen betonen die Verantwortung jedes Einzelnen für die Sicherheit und integrieren eigene Rollen wie die Security Champions und Domain Experts in die Entwicklungsprozesse. Automatisierte Tools zur Generierung von Sicherheitsanforderungen und deren Verfolgung sind ebenfalls nützliche Praktiken.

6.4 Testing von Sicherheitsanforderungen

Dieser neue Aspekt, der induktiv aus den Aussagen der Expert_innen abgeleitet wurde, beschäftigt sich mit dem Testing von Sicherheitsmaßnahmen Er wurde zusätzlich aufgenommen da Aussagen in diese Richtung mehrfach in den Gesprächen genannt und als besonders wichtig hervorgehoben wurden.

Die Kernaussagen dieser Kategorie sind:

P1: Bevorzugt eine Strategie in der alle Redundanzen parallel betrieben und im Normalbetrieb auch gleichzeitig bespielt werden. Im Fehlerfall auf Backup-Lösungen zurückzugreifen ist zwar häufig anzutreffen birgt aber die Gefahr, dass das vernachlässigt wird oder in Vergessenheit gerät und dann eben nicht funktioniert, wenn es darauf ankommt. Redundanzen, die nicht ohnehin im Normalbetrieb parallel getestet werden, müssen also zumindest regelmäßig geübt werden.

P2/3: Regelmäßiges Testen ist entscheidend und wird häufig vernachlässigt. Bei der initialen Einführung müssen alle Redundanzen gründlich getestet werden und danach, in regelmäßigen Abständen, hinterfragt und nochmals durchgeführt werden.

P6: Setzt auf Lasttests und Ausfalltests um einerseits die Peformance und andererseits die Resilienz der Systeme zu prüfen. Diese werden während Wartungszeitfenstern durchgefühlt. Zusätzlich kommen sog. *Red-Team-Audits* zum Einsatz und zwar sowohl von intern als auch von extern. Von intern wird das Team mit einem Laptop und einem Account ausgestattet und es wird geprüft wie weit man damit kommt. Hier geht es also in erster Linie darum Schwachstellen zu finden. Von extern wird wirklich der Angriff von außen simuliert und hier steht in erster Linie das prozessual richtige Verhalten im Vordergrund. D.h. hier wird geprüft wie sich die Teams verhalten, ob die Prozesse eingehalten werden und funktionieren, und wo es ggfs. noch blinde Flecke gibt.

P7: Tests der Security Maßnahmen sollten vor allem auch im Rahmen von Business Continuity Management und Desaster Recovery Tests durchgeführt werden. „Man sollte diese Dinge nicht zur Ausnahme, sondern zur Regel machen. Alles, was ich regelmäßig mache im Unternehmen läuft oder ist geübt, ist eingeübt, können die Leute. Und wenn ich es nur einmal alle drei Jahre mache, ist die Chance groß, dass irgendwelche Fehler passieren.“(P7, 2024, l. 28) Manche Unternehmen machen also nur alle 3 Jahre Übungen während in anderen Unternehmen der Wechsel der Umgebung eine Routinetätigkeit ist, die regelmäßig ausgeführt wird. In Bezug auf die Resilienz von Systemen empfiehlt er auch die Verwendung des Chaos Monkey von Netflix um zufällige Ausfälle zu simulieren und so zum Normalzustand zu machen.

P8: Auf Anwendungs-Ebene müssen verpflichtende Penetration Tests bei jeder größeren Änderung durchgeführt werden. Bei Anwendungen die als „Mission Critical“ definiert sind, muss darüber hinaus zumindest 1x/Jahr ein Penetration Test auf jeden Fall durchgeführt werden. Auf Infrastruktur-Ebene werden diverse Scan-Tools eingesetzt um

Schwachstellen aufzuspüren bzw. die interne Compliance sicherzustellen. Ein weiterer Aspekt ist, dass sich die Produktteams nicht selbst auditieren dürfen, sondern diese Überprüfungen müssen durch andere Organisationsteile durchgeführt werden.

Fazit:

Die Expert_innen haben hervor, dass regelmäßiges und umfassendes Testing von Security-Anforderungen entscheidend für die Sicherheit kritischer Systeme ist. Sie betonen die Notwendigkeit regelmäßiger Tests und Übungen, um die Resilienz der Systeme zu gewährleisten und die Kompetenz der Mitarbeiter zu stärken. Strategien wie paralleler Betrieb und regelmäßige Übungen von Redundanzen, Last- und Ausfalltests, Red-Team-Audits sowie der Einsatz von Tools wie Chaos Monkey und Penetration Tests sind bewährte Methoden. Es ist außerdem wichtig, dass Überprüfungen nicht von den Produktteams selbst durchgeführt werden, um Unabhängigkeit und Objektivität zu gewährleisten.

6.5 Wirtschaftlichkeit

Von den Expert_innen wurden verschiedene Ansätze zur Beurteilung der Wirtschaftlichkeit von Sicherheitsanforderungen in kritischen Systemen genannt, die in diesem Kapitel zusammengefasst werden.

Die Kernaussagen können wie folgt zusammengefasst werden:

P1: Kennt strikte Beurteilungen der Wirtschaftlichkeit eher in Bezug auf Vertraulichkeit und Datenschutz, und den damit in Zusammenhang stehenden Strafzahlungen, und weniger im Bereich von kritischen Systemen für Notruf-Leitstellen oder im Katastrophenschutz bei denen es um Menschenleben geht. In diesen Bereichen würde er zwar keine vollkommen unwirtschaftlichen Systeme entwerfen, aber kostenmäßig auch keine Abstriche machen. „Wir vertreten auch die Meinung, dass das gemacht werden muss und das kostet halt etwas“, meint er dazu.(P1, 2024, l. 85)

P2/P3: Aus den Überlegungen des *Business Continuity Management (BCM)* heraus wurde versucht abzuschätzen was es finanziell bedeutet, wenn bestimmte Systeme eine Zeit lang nicht verfügbar sind, aber es hat sich herausgestellt, dass das nur schwer mit einer allgemein gültigen Formel berechenbar ist. Ein möglicher Imageschaden kann etwa kaum monetär bemessen werden. Darum wird in dieser Organisation von einer zu strikten, akademischen Beurteilung der Wirtschaftlichkeit abgesehen. Stattdessen herrscht die Meinung, dass die Sicherheit nie vernachlässigt werden sollte nur wegen ein paar

zusätzlicher Euro die das Produkt dann kostet. Schlussendlich werden seitens des Security-Teams aber die Risiken und auch die Lösungen aufgezeigt, aber es obliegt schlussendlich der Geschäftsführung darüber zu entscheiden.

P4: Betont, dass zuallererst der wirtschaftliche Erfolg der Produkte und Dienstleistungen gegeben sein muss und sieht Sicherheitsanforderungen mehr als Hygienefaktoren, die zwar erfüllt sein müssen aber beim Kunden keine Begeisterung auslösen, wenn sie erfüllt sind. In der Beurteilung der Wirtschaftlichkeit berechnet er das Schadensvolumen pro Jahr in Euro, indem er die Eintrittswahrscheinlichkeit mit dem Schadenspotenzial multipliziert, wobei in die Beurteilung des Schadens ein entgangener Umsatz ebenso berücksichtigt wird wie mögliche Strafzahlungen, unproduktive Personentage und Kosten für die Wiederherstellung. Auf der anderen Seite werden die Kosten in CAPEX und OPEX pro Jahr bemessen. Diese Werte werden einander gegenübergestellt und so die Wirtschaftlichkeit bemessen. In dieser Berechnung sind immer gewisse Annahmen und Schätzungen enthalten, die bei der Entscheidung mit dokumentiert werden.

P5: Bewertet die Wirtschaftlichkeit über eine einfache Kosten-Nutzen-Analyse. In die Kosten werden sowohl die Investitions- als auch die Personalkosten eingerechnet und dem maximalen Schaden, der über Eintrittswahrscheinlichkeit mal Schadenspotenzial berechnet wird, gegenübergestellt. Allerdings weist er darauf hin, dass Security immer ein Versicherungsprodukt und kein Teil vom Kerngeschäft ist, daher muss eine Investition darin immer auch argumentiert werden. Und letztendlich ist es dann die Entscheidung des Managements ob die Investition getätigt oder das Risiko getragen wird.

P6: Findet es schwierig, wenn auf den kommerziellen Aspekt zu viel wert gelegt wird, denn Security ist aus seiner Sicht ein Vertrauens- und ein Qualitätsthema. Was nicht heißt, dass sein Unternehmen nur hochpreisige Lösungen anbieten würde. Ganz im Gegenteil, oft werden zunächst nur die „Low-hanging-Fruits“ adressiert und versucht mit kleinen Maßnahmen den Security Reifegrad zu verbessern. Das können auch nur Konfigurationen oder kleine Prozessänderungen sein. Bewertet werden die einzelnen Maßnahmen schließlich in Ampelfarben, wobei in die Bewertung einerseits einfließt wie viel die Anschaffung kostet und wie viel Aufwand es ist diese zu integrieren, und auf der anderen Seite welche Auswirkungen sie auf den Security-Reifegrad haben.

P7: Weist auf das NIS-Gesetz und die DSGVO hin, laut denen die Maßnahmen im Rahmen der wirtschaftlichen Möglichkeiten durchzuführen sind. Weist aber auch darauf hin, dass es eine grundsätzliche Frage ist, welchen Maßstab man für die Bewertung der

Risiken heranzieht, denn bei kritischen Infrastrukturen müssen nicht nur die finanziellen Auswirkungen für die einzelnen Unternehmen herangezogen werden, sondern auch jene für die Gesellschaft. In der Beurteilung wie viel das wert ist und wie viel es kosten darf muss das also mitberücksichtigt werden. Entsprechend gibt es zunehmend Gesetze und Regulierungen, die hier klare Grenzen festlegen.

Zusätzlich gibt er zu bedenken, dass das Risiko in der technischen Risikoanalyse über die Bedrohung und die Verwundbarkeit ermittelt werden sollte und nicht über die Eintrittswahrscheinlichkeit. Der Grundgedanke dahinter ist, dass die Einschätzung der Eintrittswahrscheinlichkeit von Sicherheitsvorfällen oft schwierig ist, weil es viele unbekannte Variablen gibt. Daher werden zum einen die Bedrohungen bestimmt, denen das System ausgesetzt ist, und zum anderen die Verwundbarkeiten, also die Schachstellen im System die ausgenutzt werden könnten.

P8: Eine Risikoabschätzung wird durchgeführt und Risiko-Kategorien werden zugeordnet, und anhand dieser erfolgt die Einstufung des Service. Danach wird der maximale Schaden geschätzt und dem Invest gegenübergestellt, und anhand dessen wird entschieden ob die Investition getätigt wird oder nicht. Die Bewertung von noch nicht eingetretenen Security-Vorfällen monetär zu bewerten ist dabei eine große Herausforderung und dem Vorstand oft schwierig zu verkaufen.

Fazit

Die Beurteilung der Wirtschaftlichkeit von Sicherheitsanforderungen variiert stark je nach Fokus und Prioritäten der jeweiligen Organisation. Während einige den wirtschaftlichen Aspekt stark berücksichtigen, steht bei anderen die Notwendigkeit der Sicherheitsmaßnahmen, unabhängig von den Kosten, im Vordergrund. Gesetzliche Vorgaben und der gesellschaftliche Kontext spielen ebenfalls eine wichtige Rolle in der Entscheidungsfindung.

6.5.1 Return on Security Investment (ROSI)

Diese Kapitel bezieht sich auf die Aussagen der Security Expert_innen zu der Berechnung eines Return on Security Investment und wie in ihrer Organisation in Bezug auf Sicherheitsanforderungen mit solchen betriebswirtschaftlichen Kennzahlen umgegangen wird.

Die wesentlichen Aussagen lassen sich wie folgt zusammenfassen:

P1: Sieht in seinem Bereich keine ROSI-Berechnung und hält diese für Systeme zur Abwehr von Gefahren auf Menschenleben auch nicht für durchführbar.

P2/P3: In ihrer Organisation kommt es schon vor, dass Security-Vorschläge hart hinterfragt werden, aber die Investition wird nicht mittels Standard-Formel bewertet oder ein ROSI berechnet.

P4: In seinem Unternehmen ist es normal, dass die Investitionen monetär bewertet und ein ROSI berechnet wird, auch wenn dies bei ihnen nicht also ROSI bezeichnet wird. Er nennt auch ein konkretes Beispiel, das aufgrund seiner schlechten Wirtschaftlichkeit nicht umgesetzt worden ist.

P5: Kennt das Konzept des Return on Security Investment und ist ihm auch schon häufiger begegnet. Er hält es für nachvollziehbar solche betriebswirtschaftlichen Kennzahlen auch für Sicherheitsmaßnahmen zu berechnen und sie auch rückwirkend zu prüfen. Er schildert etwa ein Unternehmen bei dem es üblich war die berechneten Business Cases ein Jahr nach deren Umsetzung durch den ursprünglichen Projektleiter noch einmal zu validieren.

P6: Seine Organisation beurteilt die Kosten nicht in Euro-Werten, sondern nur in den Bandbreiten niedrig, mittel und hoch, und die Wirtschaftlichkeit wiederum nur in Ampelfarben.

P7: Kennt Unternehmen bei denen versucht wird einen ROSI zu berechnen, allerdings stoßen die immer wieder auf die Probleme der quantitativen Risikoanalyse, da es schwierig ist wirklich verlässliche und belastbare Zahlen zu der Quantifizierung von Sicherheitsrisiken zu erhalten. Selbst als Unternehmen berechnen sie den ROSI nicht.

P8: In seiner Organisation berechnen sie den ROSI nicht, er fände es aber grundsätzlich interessant das zu tun. Er könnte sich vorstellen den ROSI dafür zu nutzen um gegenüber den anderen Stakeholdern den Mehrwert der Security darzustellen. Er schildert das Problem, dass die Security mehr als Kritiker oder gar Verhinderer wahrgenommen wird, die viel Geld kostet, und der ROSI könnte eine Möglichkeit sein das zu entkräften.

Fazit:

Die Anwendung des Return on Security Investment (ROSI) zur Bewertung von Sicherheitsmaßnahmen variiert zwischen den Organisationen. Während einige das

Konzept kennen und anwenden, stoßen andere auf praktische Schwierigkeiten bei der quantitativen Risikoanalyse oder verzichten ganz auf die Berechnung. In einigen Fällen wird die Wirtschaftlichkeit von Investitionen zwar monetär bewertet, aber nicht explizit als ROSI bezeichnet. Der ROSI könnte jedoch dazu beitragen, den Wert von Sicherheitsmaßnahmen gegenüber anderen Stakeholdern besser zu kommunizieren.

6.6 Vertraulichkeit & Integrität vs. Verfügbarkeit

Dieses Kapitel behandelt schließlich die Meinungen der Expert_innen über den Zusammenhang von hohen Anforderungen an Vertraulichkeit & Integrität einerseits und einer hohen Systemverfügbarkeit andererseits.

Die wesentlichen Kernaussagen in dieser Kategorie sind:

P1: Sieht in Bezug auf kritische Systeme wie Notruf-Leitstellen durchaus einen gewissen Widerspruch zwischen hohen Anforderungen an Vertraulichkeit & Integrität und einer hohen Verfügbarkeit, auch wenn er darauf hinweist, dass alle drei gleichwertige Schutzziele der IT-Security sind. Insbesondere weist er auf mögliche Probleme mit Verschlüsselungssystemen und Authentifizierungsdiensten hin, die fehleranfällig sein können, weil sich durch deren technische Komplexität wiederum Schachstellen auftun können. Gleichzeitig gibt er zu bedenken, dass es für solche Systeme eine Vielzahl von technischen und organisatorischen Maßnahmen für deren physischen Schutz gibt und ein unbefugter Zugang zu den Systemen nahezu ausgeschlossen werden kann. Er hält es daher für angemessen zugunsten der Verfügbarkeit bei anderen Schutzmaßnahmen wie Verschlüsselung und Authentifizierung Abstriche zu machen. Er ist der Meinung, dass in solchen Systemen über das Maß an Vertraulichkeit durchaus diskutiert werden kann und man sie hier im Verhältnis zur Verfügbarkeit nicht überbetonen muss.

P2/3: Sind der Meinung, dass man in jedem System eine Balance zwischen Prävention, Detektion und Reaktion finden muss. So finden sie, dass es legitim sein kann auf präventive Maßnahmen zu verzichten, wenn im Störungsfall eine hinreichend schnelle Detektion und Reaktion gegeben ist. Um aber in den Bereich der Höchstverfügbarkeit zu gelangen muss auch viel in die Prävention investiert werden und bereits beim kleinsten Verdacht auf eine Fehlfunktion reagiert werden, noch bevor diese wirklich schlagend wird. Den Zusammenhang zwischen Sicherheitsmaßnahmen und Verfügbarkeit sehen sie als zweischneidiges Schwert. Zum einen erhöhen die Sicherheitsmaßnahmen die Komplexität und erhöhen so das Risiko von Ausfällen. Zum anderen erhöhen zu wenige

Sicherheitsmaßnahmen die Angriffsflächen und können auf diese Weise ebenso die Verfügbarkeit verringern.

P4: Sieht mit Verweis auf die CIA Triade per se keinen Widerspruch in einer hohen Verfügbarkeit und hohen Anforderungen an Vertraulichkeit & Integrität, gibt aber zu bedenken, dass mit jeder Maßnahme die Komplexität steigt und jede zusätzliche Komponente eine Komponente mehr ist, die ausfallen kann. Außerdem meint er, dass es legitim ist einzelne Maßnahmen aus wirtschaftlichen Gründen nicht umzusetzen.

P5: Sieht es als eine Aufgabe des Risikomanagements sich zu überlegen wie man aus seinen begrenzen Ressourcen für die Security am meisten herausholen kann und meint, dass das immer eine Art Kompromiss ist. Er empfiehlt daher gemeinsam mit dem Business eine Art Scoring-System zu verwenden um festzulegen wo die Prioritäten liegen sollen, und das kann durchaus ergeben, dass die Erfüllung des einen Schutzziels Abstriche in der Erfüllung eines anderen bewirkt. Insbesondere geht er aber auch auf die Problematik der Komplexität ein. Um eine hohe Verfügbarkeit zu erreichen bedarf es vieler Redundanzen und das wiederum erhöht die Komplexität des Ganzen, und es stellt sich die Frage, ob diese Komplexität von dem IT-Betrieb noch beherrschbar ist. Er gibt zu bedenken, dass die einfachen Lösungen womöglich doch die resilientesten sind.

P6: Berichtet darüber, dass sich Usability, Performance und Security häufig in die Quere kommen und man entsprechend abwägen muss auf welche Faktoren man seine Schwerpunkte legt. Im Fall von kritischen Systemen, insbesondere bei Systemen im Notfall- und Katastrophenmanagement, betrachtet er die Verfügbarkeit als größeres Thema als die anderen, auch wenn er betont, dass die Verfügbarkeit genauso wie die Vertraulichkeit und die Integrität Schutzziele derselben Ebene sind und alle betrachtet werden müssen. In Bezug auf das Erreichen einer hohen Verfügbarkeit betont er allerdings auch, dass das auch eine Komplexitätsfrage ist. Eine starke Redundanz erhöht die Komplexität der Infrastruktur oder der Applikation und entsprechend ist es schwieriger diese sicher zu designen und auch zu betreiben. Das wiederum führt zu höheren Aufwänden, und das alles muss in der Architekturentscheidung mitberücksichtigt werden.

P7: Weist darauf hin, dass die Verfügbarkeit zu denselben Schutzzielen der Security gehört wir die Vertraulichkeit und die Integrität, auch wenn häufig, wenn man von Sicherheit spricht, vor allem die Vertraulichkeit gemeint ist und eventuell noch die Integrität. Aber sämtliche Standards, die er kennt, würden alle drei Bereiche adressieren

und in seiner Interpretation geht es immer darum ein angemessenes Niveau der Anforderungen in den jeweiligen Bereichen zu finden. Und diese Anforderungen müssen nicht immer hoch sein. In Bezug auf kritische Systeme bringt er etwa das Beispiel, dass man am Leitstand von einem Kraftwerk kein hoch-sicheres Passwort verwenden kann, weil der Operateur ständig einen Zugriff auf das System haben muss. In Bezug auf Leitsysteme berichtet er, dass es durchaus State-of-the-Art ist diese ohne Passwortschutz, also ohne Authentifizierung betreiben, was bei anderen Anwendungen undenkbar wäre. Kompensiert wird das allerdings durch andere Schutzmaßnahmen, wie im Fall des Leitsystems mit einem Schutz der physischen Umgebung des Leitsystems.

P8: Versucht eine Balance zwischen Usability, Security und Kosten zu finden und nimmt sich in Bezug auf die Umsetzung von Sicherheitsmaßnahmen die 80:20 Regel zum Vorbild. Er versucht 80% der Risiken zu behandeln und für die verbleibenden 20%, die zumeist mit hohen Kosten verbunden sind, nur noch risikominimierende Maßnahmen einzusetzen. In der Beurteilung der Maßnahmen überwiegen also die Komplexität und die Kosten der Umsetzung und ein gewisses Restrisiko wird dann in Kauf genommen. Dies gilt sowohl für Sicherheitsmaßnahmen in Bezug auf externe Zugriffe als auch für welche die nach intern gerichtet sind. Er berichtet etwa, dass sie bei sich im Unternehmen eine zentrale *Privileged Access Management* Lösung einsetzen, die sicherstellt, dass nur befugte Personen auf ein System zugreifen können bzw. auch, dass der Zugriff auf diese Systeme nie direkt, sondern über sogenannte Sprung-Server erfolgen muss. Das Problem damit ist allerdings, dass dieses System einen Single-Point-of-Failure darstellt und es eine alternative Möglichkeit braucht um sich auf die Systeme verbinden zu können, falls dieses Hauptsystem nicht verfügbar ist. Und diese wiederum unterminiert gewissermaßen den Schutz des Systems. Da sich das aber nicht verhindern lässt, wird an dieser Stelle risikominimierend gearbeitet und ein verstärktes Monitoring eingesetzt.

Fazit:

Die Experten erkennen die Notwendigkeit, eine Balance zwischen Vertraulichkeit & Integrität einerseits und hoher Verfügbarkeit andererseits zu finden. Hohe Verfügbarkeit kann durch die Komplexität von Sicherheitsmaßnahmen beeinträchtigt werden, während unzureichende Sicherheitsmaßnahmen die Angriffsflächen vergrößern. In kritischen Systemen kann es legitim sein, zugunsten der Verfügbarkeit Abstriche bei anderen Schutzmaßnahmen zu machen. Risikomanagement und die Berücksichtigung wirtschaftlicher Faktoren sind aus Sicht mancher Expert_innen ebenfalls wichtig, um ein angemessenes Niveau der Anforderungen zu gewährleisten, gerade in Bezug auf die Wirtschaftlichkeit gehen die Meinungen aber deutlich auseinander. Alternative

Zugangsmöglichkeiten und redundante Systeme müssen sorgfältig geplant werden, um Single Points of Failure zu vermeiden und die Gesamtresilienz zu erhöhen.

7 Diskussion

In diesem Kapitel werden abschließend die Ergebnisse der Literaturstudie jenen der Expert_innen-Interviews gegenübergestellt, zusammengefasst und interpretiert. Im Anschluss daran kann schließlich die Forschungsfrage beantwortet werden.

Zusätzlich wird die angewandte Forschungsmethode kritisch reflektiert und es werden Aspekte angeführt die durch diese Arbeit erst aufgezeigt und/oder darin nicht ausreichend betrachtet werden konnten und somit für eine zukünftige Forschung herangezogen werden könnten.

7.1 Zusammenfassung und Beantwortung der Forschungsfrage

In Kapitel 4 wurden anhand der Literaturrecherche bestimmte Erwartungshaltungen in Bezug auf die Anforderungsquellen, die Anforderungen an Vertraulichkeit und Integrität, die Strategien zur Erreichung von Hochverfügbarkeit und die Berücksichtigung der Wirtschaftlichkeit gebildet. Diese werden nun den aus den Expert_innen-Interviews gewonnenen Erkenntnissen gegenübergestellt.

7.1.1 Anforderungsquellen

Die in Kapitel 4 aufgestellte Erwartungshaltung, dass die Expert_innen in Analogie zur Anlage 1 der NIS-Verordnung eine risikobasierte Vorgangsweise anwenden würden wurde weitestgehend bestätigt. Mehrere der Expert_innen strichen im Gespräch diesen Ansatz hervor und verwiesen auf seine grundlegende Bedeutung für die Bestimmung der Anforderungen. Allerdings nannte keine_r der Expert_innen unmittelbar die NIS-Richtlinie als Anhaltspunkt und nur eine_r erwähnte sich überhaupt. Nichtsdestotrotz hat sich in Bezug auf die Referenz-Modelle und Best Practices bestätigt, dass mehrere der in den NIS-Factsheets angegebenen Standards und Normen herangezogen werden würden um die Anforderungen zu bestimmen. Insbesondere die ISO/IEC 27000 wurde mehrfach genannt, aber auch die CIS Controls. Dass die Expert_innen ein bis zwei weitere Modelle heranziehen würden hat sich ebenfalls bestätigt, denn mit Ausnahme eines der Interviews wurden in allen anderen mehrere genannt. Nicht bestätigt hat sich hingegen der Bezug auf das österreichische Sicherheitshandbuch. Dieses nannte nur eine_r der Expert_innen als gut geeignete Quelle, während die andere es zwar kannten aber nicht unmittelbar einsetzen würden. Mehrere waren überhaupt der Ansicht, dass es den Privatsektor gar nicht adressieren würde. Noch weniger von Bedeutung wurden die Ö-

Normen angesehen, die – obwohl welche in den NIS-Factsheets als Referenz angegeben werden – keine_r der Expert_innen für relevant hält. Einige geben dazu aber zu bedenken, dass auch für andere, internationale Standards Ö-Normen existieren, wie für die ISO/IEC 27000, und diese somit implizit auch berücksichtigt sein könnten.

7.1.2 Vertraulichkeit und Integrität

In Bezug auf die Anforderungen an Vertraulichkeit und Integrität haben sich die in Kapitel 4 aufgestellten Erwartungen vollinhaltlich erfüllt. In den Interviews wurden speziell die Themen Verschlüsselung, Authentifizierung und Autorisierung sowie die Absicherung der Schnittstellen mittels Reduktion der Angriffsfläche mehrmals genannt und als die entscheidenden Faktoren betont. Zusätzlich wurden weitere, zentrale Sicherheitsaspekte genannt. Allen voran wurde die Bedeutung eines vollständigen und gepflegten Asset-Managements mehrfach hervorgehoben.

7.1.3 Verfügbarkeit

Bezogen auf Maßnahmen zur Erreichung einer hohen Verfügbarkeit erfüllt sich die Erwartung, dass die Expert_innen vor allem auf Redundanzen setzen würden und sie deren Umsetzung auf sämtlichen Ebenen empfehlen. Ebenso bestätigt sich, dass sie diese nicht nur auf eine reine Duplizierung der Komponenten anwenden, sondern sie auch auf eine Diversität von kritischen Komponenten achten. Manche Expert_innen geben darüber hinaus zu bedenken, dass auch auf personeller Ebene Redundanzen geschaffen werden müssen um sich nicht von einzelnen Personen abhängig zu machen.

In Bezug auf die Verwendung externer Dienste und die dadurch steigende Systemkomplexität gehen die Meinungen der Expert_innen hingegen auseinander, daher erfüllt sich die in Kapitel 4.3 formulierte Erwartungshaltung nur zum Teil. Während mehrere Expert_innen betonen, dass sie in ihren kritischen Systemen von externen Diensten möglichst unabhängig sein wollen halten das andere nicht für problematisch, solange auch bei ihnen eine ausreichende Redundanz gewährleistet ist. Manche Expert_innen heben sogar hervor, dass die Verwendung externer Dienste aufgrund der dadurch erreichten Diversität die Verfügbarkeit sogar erhöhen kann. Die steigende Komplexität wird allerdings größtenteils erkannt und als kritisch angesehen, daher wird eine Risikoanalyse und eine sorgfältige Planung empfohlen.

Der Umgang mit dem Security by Design Prinzip variiert zwischen den Expert_innen ebenfalls und wird daher auch nur teilweise den Erwartungen gerecht. Sämtliche befragte

Expert_innen kennen zwar den Begriff und befürworten den dahinterliegenden Ansatz, in dessen praktischer Umsetzung sehen viele aber noch Handlungsbedarf. Andere hingegen haben in ihren Organisationen das Prinzip bereits vollständig und mit Tools unterstützt umgesetzt. Diese Integration reicht dabei teilweise so weit, dass sie selbst in der Organisation spezifische Rollen geschaffen haben, welche die Security by Design Denkweise in das Bewusstsein der Mitarbeiter bringen und dessen Zielerreichung sicherstellen.

In Bezug auf das Erreichen einer hohen Verfügbarkeit haben schließlich einige der Expert_innen die Bedeutung des Testens der Sicherheits- und Redundanzmaßnahmen hervorgehoben, weswegen dieses als zusätzlicher Aspekt aufgenommen und dediziert behandelt wurde. Die vorgeschlagenen Methoden reichen von regelmäßigen Funktionstests über Performance- und Penetration-Tests bis hin zu Red-Team Audits zum Aufspüren von Sicherheitslücken und zum Optimieren der internen Prozesse. Besonders hervorzuheben ist das Testen der Redundanzen und der Verbindungswege zwischen ihnen. Hier wird empfohlen diese in den normalen Systemablauf vollständig zu integrieren und dadurch permanent zu erproben, anstatt sie nur auf Abruf bereit zu halten. Manche Expert_innen gehen auch noch einen Schritt weiter und empfehlen auch den plötzlichen Ausfall von Systemkomponenten permanent zu üben, um so auch den Ausfall zu einer normalen Situation zu machen und darauf vorbereitet zu sein.

7.1.4 Wirtschaftlichkeit

Bezogen auf die Wirtschaftlichkeit werden die Erwartungen des Kapitels 4.4 nur teilweise erfüllt, denn der Umgang damit unterscheidet sich zwischen den Expert_innen deutlich. Während es für manche Expert_innen Usus ist für die Beurteilung der Wirtschaftlichkeit von Sicherheitsmaßnahmen ganz konkrete, monetäre Kosten-Nutzen-Analyse durchzuführen, arbeiten andere Expert_innen nur mit qualitativen Einschätzungen in Ampelfarben oder Kategorien, und wieder andere messen der Wirtschaftlichkeit eine untergeordnete Bedeutung zu und empfehlen diese nur bedingt zu berücksichtigen. Entsprechend verhält es sich auch bei der Berechnung eines Return on Security Investment. Alle Expert_innen kennen zwar den Begriff, auch wenn manche ihn in ihren Organisationen nicht so nennen, aber ob in welcher Form dieser berechnet wird hängt von der jeweiligen Organisation ab.

7.1.5 Vereinbarkeit von Vertraulichkeit & Integrität mit Verfügbarkeit

In Bezug auf die Vereinbarkeit von hohen Anforderungen an Vertraulichkeit & Integrität einerseits und einer hohen Verfügbarkeit andererseits weisen mehrere der Expert_innen darauf hin, dass alle drei Aspekte ebenbürtige Schutzziele der Informationssicherheit, der sogenannten CIA-Triade, sind und demnach in keinem Widerspruch zueinander stehen. Gleichzeitig herrscht aber auch Einigkeit bei den Expert_innen darüber, dass für jedes System anhand seiner Risikoeinschätzung individuell beurteilt werden muss auf welche dieser Aspekte der Schwerpunkt gelegt werden soll. Das wiederum impliziert, dass der Fokus auf den einen Bereich sehr wohl Abstriche bei einem anderen Bereich bewirken kann und dass das auch so in Ordnung ist, sofern es durch die individuellen Anforderungen des Systems gerechtfertigt ist. Die Empfehlung der Expert_innen ist es daher auf Basis der Risikoanalyse ein ausbalanciertes Niveau zwischen den drei Schutzzielen zu finden. Und im Extremfall kann das schließlich sogar bedingen, dass selbst zentrale Anforderungen an Vertraulichkeit und Integrität, wie es die Authentifizierung und Autorisierung - also Kernanforderungen sowohl der Literatur als auch der befragten Expert_innen - darstellen (siehe dazu die Erläuterungen in Kapitel 7.1.2), in einzelnen, kritischen Systemen schlicht nicht umgesetzt werden. Dies unterstreicht der Fall von Leitsystemen in Kraftwerken, bei denen es gelebte Praxis ist, dass es keine Passwortsicherung gibt.

Die Forschungsfrage dieser Arbeit, ob sich in Bezug auf kritische Systeme mit externen Schnittstellen sowohl hohe Anforderungen im Bereich der Vertraulichkeit und Integrität als auch eine hohe Systemverfügbarkeit gleichzeitig umsetzen lassen, kann daher nicht eindeutig und vollumfänglich beantwortet werden. Die hier durchgeführte Forschung hat zwar gezeigt, dass es Konstellationen gibt, in denen es akzeptiert ist zugunsten einer hohen Verfügbarkeit selbst auf absolute Basis-Anforderungen an Vertraulichkeit und Integrität vollkommen zu verzichten, eine allgemeingültige Aussage ist das allerdings nicht. Stattdessen soll eine solche Entscheidung auf Basis der Risikoanalyse und der individuellen Bedürfnisse des Systems getroffen werden. Allerdings basiert eine solche Risikoanalyse auf subjektiven Einschätzungen und die Anforderungen an die Systeme ebenso, daher ist die Entscheidung über die umzusetzenden Sicherheitsmaßnahmen keine objektive, sondern eine Frage der individuellen Argumentation. Objektiv lassen sich diese im Kontext dieser Arbeit weder anhand der Literatur noch anhand der Expert_innen-Aussagen eindeutig festlegen.

7.2 Offenbarte Problemfelder

Die in dieser Arbeit durchgeführte Forschung hat mehrere Problemfelder offenbart. Ein Problemfeld ist die große Anzahl an Standards, Normen, Frameworks und Best Practises die es im Umfeld der Informationssicherheit gibt. Für jede Zielgruppe, sei es Management-Ebene, operative Ebene oder technische Ebene, stehen mehrere solcher Werke zur Verfügung, von denen jedes für sich sehr umfangreich ist. Entsprechend schwierig gestaltet es sich festzustellen wo es zwischen ihnen Überschneidungen gibt und worin sie sich unterscheiden, daher kann nicht eindeutig festgelegt werden an welchen von ihnen man sich orientieren soll. In der praktischen Anwendung gehen Unternehmen daher dazu über sich nicht auf einen einzigen, konkreten Standard zu beziehen, sondern eine eigene Software zu nutzen, welche die Anforderungen der unterschiedlichen Standards miteinander kombiniert. Eine_r der Expert_innen hat diese als Meta-ISMS bezeichnet.

Ein weiteres Problemfeld stellt die Beurteilung von Sicherheitsrisiken dar, die sogenannte Risikoanalyse. Diese basiert zumeist nur auf qualitativen Einschätzungen die von Expert_innen vorgenommen werden, und nicht auf quantitativ messbaren und sind dementsprechend subjektiv. Dies betrifft sowohl die Einschätzung der Eintrittswahrscheinlichkeit von Risiken als auch die Bemessung der Auswirkungen von Sicherheitsvorfällen. Beides sind am Ende des Tages nur Schätzungen.

Ein Folge-Problemfeld stellt die Wirtschaftlichkeitsprüfung von Sicherheitsmaßnahmen dar. Hier stellt sich einerseits die Frage inwiefern die Wirtschaftlichkeit bei der Umsetzung von kritischen Systemen überhaupt eine entscheidende Rolle spielen darf und andererseits wie die Wirtschaftlichkeit bestimmt werden kann. Da sowohl die Risiken als auch die Auswirkungen von Sicherheitsvorfällen auf Schätzungen beruhen suggeriert die Formel zur Berechnung des Return on Security Investment eine mathematische Schein-Genauigkeit, die nicht gerechtfertigt erscheint.

Als Konsequenz des oben Gesagten ist schließlich auch die Beurteilung der Angemessenheit von Sicherheitsmaßnahmen ein Problemfeld. Das NIS-Gesetz verlangt wie beschrieben in §17 (1), dass die Sicherheitsmaßnahmen den Stand der Technik berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen sein müssen. Unabhängig von dem nicht näher erläuterten vernünftigen Aufwand sind entsprechend der obigen Argumentation auch weder der Stand der Technik noch das Risiko eindeutig feststellbar. Entsprechend ist es selbst in Bezug auf das NIS-Gesetz aus Sicht des Autors nicht möglich objektiv festzustellen ob eine

Sicherheitsmaßnahme umgesetzt werden muss und/oder gerechtfertigt ist. Stattdessen ist es rein eine Frage der Argumentation und somit subjektiv.

Angesichts des technischen Themengebiets dieser Arbeit und des der Informatik anhaftenden, mathematischen korrekten Rufs, zeichnen die angeführten Problemfelder ein für den Autor überraschend vages und undeterministisches Bild. Dies erklärt allerdings die unterschiedlichen Aussagen der Expert_innen, die ebenso viele Überlappungen wie unterschiedliche Sichtweisen gezeigt haben.

7.3 Gegenüberstellung der Forschungsergebnisse

In der Einleitung wurden zwei Arbeiten hervorgehoben und deren Zusammenhang mit dieser Masterarbeit betont. Dies sind einerseits die Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen (Ulrike Lechner et al., 2018) und andererseits der Themenband Resilienz (Volker Wittpahl, 2023). In diesem Kapitel werden nun die Ergebnisse dieser Arbeiten miteinander verglichen, Überschneidungen dargestellt und Unterschiede hervorgehoben.

7.3.1 Gegenüberstellung mit den Fallstudien zur IT-Sicherheit

In den Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen wurde die sogenannte *eXperience Methodik* eingesetzt um die Fallstudien durchzuführen und die Ergebnisse auszuwerten. Diese Methodik soll speziell ein authentisches Wissen rund um E-Business und IT-Management vermitteln. Von den durchgeführten Studien ist vor allem jene in Kapitel 11 über die IT-Sicherheit in der zentralen Leitstelle Ostthüringen mit dem Kontext dieser Arbeit vergleichbar. Hier wurde untersucht welche Maßnahmen umgesetzt wurden um eine hohe Verfügbarkeit der Leitstelle zu erreichen um permanent in der Lage zu sein Notrufe entgegenzunehmen und abzuwickeln.

Gemeinsamkeiten

In Übereinstimmung mit den Erwartungen und den Aussagen der in dieser Arbeit befragten Expert_innen setzt die Leitstelle auf Redundanzen ihrer Kernkomponenten, um eine hohe Verfügbarkeit zu erreichen, und zwar sowohl auf organisatorischer, prozessualer und auf technischer Ebene. Die umgesetzten Maßnahmen reichen von der Definition von drei Rückfall-Ebenen aus Prozesssicht, die jeweils zum Tragen kommen wenn eine der Kernkomponenten ausfallen sollte, über die Beschaffenheit und Sicherheit der Arbeitsplatzrechner der Disponenten bis hin zur redundanten Netzwerkanbindung

und ISDN-Leitung, welche wiederum über mehrfache Zubringerleitungen integriert worden sind. Zusätzlich wurde eine Kaltreserve für essenzielle Komponenten geschaffen, sodass diese ich Notfall rasch ersetzt werden können. Ebenfalls wurde Hervorgehoben, dass versucht worden ist, die externen Abhängigkeiten der Leitstellen möglichst gering zu halten, was sich dadurch manifestiert, dass das System weitestgehend autonom ist und nur wenige externe Schnittstellen bestehen.

Ebenso im Einklang mit den Erkenntnissen dieser Arbeit wurde auch das regelmäßige Trainieren von Systemausfällen und die entsprechende Aktivierung der Rückfall-Ebenen als besonders wichtig herausgestrichen.

Unterschiede

In der Fallstudie wird nicht explizit darauf eingegangen welche Herangehensweise die Leitstelle genutzt hat um die Anforderungen an die IT-Sicherheit festzulegen, allerdings wird deren Einstufung als kritische Infrastruktur (KRITIS) hervorgehoben, aufgrund derer sich eine Reihe von regulatorischen Anforderungen ergeben. In Deutschland sind das allen voran das IT-Sicherheitsgesetz 2.0 und das BSI-Gesetz. Diese können als Pendant zum österreichischen NIS-Gesetz und der NIS-Verordnung gesehen werden. Ob und wenn ja inwiefern weitere Standards und Normen in die Definition der konkreten Sicherheitsmaßnahmen der Leitstelle eingeflossen sind, geht aus der Fallstudien-Beschreibung nicht hervor.

Ebenso nimmt die Fallstudie keinen Bezug darauf ob zugunsten der Verfügbarkeit auf die Umsetzung von anderen Sicherheitsmaßnahmen verzichtet wurde. Er werden zwar spezielle technische Maßnahmen erwähnt, wie dass der direkte Zugriff der Arbeitsplatzrechner auf das Internet unterbunden wird, als auch organisatorische, wie der Einsatz von speziellen Schleusensystemen. Wie aber etwa mit der Authentifizierung und Autorisierung am Leitstellensystem umgegangen wird, wird ebenso wenig erläutert wie der Umgang mit Zertifikaten oder mit Verschlüsselung.

7.3.2 Gegenüberstellung mit dem Themenband Resilienz

Im Gegensatz zu den oben beschriebenen, konkreten Fallstudien bezieht sich der Themenband Resilienz in erster Linie auf die Literatur sowie auf einschlägige Berichte über aktuelle Sicherheitsereignisse. Von den darin vorgestellten Themenbereichen ist allen voran das Kapitel 10 über die Resilienz von kritischen und sensiblen Infrastrukturen im Kontext von modernen Kommunikationssystemen mit dem Themengebiet dieser

Arbeit überschneidend. Darin gehen die Autoren auf die zunehmende Vernetzung der Systeme im Zuge der voranschreitenden Digitalisierung ein und den Herausforderungen, die sich dadurch stellen. Insbesondere nennen sie auch einige, konkrete Vorfälle der jüngsten Vergangenheit, die aufgrund dieser Vernetzung zu teils globalen Systemausfällen geführt haben.

Gemeinsamkeiten

Übereinstimmend mit den Erkenntnissen dieser Arbeit betonen die Autoren die Notwendigkeit von Redundanzen auf allen Ebenen, geben aber gleichzeitig zu bedenken, dass diese angesichts der hohen Vernetzung und der komplexen Abhängigkeitsverhältnisse kaum noch erreichbar oder zumindest sehr teuer ist. Insbesondere wird auch hervorgehoben, dass Abhängigkeiten vermieden werden sollen, was auch bedeutet, dass Schlüsselkomponenten nur aus vertrauenswürdigen Quellen bezogen werden dürfen oder sogar aus eigener Produktion stammen müssen. Ebenso wird die unbedingte Notwendigkeit von Security by Design hervorgehoben, welche sogar zum Ansatz des *Resilience by Design* ausgebaut wird. Und in Bezug auf die Wirtschaftlichkeit von Sicherheitsmaßnahmen hinterfragen die Autoren ob diese wirklich zwingend gegeben sein muss und weisen darauf hin, dass die Dienste der kritischen Infrastruktur nicht nur für die jeweiligen Unternehmen gewinnbringend sein müssen, sondern vor allem auch eine gesellschaftliche Bedeutung haben. In Katastrophenfällen könne deren Verfügbarkeit oder Nichtverfügbarkeit sogar über Leben und Tod entscheiden.

Unterschiede

Auch diese Arbeit geht vor allem auf jene Sicherheitsanforderungen ein, die sich aufgrund der gesetzlichen Lage in Deutschland in Bezug auf die kritische Infrastruktur ergeben. Weitere Standards und Best Practices finden keine Erwähnung. Ebenso wird auch hier kein Bezug darauf genommen, dass zugunsten einer hohen Verfügbarkeit auf die Umsetzung anderer Sicherheitsmaßnahmen verzichtet werden kann. Dadurch, dass dieses Thema aber grundsätzlich nicht diskutiert wird, kann nicht festgestellt werden wie die Autoren dazu stehen.

7.4 Reflexion der Methode

Die Forschung in dieser Arbeit wurde mittels der Design Science Methode durchgeführt, die es einerseits verlangt ein (Design-)Artefakt zu erstellen und andererseits dieses zu evaluieren. In der Durchführung hat sie sich für den Autor lange Zeit als schwierig

herausgestellt, weil er sich die Frage gestellt hat wie dieses Artefakt genau beschaffen sein muss um es evaluieren zu können und wie diese Evaluation genau vonstattengehen soll. Schließlich war es ihm aufgrund der generischen Fragestellung nicht möglich ein konkretes Systemdesign zu entwickeln oder auch nur eine taxative Aufstellung von Sicherheitsanforderungen die geprüft werden könnten. Der Durchbruch dazu gelang schließlich im Austausch mit dem Betreuer, in dem das Artefakt definiert wurde als die Erwartungshaltung an die Umsetzung von kritischen Systemen, die auf Basis der Literaturstudie iterativ erstellt und schließlich mit Expert_innen-Interviews evaluiert wird.

In der Durchführung der Interviews hat sich Microsoft Teams einerseits bewährt, denn so konnten sie ortsunabhängig und flexibel durchgeführt werden. Mit der Aufzeichnung und den Transkriptionen gab es andererseits Probleme. Bei einem der Interviews ist Teams offensichtlich mit seinen internen Aufzeichnungs-IDs durcheinandergekommen und so führte der Link zu der Aufzeichnung des einen Interviews auf die Aufzeichnung eines vollkommen anderen. Ein Problem das auch mit Hilfe des IT Supports der FernFH nicht gelöst werden konnte und die Aufzeichnung des einen Interviews ging somit unwiederbringlich verloren. In Bezug auf die automatische Transkription offenbarte Teams weitere Schwächen. Trotz richtiger Sprachauswahl und einer aus Sicht des Autors weitestgehend akzentfreien, sauberen Aussprache der Interviewpartner war das automatisch erstellte Transkript nur mangelhaft und konnte lediglich als Ausgangspunkt herangezogen werden. Die Aufzeichnung und Transkription mit Microsoft Teams wurde daher nur für die ersten drei Interviews verwendet. Spätere Interviews wurden hingegen mit den aus Redundanz-Gründen parallel mitlaufenden, digitalen Sprachaufnahmen mit der Software MAXQDA 2024 transkribiert. Das lieferte wesentlich bessere Ergebnisse.

Die besagte Software MAXQDA 2024 kam auch bei der Auswertung der Interviews zum Einsatz. Diese erfüllte alle Erwartungen und war eine enorme Unterstützung, auch mit der hierfür angeschafften, limitierten Studenten-Lizenz.

7.5 Forschungsausblick

Für anschließende Forschungen bestehen aus Sicht des Autors mehrere Anknüpfungspunkte. Insbesondere wurden die Expert_innen-Interviews ausschließlich mit Männern durchgeführt, obwohl die Suche nach Expert_innen vollkommen offen gestaltet wurde. Es konnte aber im Netzwerk des Autors keine Frau in einer entsprechenden Position gefunden werden. Aus wissenschaftlicher Sicht wäre es

allerdings interessant auch die Meinungen von Frauen in ähnlichen Positionen einzuholen und mit den Ansichten der Männer zu vergleichen.

Dasselbe gilt auch für die Nationalität der befragten Expert_innen. Sämtliche befragte Expert_innen sind Österreicher_innen, von denen der Großteil im Osten Österreichs, im Ballungsraum Wien, beheimatet ist. Das Ergebnis dieser Forschung ist also nur für den österreichischen Raum, bestenfalls für die DACH-Region, repräsentativ und es stellt sich die Frage wie Expert_innen in anderen Regionen vorgehen würden.

Schließlich steht zum Zeitpunkt dieser Arbeit auch das NIS-Gesetz unmittelbar vor einer Novellierung und es wird erwartet, dass es im Laufe des kommenden halben Jahres veröffentlicht wird. Entsprechend stellt sich in Bezug auf die Sicherheitsanforderungen die Frage inwiefern sich die Anforderungen durch das geplante NIS2-Gesetz ändern werden bzw. ob die Kritikpunkte am NIS-Gesetz dann noch begründet sind.

7.6 Fazit

Die vorliegende Masterarbeit hat sich mit der Umsetzung von Sicherheitsanforderungen beschäftigt und dabei konkret untersucht ob in Bezug auf kritische Systeme hohe Anforderungen an die Vertraulichkeit & Integrität mit einer hohen Verfügbarkeit vereinbar sind. Um diese Fragestellung zu untersuchen wurde die Design Science Methode eingesetzt. Damit wurde zunächst anhand der Literatur iterativ eine Erwartungshaltung für die Umsetzung solcher Systeme formuliert, welche im Anschluss mithilfe von Expert_innen-Interviews auf den Prüfstand gestellt und evaluiert wurde.

Die Literaturstudie hat dabei gezeigt, dass es eine Vielzahl an Standards, Normen, Richtlinien und Best Practices gibt, die alle Sicherheitsanforderungen definieren und es schwierig ist jene auszuwählen, die für das konkrete System zum Einsatz kommen sollen. Daher wurde ein anderer Ansatz gewählt und ein Brückenschlag über das Netz- und Informationssystemsicherheitsgesetz (NISG) versucht, der österreichischen Umsetzung der europäischen NIS-Richtlinie. Dieses definiert gemeinsam mit der NIS-Verordnung und den Erklärungen des NIS-Factsheets konkrete Anforderungen für die Systeme der kritischen Infrastruktur und konnte so als Referenz für die Umsetzung allgemeiner, kritischer Systeme herangezogen werden. Neben diesen Anforderungen wurde auch das Security-by-Design Prinzip erläutert, welches eine Methode propagiert um die Sicherheit von Systemen von vornherein in deren Design zu berücksichtigen.

Im nächsten Schritt wurden einige Aspekte in der Umsetzung von Sicherheitsmaßnahmen ausgearbeitet. Diese reichen vom Risikomanagement zu Beginn, über die Art und Weise wie Hochverfügbarkeit erreicht und gemessen werden kann, weiter über die kritischen Aspekte einer hohen System-Komplexität bis hin zur Beurteilung der Wirtschaftlichkeit von Sicherheitsanforderungen. In diesem Abschnitt wurde also zusammengestellt wie sich die Sicherheitsanforderungen in der Praxis auswirken und welche Aspekte es hier zu berücksichtigen gilt.

Mit diesem theoretischen Input konnte schließlich definiert werden welche Erwartungen aus Sicht der Literatur an die Umsetzung von Sicherheitsanforderungen von kritischen Systemen bestehen, was das Ende des theoretischen Teils besiegelte und den empirischen Teil einläutete.

Zur Evaluierung der im theoretischen Teil aufgestellten Erwartungen wurden leitfadengestützte Interviews mit 8 Expert_innen aus 7 Organisationen durchgeführt. Diese Interviews wurden anschließend transkribiert und mithilfe der qualitativen Inhaltsanalyse nach Mayring ausgewertet.

Abschließend wurden die theoretischen Erwartungen mit den empirisch ermittelten, praktischen Empfehlungen der Expert_innen abgeglichen und somit evaluiert. Auf diese Art und Weise konnte schlussendlich die Forschungsfrage beantwortet und festgestellt werden, dass in Bezug auf die Verträglichkeit von hohen Anforderungen an Vertraulichkeit & Integrität einerseits und einer hohen Verfügbarkeit andererseits, keine allgemeingültige Aussage möglich ist. Zwar wurden deutliche Indizien festgestellt, dass es legitim ist zugunsten einer hohen Verfügbarkeit selbst auf zentralste Vertraulichkeits- und Integritäts-Anforderungen zu verzichten, eine allgemeine Regel dafür konnte aber weder aus der Literatur noch anhand der Expert_innen-Interviews aufgestellt werden.

8 Literaturverzeichnis

Amazon.com (2024). Was sind Microservices? aws. Online: https://aws.amazon.com/de/microservices/ [Abruf am 24.07.2024].

Andrea Held (2015). Hochverfügbarkeit und Downtime: Metriken. Informatik Aktuell. Online: https://www.informatik-aktuell.de/betrieb/verfuegbarkeit/hochverfuegbarkeit-und-downtime-metriken.html [Abruf am 01.07.2023].

Andrea Held (o. J.). Hochverfügbarkeit und Downtime: Eine Einführung. Informatik Aktuell. Online: https://www.informatik-aktuell.de/betrieb/verfuegbarkeit/hochverfuegbarkeit-und-downtime-eine-einfuehrung.html [Abruf am 09.04.2023].

A-SIT Zentrum für sichere Informationstechnologie – Austria (2017). Cloud Computing Kompass. Online: https://www.onlinesicherheit.gv.at/dam/jcr:da65575d-d91a-4795-983b-c5e5a753bd80/Cloud-Computing-Kompass.pdf [Abruf am 24.07.2024].

Atlassian (2024a). Microservice-Architektur. Atlassian. Online: https://www.atlassian.com/de/microservices/microservices-architecture [Abruf am 24.07.2024].

Atlassian (2024b). Vor- und Nachteile von Microservices, die du kennen solltest. Atlassian. Online: https://www.atlassian.com/de/microservices/cloud-computing/advantages-of-microservices [Abruf am 24.07.2024].

A-Trust GmbH (2024). PDF signieren. A-Trust. Online: https://www.a-trust.at/pdfsign/ [Abruf am 01.08.2024].

Austrian Standards International (2024). Sichere Apps für das Web. Austrian Standards. Online: https://www.austrian-standards.at/de/newsroom/pressemeldungen/sichere-apps-fuer-das-web [Abruf am 16.07.2024].

Axelos Ltd. (o. J.). ITIL® 4 and DevOps White Paper. AXELOS. Online: https://www.axelos.com/resource-hub/white-paper/itil-4-and-devops-white-paper [Abruf am 08.05.2023].

Brenner, Michael et al. (2022). Praxisbuch ISO/IEC 27001 (4., überarbeitete Auflage). München: Hanser.

Bundesamt für Sicherheit in der Informationstechnik (2002). Technische Grundlagen der Wurzelzertifizierungsstelle. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/VerwaltungsPKI/techwurzelz_pdf.pdf?__blob=publicationFile&v=1 [Abruf am 24.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2013a). Hochverfügbarkeitskompendium Band G Kapitel 7: HV-Prinzipien. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandG/G7_HV-Prinzipien.pdf?__blob=publicationFile&v=3 [Abruf am 22.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2013b). Hochverfügbarkeitskompendium Band G Kapitel 1: Einführung. Online:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandG/G1_Einfuehrung.pdf?__blob=publicationFile&v=4 [Abruf am 22.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2013c). Hochverfügbarkeitskompendium Band G Kapitel 2: Definitionen. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandG/G2_Definitionen.pdf?__blob=publicationFile&v=3 [Abruf am 22.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2017a). Sicherheit von Geräten im Internet der Dinge. Online: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_128.pdf?__blob=publicationFile&v=3 [Abruf am 17.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2017b). BSI-Standard 200-3. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2 [Abruf am 22.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2019). Kriterien für die Standortwahl von Rechenzentren. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.html [Abruf am 08.04.2023].

Bundesamt für Sicherheit in der Informationstechnik (2022). Mindeststandard des BSI zur Nutzung externer Cloud-Dienste. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste_Version_2_1.pdf?__blob=publicationFile&v=4 [Abruf am 24.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2023a). IT-Grundschutz-Kompendium. Köln: Bundesanzeiger-Verl.

Bundesamt für Sicherheit in der Informationstechnik (2023b). IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/itgrundschutzKompendium.html?nn=128568 [Abruf am 08.10.2023].

Bundesamt für Sicherheit in der Informationstechnik (2024a). Weltweite IT-Ausfälle. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Krisen-Grosslagen/Crowdstrike_Microsoft/Crowdstrike_Microsoft_node.html [Abruf am 24.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2024b). ISO 27001-Zertifizierung auf Basis von IT-Grundschutz. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html [Abruf am 11.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2024c). Hochverfügbarkeitskompendium Band G. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/HVKompendium/BandG/HVKompendium_Band_G_node.html [Abruf am 11.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2024d). Consumer IoT. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Consumer-IoT/Consumer-IoT_node.html [Abruf am 17.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2024e). BSI - Lerneinheit 7.7: Risiken bewerten. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_07/Lektion_7_07_node.html [Abruf am 22.07.2024].

Bundesamt für Sicherheit in der Informationstechnik (2024f). Kriterienkatalog C5. Bundesamt für Sicherheit in der Informationstechnik. Online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html [Abruf am 24.07.2024].

Bundeskanzleramt (2018). Erläuterungen. Online: https://www.parlament.gv.at/dokument/XXVI/ME/78/fname_710319.pdf [Abruf am 13.07.2024].

Bundeskanzleramt (2023). Technische Ausgestaltung eines öffentlichen Warnsystems, Bundesrecht konsolidiert, Fassung vom 02.07.2023. RIS. Online: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20012189 [Abruf am 02.07.2023].

Bundeskanzleramt (2024a). Standards für Telekom-Betreiber. onlinesicherheit.at. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/Standards-Telekom-Betreiber.html [Abruf am 11.07.2024].

Bundeskanzleramt (2024b). Gesamte Rechtsvorschrift für Netz- und Informationssystemsicherheitsverordnung, Fassung vom 09.05.2024. RIS. Online: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536 [Abruf am 09.05.2024].

Bundeskanzleramt (2024c). Gesamte Rechtsvorschrift für Netz- und Informationssystemsicherheitsgesetz, Fassung vom 09.05.2024. Online: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536 [Abruf am 09.05.2024].

Bundeskanzleramt (2024d). ID Austria. oesterreich.gv.at. Online: https://www.oesterreich.gv.at/id-austria.html [Abruf am 01.08.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2017). 1. Vorteile und Risiken. onlinesicherheit.gv.at. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Sicherheitsmanagement/Outsourcing-und-Cloud-Computing/Vorteile-und-Risiken-Outsourcing-und-Cloud-Computing.html [Abruf am 24.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2023a). Österreichisches Informationssicherheitshandbuch. unveröffentlicht: Bundeskanzleramt Österreich (BKA). Online: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf [Abruf am 30.03.2023].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2023b). Österreichisches Informationssicherheitshandbuch. Österreichisches Informationssicherheitshandbuch. Online: https://www.sicherheitshandbuch.gv.at/index.php [Abruf am 16.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024a). ISO/IEC 27000 - ISMS-Normenreihe. IKT-Sicherheitsportal. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000-ISMS-Normenreihe.html [Abruf am 10.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024b). Standards mit IT-Sicherheitsaspekten. IKT-Sicherheitsportal. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/IT-Sicherheitsstandards.html [Abruf am 10.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024c). ISO/IEC 27001 - Anforderungen an Informationssicherheits-Managementsysteme. IKT-Sicherheitsportal. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000-ISMS-Normenreihe/ISO-IEC-27001-Informationssicherheits-Managementsysteme-ISMS.html [Abruf am 10.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024d). ISO/IEC 27002 - Leitfaden für das Management der Informationssicherheit. IKT-Sicherheitsportal. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/ISO-IEC-27000-ISMS-Normenreihe/ISO-IEC-27002-Management-der-Informationssicherheit.html [Abruf am 10.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024e). BSI IT-Grundschutz-Standards. IKT-Sicherheitsportal. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/BSI-IT-Grundschutz-Standards.html [Abruf am 10.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024f). Open Web Application Security Project (OWASP). IKT-Sicherheitsportal. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/OWASP.html [Abruf am 10.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (2024g). ÖNORM A7700 - Sichere Webapplikationen. oesterreich.gv.at. Online: https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-

Standards/OENORM-A7700-Sichere-Webapplikationen.html [Abruf am 16.07.2024].

Bundeskanzleramt/A-SIT Zentrum für sichere Informationstechnologie – Austria (o. J.). Für Betreiber wesentlicher Dienste. Anlaufstelle NISG. Online: https://www.nis.gv.at/fragen-und-antworten/fuer-betreiber-wesentlicher-dienste.html [Abruf am 16.05.2024].

Bundeskanzleramt/Bundesministerium für Inneres (2022). Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste. Online: https://www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf [Abruf am 16.07.2024].

Bundeskanzleramt/Bundesministerium für Inneres (2024a). Allgemeines zum NIS-Gesetz. Anlaufstelle NISG. Online: https://www.nis.gv.at/fragen-und-antworten/allgemeines-zum-nis-gesetz.html [Abruf am 13.07.2024].

Bundeskanzleramt/Bundesministerium für Inneres (2024b). Rechtliches und Dokumente. Anlaufstelle NISG. Online: https://www.nis.gv.at/rechtliches-und-dokumente.html [Abruf am 16.07.2024].

Bundesministerium für Inneres (2023). Krisen- und Katastrophenmanagement - Warnung und Alarmierung. Staatliches Krisen- und Katastrophenschutzmanagement (SKKM). Online: https://www.bmi.gv.at/204/skkm/Warnung.aspx [Abruf am 02.07.2023].

CIS (2024a). About us. CIS. Center for Internet Security. Online: https://www.cisecurity.org/about-us [Abruf am 10.07.2024].

CIS (2024b). CIS Critical Security Controls. CIS. Center for Internet Security. Online: https://www.cisecurity.org/controls [Abruf am 10.07.2024].

CIS (2024c). CIS Critical Security Controls Version 8.1. CIS. Center for Internet Security. Online: https://www.cisecurity.org/controls/v8-1 [Abruf am 10.07.2024].

ComputerWeekly (2023). Was ist OTP (One-Time-Password, Einmalpasswort)? ComputerWeekly. Online: https://www.computerweekly.com/de/definition/OTP-One-Time-Password-Einmal-Passwort [Abruf am 01.07.2023].

ENISA (2012). Introduction to Return on Security Investment. Online: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment [Abruf am 24.07.2024].

ENISA (2022). RISK MANAGEMENT STANDARDS. Online: https://www.enisa.europa.eu/publications/risk-management-standards/@@download/fullReport [Abruf am 11.07.2024].

Europäisches Parlament/Europäische Kommission (2016). RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148.

Ferdinand Porsche FernFH (2023a). Einführung in die Literaturstudie. Forschungsmethoden in der Wirtschaftsinformatik. Online: https://onlinecampus.fernfh.ac.at/mod/h5pactivity/view.php?id=133886 [Abruf am 30.06.2023].

Ferdinand Porsche FernFH (2023b). Einführung in die Design Science. Forschungsmethoden in der Wirtschaftsinformatik. Online: https://onlinecampus.fernfh.ac.at/mod/h5pactivity/view.php?id=133894 [Abruf am 30.06.2023].

Ferdinand Porsche FernFH (2024a). Methodenwahl. Qualitorial. Online: https://qualitorial.fernfh.ac.at/methodenwahl/#grundlagen [Abruf am 01.08.2024].

Ferdinand Porsche FernFH (2024b). Leitfadenentwicklung. Qualitorial. Online: https://qualitorial.fernfh.ac.at/leitfadenentwicklung/#grundlagen [Abruf am 01.08.2024].

Ferdinand Porsche FernFH (2024c). Interviewvorbereitung. Qualitorial. Online: https://qualitorial.fernfh.ac.at/interviewvorbereitung/#grundlagen_einverst%C3%A4ndniserklaerung [Abruf am 01.08.2024].

Flick, Uwe (2020). Sozialforschung. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.

Franziska Pfeiffer (2023). Qualitative Inhaltsanalyse nach Mayring in 5 Schritten. Scribbr. Online: https://www.scribbr.at/methodik-at/qualitative-inhaltsanalyse/ [Abruf am 01.07.2023].

F-Secure Deutschland (2019). Veraltete Internet-Technologien sind Sicherheitsrisiken. F-Secure. Online: https://blog.f-secure.com/de/veraltete-internet-technologien-sind-sicherheitsrisiken/ [Abruf am 17.07.2024].

G-Core Labs S.A. (2021). Zuverlässigkeitsgrad des Rechenzentrums. G-Core. Online: https://gcore.com/de/learning/data-center-reliability-levels/ [Abruf am 22.07.2024].

Geißler, Otto/Schmitz, Peter (2020). Return on Security Investment (RoSI) als Entscheidungshilfe. Security Insider. Online: https://www.security-insider.de/return-on-security-investment-rosi-als-entscheidungshilfe-a-923730/ [Abruf am 24.07.2024].

Gläser, Jochen/Laudel, Grit (2009). Experteninterviews und qualitative Inhaltsanalyse. Wiesbaden: vs Verlag für Sozialwissenschaften.

Hevner, Alan/Chatterjee, Samir (2010). Design Research in Information Systems: Theory and Practice. unveröffentlicht: Springer US.

Hevner, A.R.; March, S.T.; Park, J.; Ram, S. (2004). Design Science in Information Systems Research. In *MIS Quarterly, Vol. 28 (2004) No. 1* (S. 75–105). unveröffentlicht: o.V.

Hochschule Luzern (2023). Auswahl der Erhebungsmethode. HSLU. Online: https://www.empirical-methods.hslu.ch/forschungsprozess/qualitative-forschung/auswahl-der-erhebungsmethode/ [Abruf am 01.07.2023].

IBM Deutschland GmbH (2024). Was sind Microservices? IBM. Online: https://www.ibm.com/de-de/topics/microservices [Abruf am 24.07.2024].

IETF (2012). The OAuth 2.0 Authorization Framework. Internet Engineering Task Force (IETF). Online: https://datatracker.ietf.org/doc/html/rfc6749 [Abruf am 28.11.2023].

International Eletrotechnical Commission (2024). Understanding IEC 62443. IEC. Online: https://www.iec.ch/blog/understanding-iec-62443 [Abruf am 16.07.2024].

ISACA (2018a). COBIT 2019 Framework: Governance and Management Objectives. Schaumburg: ISACA.

ISACA (2018b). COBIT 2019 Framework: Introduction and Methodology. Schaumburg: ISACA.

Iserlohn, Christoph/Schulte-Coerne, Till (2017). Warum es nicht immer Microservices sein müssen. Informatik Aktuell. Online: https://www.informatik-aktuell.de/entwicklung/methoden/warum-es-nicht-immer-microservices-sein-muessen.html [Abruf am 24.07.2024].

ISO (2018). ISO/IEC 20000-1:2018. ISO - International Organization for Standardisation. Online: https://www.iso.org/standard/70636.html [Abruf am 10.07.2024].

ISO (2024a). ISO/IEC 27000:2009. ISO - International Organization for Standardisation. Online: https://www.iso.org/standard/41933.html [Abruf am 10.07.2024].

ISO (2024b). ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements. Online: https://www.iso.org/standard/75106.html [Abruf am 11.07.2024].

ISO (2024c). ISO 31000 Risk management. Online: https://www.iso.org/iso-31000-risk-management.html [Abruf am 11.07.2024].

Jürgen Bortz/Nicola Döring (1995). Forschungsmethoden und Evaluation. Berlin: Springer.

Kersten, Heinrich/Schröder, Klaus-Werner (2023). ISO 27001:2022/2023. Management der Informationssicherheit nach den aktuellen Standards (Edition <kes>). Wiesbaden: Springer Vieweg.

Kotthaus, Jochem (2020). FAQ Methoden der empirischen Sozialforschung. Opladen & Toronto: Verlag Barbara Budrich.

Lea Toms (2016). Abgelaufene SSL-Zertifikate, die unterschätzte Gefahr. manage it | IT Strategien und Lösungen. Online: https://ap-verlag.de/abgelaufene-ssl-zertifikate-die-unterschaetzte-gefahr/16727/ [Abruf am 01.07.2023].

Luber, Stefan/Schmitz, Peter (2021). Was ist Security by Design? Security Insider. Online: https://www.security-insider.de/was-ist-security-by-design-a-1071181/ [Abruf am 17.07.2024].

Lunkeit, Armin/Zimmer, Wolf (2021). Security by Design: Security Engineering informationstechnischer Systeme. Berlin: Springer Vieweg.

Maxpert GmbH (2024). COBIT® 2019 Definitionen | Was ist COBIT2019? Online: https://www.maxpert.de/de/profil/schulungsspektrum/cobit-methode-definitionen/514 [Abruf am 10.07.2024].

Melanie Rainer/Thomas Neuroth-Pfeiffer/Martin Latzenhofer/Christian Focke (2022a). Informationssicherheitsmanagement. Wiener Neustadt: Ferdinand Porsche Fernfachhochschule GmbH.

Melanie Rainer/Thomas Neuroth-Pfeiffer/Martin Latzenhofer/Christian Focke (2022b). IT-Governance. Wiener Neustadt: Ferdinand Porsche Fernfachhochschule GmbH.

Microsoft (2023). Übersicht über Active Directory Domain Services. Microsoft Learn. Online: https://learn.microsoft.com/de-de/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview [Abruf am 24.07.2024].

Myra Security GmbH (2024). OWASP Top 10: Definition und Sicherheitsrisiken. Myra. Online: https://www.myrasecurity.com/de/knowledge-hub/owasp-top-10/ [Abruf am 10.07.2024].

National Institute of Standards and Technology (2024). Cybersecurity Framework. NIST. Online: https://www.nist.gov/cyberframework [Abruf am 01.07.2024].

NIST (2024a). Frequently Asked Questions. NIST. Online: https://www.nist.gov/cyberframework/faqs [Abruf am 10.07.2024].

NIST (2024b). NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE. Online: https://doi.org/10.6028/NIST.SP.1299 [Abruf am 10.07.2024].

Olbrich, Alfred (2008). ITIL kompakt und verständlich 4. Aufl. Aschaffenburg: Vieweg + Teubner Verlag.

OpenID Foundation, (2023). How OpenID Connect Works. OpenID. Online: https://openid.net/developers/how-connect-works/ [Abruf am 29.11.2023].

OWASP Foundation (2024a). About the OWASP Foundation. OWASP. Online: https://owasp.org/about/ [Abruf am 10.07.2024].

OWASP Foundation (2024b). OWASP Top 10:2021. OWASP. Online: https://owasp.org/Top10/ [Abruf am 10.07.2024].

OWASP Foundation (o. J.). OWASP Top Ten. OWASP. Online: https://owasp.org/www-project-top-ten/ [Abruf am 25.06.2023].

P1 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

P2/P3 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

P4 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

P5 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

P6 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

P7 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

P8 (2024). Interview zu Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen.

Rich Campagna (2023). Komplexität ist Gegenspieler der IT-Sicherheit. Cloudcomputing Insider. Online: https://www.cloudcomputing-insider.de/komplexitaet-ist-gegenspieler-der-it-sicherheit-a-efc3ec07edc9cb53fb24009f7b7cb9c8/ [Abruf am 02.07.2023].

Sectigo Limited (2020). Sectigo AddTrust External CA Root Expiring May 30, 2020. Sectigo. Online: https://support.sectigo.com/articles/Knowledge/Sectigo-AddTrust-External-CA-Root-Expiring-May-30-2020 [Abruf am 01.07.2023].

TeleTrusT (2023). Handreichung zum „Stand der Technik“. Online: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/?tx_reintdownloadmanager_reintdlm%5Bdownloaduid%5D=11375&cHash=911131cf4407f73e8649e9ed5f512c6e [Abruf am 25.07.2024].

Tremp, Hansruedi (2021). Architekturen Verteilter Softwaresysteme. Wiesbaden: Springer Vieweg.

TÜV AUSTRIA (2024a). IT Service Management-Zertifizierung | ISO 20000. TÜV AUSTRIA. Online: https://www.tuv.at/it-service-management-zertifizierung-iso-20000/ [Abruf am 10.07.2024].

TÜV AUSTRIA (2024b). Industrial Security Konzepte | IEC 62443. TÜV AUSTRIA. Online: https://www.tuv.at/industrial-security-konzepte-iec-62443/ [Abruf am 16.07.2024].

TÜV SÜD AG (2024). DIN EN 50600 erklärt. TÜV SÜD. Online: https://www.tuvsud.com/de-de/indust-re/gebaeudeausruestung-info/din-en-50600 [Abruf am 16.07.2024].

Ulrike Lechner/Sebastian Dännart/Andreas Rieb/Steffi Rudel (2018). CASE KRITIS Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Berlin: Logos Verlag.

Uptime Institute, LLC (2024). Uptime Institute Tier Classification System. Uptime Institute. Online: https://uptimeinstitute.com/tiers [Abruf am 22.07.2024].

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. (2019). Rechenzentren. Online: https://www.vde-verlag.de/normen/rechenzentren.pdf [Abruf am 17.07.2024].

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. (2024). IEC 62443: Cybersecurity in der Industrieautomatisierung. DKE. Online: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung [Abruf am 16.07.2024].

Vogt, Stefanie/Werner, Melanie (2014). Forschen mit Leitfadeninterviews und qualitativer Inhaltsanalyse. Online: https://www.th-koeln.de/mam/bilder/hochschule/fakultaeten/f01/skript_interviewsqualinhaltsanalyse-fertig-05-08-2014.pdf [Abruf am 25.06.2024].

Volker Wittpahl (2023). iit-Themenband Resilienz. Berlin: Springer Vieweg.

Waidner, Michael/Backes, Michael/Müller-Quade, Jörn (2013). Entwicklung sicherer Software durch Security by Design. Darmstadt: Fraunhofer Verlag.

Weiß, Eva-Maria (2024). Weltweiter IT-Ausfall: Betrieb wird wieder aufgenommen | heise online. heise online. Online: https://www.heise.de/news/Weltweiter-IT-Ausfall-Flughaefen-Banken-und-Geschaefte-betroffen-9806343.html [Abruf am 19.07.2024].

Zeiß, Joachim/Jorns, Oliver (2022). Verteilte Systeme. Online: https://mediawiki.fernfh.ac.at/mediawiki/index.php?oldid=767 [Abruf am 24.07.2024].

9 Abbildungsverzeichnis

Abbildung 1: Empirischer, sozialwissenschaftlichen Forschungsprozess (nach Gläser & Laudei, 2009, S. 35) 4

Abbildung 2: Design Sciene Zyklen (Hevner & Chatterjee, 2010)..... 7

Abbildung 3: Detaillierte Risikoanalyse lt. österreichischem Sicherheitshandbuch (angelehnt an Bundeskanzleramt & A-SIT Zentrum für sichere Informationstechnologie – Austria, 2023a).....31

Abbildung 4: Risikomatrix nach BSI 200-3 (Bundesamt für Sicherheit in der Informationstechnik, 2024e).....33

Abbildung 5: Verfügbarkeiten in Tiers (nach G-Core Labs S.A., 2021) 37

Abbildung 6: Redundanzverfahren lt. BSI (nach Bundesamt für Sicherheit in der Informationstechnik, 2013a) 38

Abbildung 7: : Qualitative Inhaltsanalyse (nach Gläser & Laudei, 2009, S. 200) 56

10 Tabellenverzeichnis

Tabelle 1: Anlage 1 der NIS-Verordnung (Bundeskanzleramt, 2024b).....22

Tabelle 2: Typische Verfügbarkeitsklassen und ihre Ausfallzeiten lt. BSI (nach Bundesamt für Sicherheit in der Informationstechnik, 2013b).....36

Tabelle 3: Anhang D - Codesystem.....115

11 Abkürzungsverzeichnis

A-SIT	Zentrum für sichere Informationstechnologie Austria
ALF	Annualized Loss Expectancy
API	Application Programming Interface
ARO	Annualized Rate of Occurrence
BCM	Business Continuity Management
BKA	Bundeskanzleramt
BSI	Bundesamt für Sicherheit in der Informationstechnik
CENELEC	European Electrotechnical Committee for Standardization
CIRT	Computer Security Incident Response Team
CIS	Confidentiality, Integrity, Availability
CIS	Center for Internet Security
CSF	Cybersecurity Framework
CoBIT	Control Objectives for Information and Related Technology
DNS	Domain Name Service
DSGVO	Datenschutzgrundverordnung
EN	Europäische Norm
ENISA	European Union Agency for Cyber Security
EPU	Ein-Personen-Unternehmen
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISO	International Organization for Standardisation
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ISMS	Informationssicherheits-Managementsystem
KMU	Kleine und mittlere Unternehmen
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MTBF	Meantime between failures
MTTF	Meantime to failure

MTTR	Meantime to repair
NIS	Netz- und Informationssystemsicherheit
NISG	NIS-Gesetz
NIST	National Institute of Standards and Technology
NISV	NIS-Verordnung
OT	Operative Technologie
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PKI	Public Key Infrastructure
ROSI	Return on Security Investment
SaaS	Software as a Service
SLF	Single Loss Expectancy
SSL	Secure Socket Layer
TLD	Top Level Domain

Anhang A – Interviewleitfaden

FORSCHUNGSFRAGE:
LASSEN SICH IN BEZUG AUF KRITISCHE SYSTEME MIT EXTERNEN SCHNITTSTELLEN SOWOHL HOHE ANFORDERUNGEN IM BEREICH DER VERTRAULICHKEIT UND INTEGRITÄT ALS AUCH EINE HOHE SYSTEMVERFÜGBARKEIT GLEICHZEITIG UMSETZEN?

Einleitung

Vielen Dank, dass Sie sich heute die Zeit genommen haben für dieses Gespräch. Ich erkläre vielleicht noch einmal ganz kurz etwas zu meiner Masterarbeit und zum Ablauf des Interviews:

Im Rahmen meiner Masterarbeit führe ich qualitative Interviews mit mehreren Informationssicherheits-Expert_innen durch. Konkret geht es in meiner Arbeit um kritische Systeme und um die Auswirkungen die hohe Sicherheitsanforderungen auf deren Verfügbarkeit haben. Bei der Beantwortung der Fragen bitte ich Sie davon auszugehen, dass es sich um Systeme handelt, deren Anforderungen nicht durch externe Normen vorgegeben sind. Vielmehr bitte ich Sie sich in Ihrem Denken keine Grenzen zu setzen und sich ein System vorzustellen bei dem Sie selbst frei darüber entscheiden können welche Maßnahmen Sie für dessen Schutz umsetzen. Es geht mir in meiner Arbeit darum zu erfahren welche Maßnahmen Sie als Expert_in für geeignet halten und wie Sie persönlich vorgehen würden.

Das Interview wird etwa 30-45 Minuten dauern. Die Einverständniserklärung haben Sie bereits vorab per E-Mail erhalten und auch bereits unterschrieben. Vielen Dank dafür!

Mit Ihrem Einverständnis werde dieses Gespräch aufnehmen, da ich nicht alles mitschreiben kann, was Sie mir sagen. Es werden aber keine Namen oder Fakten, die auf Ihre Person rückschließen lassen, verwendet, d.h. ich werde in meiner Arbeit alles so darstellen, dass kein Rückbezug auf Ihre Person möglich ist. Alle erhobenen Daten werden streng vertraulich behandelt und nur zu Forschungszwecken herangezogen. Die Ergebnisse werden nur in anonymisierter oder pseudonymisierter Form in die Arbeit aufgenommen.

Haben Sie noch irgendwelche Fragen? Wenn nicht, dann würde ich nun die Aufnahme starten und mit dem Interview beginnen.

Interviewfragen

1. Können Sie bitte schildern was Sie beruflich tun und inwiefern Sie darin mit kritischen Systemen in Berührung kommen? (3min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Einstieg, Tätigkeiten und Expertise	Was machen Sie da genau? Wie haben Sie sich das erarbeitet?	Wie lange arbeiten Sie bereits in dem Bereich? Wie war Ihr Lebenslauf bis hierhin?
2. Wie gehen Sie vor um den Schutzbedarf und die Sicherheitsanforderungen eines Systems zu bestimmen? (5min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Anforderungsquellen	Wie ist Ihre Herangehensweise? Welchen Kriterien verwenden Sie? Allgemeine Anforderungen? Anforderungen an die eingangs beschriebenen, kritischen Systeme?	Ziehen Sie bestimmte Frameworks und Best Practices heran? Welche Bedeutung haben das österreichische Sicherheitshandbuch und ÖNORM-Standards für Sie?

3. Welche sind aus Ihrer Sicht die wichtigsten Anforderungen um Datensicherheit in kritischen Systemen zu gewährleisten? (5min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Primäre Sicherheitsanforderungen	Worum geht es da genau? Was macht man da genau? Wie meinen Sie das konkret? Noch etwas?	In Bezug auf - die Datenhaltung? - externe Schnittstellen? - Inbound / Outbound? - Authentifizierung / Autorisierung? - Verschlüsselung?
4. Wie gehen Sie vor um kritische Systeme ausfallsicher zu machen? (7min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Verfügbarkeit von Systemen	Warum ist das Ihrer Meinung nach wichtig? Können Sie ein Beispiel dafür nennen? Was meinen Sie damit genau?	Redundanzen von - Hardware-Komponenten - Netzwerken - Externen Komponenten Spezielles Testing der Sicherheitsmaßnahmen? Spezielle Rollout-Strategien davon?

5. Welchen Einfluss haben die zunehmende Integration externer Dienste und der Trend zu Microservices auf die Ausfallsicherheit und wie gehen Sie damit um? (5min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Abhängigkeit von Drittsystemen	Warum wirkt sich das aus? Was passiert in diesem Fall?	Wie versichern Sie sich gegenüber Ausfällen von externen Komponenten/Dienste?
6. Wie wirkt sich die Umsetzung von Sicherheitsmaßnahmen Ihrer Einschätzung nach auf die Verfügbarkeit aus? (10min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Auswirkungen von Sicherheitsanforderungen	Wie wirkt sich das genau aus? Was passiert in diesem Fall? Haben Sie ein Beispiel dafür? Wie gehen Sie damit um?	Verschlüsselung? Authentifizierung / Autorisierung? Externe Dienste / Komponenten? Welche Abstriche würden Sie machen um die Verfügbarkeit zu erhöhen? Wie beugen Sie dem vor? Welche Bedeutung haben sog. „Security by Design“-Prinzipien für Sie?

7. Welche Bedeutung hat die Wirtschaftlichkeit von Sicherheitsanforderungen in Ihren Entscheidungen? (5min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Kosten und Wirtschaftlichkeit	Wie gehen Sie damit um? Können Sie mir das näher erklären?	Wie wägen Sie Risiko und Kosten ab? Wie beurteilen Sie die Berechnung eines Return on Security Investment (ROSI)? In welchen Bereichen wären Sie bereit zugunsten der Kosten Zugeständnisse zu machen?
8. Gibt es noch etwas Wichtiges, das Sie zu dem Thema sagen wollen? (2min)		
Themencluster/ Inhaltliche Aspekte	Aufrechterhaltungsfragen	Nachfragen
Abschluss		Habe ich etwas Wesentliches vergessen?

Vielen Dank für Ihre Zeit und Ihre Unterstützung!

Zum Abschluss habe ich noch ein paar kurze, demografische Fragen, die für statistische Zwecke erhoben werden. Diese würde ich Ihnen gerne in Form eines einfachen Fragebogens per E-Mail zukommen lassen und mit der Bitte ihn auszufüllen. Ich habe diese Fragen aber bewusst in ein eigenes Dokument ausgelagert da sie persönlicher Natur sind und mit dem Interviewgegenstand an sich nichts zu tun haben. Bitte entscheiden Sie daher selbst ob Sie die Fragen beantworten wollen und falls ja, senden Sie mir bitte den ausgefüllten Fragebogen zurück.

Anhang B – Soziodemografische Daten

Ergänzende Demografische Daten zu dem Interview im Rahmen einer Masterarbeit zu den Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen

Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer!

Vielen Dank für Ihre Unterstützung bei meiner Masterarbeit und Ihrer Bereitschaft an meiner Interview-Serie teilzunehmen. Ergänzend dazu ersuche ich Sie mir nachfolgende, demografische Daten bekanntzugeben, die selbstverständlich vertraulich und ausschließlich entsprechend den Bedingungen der Einwilligungserklärung behandelt werden. Ich habe diese Fragen aber bewusst in ein eigenes Dokument ausgelagert da sie persönlicher Natur sind und mit dem Interviewgegenstand nur indirekt zu tun haben. Bitte entscheiden Sie daher selbst ob Sie die Fragen beantworten möchten und falls ja, senden Sie mir bitte den ausgefüllten Fragebogen zurück.

Vielen Dank,
Peter Gneist

Demografische Daten

Name des Teilnehmers: _____

Geburtsdatum: _____

Wohnort:

Stadt: _____

Land: _____

Geschlecht:

☐ Weiblich

☐ Männlich

☐ Anderes, bitte angeben _____

Schulische und akademische Ausbildung(en):

_____

_____

_____

_____

_____

Erwerbstätigkeit:

☐ Angestellt

☐ Selbstständig

☐ Sowohl angestellt als auch selbstständig

☐ Ohne Beschäftigung

☐ Pensioniert

☐ Andere, bitte angeben _____

Wöchentliche Normalarbeitszeit:

☐ <= 20 Stunden

☐ 21 – 40 Stunden

☐ Andere, bitte angeben _____

Anhang C – Einwilligungserklärung

Information und Einverständniserklärung zur Teilnahme an einem Interview im Rahmen einer Masterarbeit zu den Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen

Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer!

Mein Name ist Peter Gneist und ich bin Studierender des Studiengangs Wirtschaftsinformatik Master an der Ferdinand Porsche FernFH in Wiener Neustadt. Ich lade Sie ein, im Zuge meiner Masterarbeit zum Thema *Auswirkungen von IT-Sicherheitsarchitekturen in Krisensituationen* an der Ferdinand Porsche FernFH, an einem Interview teilzunehmen.

Ihre Teilnahme erfolgt freiwillig. Sie können jederzeit ohne Angabe von Gründen aufhören. Die Ablehnung der Teilnahme oder ein vorzeitiges Beenden haben keine nachteiligen Folgen für Sie.

Bitte lesen Sie den folgenden Text sorgfältig durch und bestätigen Sie die Einwilligung zur Teilnahme nur

- wenn Sie Art und Ablauf dieser Studie vollständig verstanden haben,
- wenn Sie bereit sind, der Teilnahme zuzustimmen und
- wenn Sie sich über Ihre Rechte als Teilnehmer_in an dieser Studie im Klaren sind.

1. Was ist der Zweck der Studie?

Ziel der Arbeit ist es zu erforschen ob hohe Sicherheitsanforderungen und eine hohe Systemverfügbarkeit miteinander vereinbar sind, im Kontext kritischer Systeme mit externen Schnittstellen.

2. Wie läuft die Studie ab?

Im Rahmen dieser Masterarbeit werden 6-10 Personen befragt, die Expert_innen im Bereich Informationssicherheit sind und mit Anforderungen an kritische Anwendungen vertraut sind. Die Fragen beziehen sich sowohl auf die Quellen, die für die Anforderungen herangezogen werden, als auch auf die praktische Umsetzung der Sicherheitsanforderungen selbst. Außerdem werde ich Sie um ein paar persönliche Angaben wie Geschlecht, Alter, Ausbildung und Beruf, bitten. Die Dauer des Interviews wird ca. 30-45 Minuten betragen. Das Interview wird durch eine Software aufgezeichnet und anschließend in ein Textdokument transkribiert.

3. Welche Risiken gibt es und wie kann die Teilnahme vorzeitig beendet werden?

Die Teilnahme ist mit keinen Risiken für Sie verbunden und Sie können jederzeit auch ohne Angabe von Gründen aus der Studie ausscheiden.

4. Datenschutz

Im Rahmen dieser Studie werden Daten über Sie erhoben und verarbeitet werden. Es ist grundsätzlich zu unterscheiden zwischen

1) jenen personenbezogenen Daten, anhand derer eine Person direkt identifizierbar ist (z.B. Name, Geburtsdatum, Adresse, Sozialversicherungsname, Bild- oder Tonbandaufnahmen, …).
2) pseudonymisierten personenbezogenen Daten, das sind Daten, bei denen alle Informationen, die direkte Rückschlüsse auf die konkrete Person zulassen, entweder entfernt oder durch einen Code (z. B. eine Zahl) ersetzt oder (z.B. im Fall von Bildaufnahmen) unkenntlich gemacht werden. Es kann jedoch trotz Einhaltung dieser Maßnahmen nicht vollkommen ausgeschlossen werden, dass es zu einer Re-Identifizierung kommt.
3) anonymisierten Daten, bei denen eine Rückführung auf die konkrete Person ausgeschlossen werden kann.

Zugang zu den Daten anhand derer Sie direkt identifizierbar sind (siehe Punkt 1), hat nur der Autor der Masterarbeit. Die Daten sind gegen unbefugten Zugriff geschützt. Sämtliche Personen, die Zugang zu diesen Daten erhalten, unterliegen im Umgang mit den Daten den geltenden nationalen Datenschutzbestimmungen und/oder der EU-Datenschutz-Grundverordnung (DSGVO).

Die Weitergabe der Daten an den/die Betreuer_in der Masterarbeit zum Zweck der Begutachtung der Arbeit erfolgt nur in pseudonymisierter oder anonymisierter Form. Auch für die Masterarbeit oder etwaige Publikationen werden nur die pseudonymisierten oder anonymisierten Daten verwendet.

Der Code, der eine Zuordnung der pseudonymisierten Daten zu Ihrer Person ermöglicht, wird nur von dem Autor der Masterarbeit aufbewahrt.

Im Rahmen dieser Studie ist keine Weitergabe von Daten in Länder außerhalb der EU vorgesehen. [1]

[1] Beachten Sie hierbei bitte lediglich, dass im Falle der Verwendung der Software MS Teams für das Interview nicht gänzlich ausgeschlossen werden kann, dass Daten des Interviews seitens Microsofts an Dritte (allenfalls auch in Drittstaaten) weitergegeben werden könnte. Für weitere Informationen hierzu siehe die Datenschutzerklärung von Microsoft: https://privacy.microsoft.com/de-de/privacystatement.

Ihre Einwilligung bildet die Rechtsgrundlage für die Verarbeitung Ihrer personenbezogenen Daten. Sie können Ihre Einwilligung zur Erhebung und Verarbeitung Ihrer Daten jederzeit widerrufen. Nach Ihrem Widerruf werden keine weiteren Daten mehr über Sie erhoben. Die bis zum Widerruf erhobenen Daten können allerdings weiter im Rahmen dieser Studie verarbeitet werden.

Nach der DSGVO stehen Ihnen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch zu, soweit dem nicht andere gesetzliche Vorschriften widersprechen.

Sie haben auch das Recht, bei der österreichischen Datenschutzbehörde eine Beschwerde über den Umgang mit Ihren Daten einzubringen (www.dsb.gv.at).

Die voraussichtliche Dauer der Masterarbeit ist bis Oktober 2024. Die Dauer der Speicherung der erhobenen Daten über das Ende der Studie hinaus ist durch Rechtsvorschriften geregelt und beträgt 10 Jahre.

Falls Sie Fragen zum Datenschutz in dieser Studie haben, wenden Sie sich bitte zunächst an mich. Ich kann Ihr Anliegen ggf. an die Personen, die für den Datenschutz verantwortlich sind, weiterleiten.

Datenschutzbeauftragter der FernFH: datenschutz@fernfh.ac.at

5. Möglichkeit, weitere Fragen zu stellen:

Für weitere Fragen im Zusammenhang mit dieser Studie stehe ich Ihnen gerne zur Verfügung. Auch Fragen, die Ihre Rechte als Teilnehmer_in an dieser Studie betreffen, werden Ihnen gerne beantwortet.

Name der Kontaktperson: Peter Gneist

Erreichbar unter: Mail: [redacted]

Telefon: [redacted]

6. Einwilligungserklärung

Name des Teilnehmers: _____

Ich erkläre mich bereit, an einem Interview im Rahmen der Masterarbeit von Name Peter Gneist teilzunehmen.

Ich habe den Text der Einwilligungserklärung, der insgesamt vier Seiten umfasst, gelesen. Aufgetretene Fragen wurden mir verständlich und genügend beantwortet. Ich hatte ausreichend Zeit, mich zu entscheiden. Ich habe zurzeit keine weiteren Fragen mehr.

Ich behalte mir jedoch das Recht vor, die Teilnahme jederzeit zu beenden, ohne dass mir daraus Nachteile entstehen. Ich behalte mir außerdem das Recht vor, meine Einwilligung zur Erhebung und Verarbeitung meiner Daten zu einem späteren Zeitpunkt zu widerrufen.

Ich stimme ausdrücklich zu, dass meine im Rahmen dieser Studie erhobenen Daten wie im Abschnitt „Datenschutz“ dieses Dokuments beschrieben, verwendet werden.

Eine Kopie der Einwilligungserklärung habe ich erhalten. Das Original verbleibt bei dem Autor der Masterarbeit.

.....

(Datum und Unterschrift der Teilnehmerin / des Teilnehmers)

.....

(Datum und Unterschrift des Autors der Masterarbeit)

Anhang D – Codesystem

Code	Beschreibung	Häufigkeit
Anforderungsquellen	Mit diesem Code werden Passagen gekennzeichnet, die sich auf die Quellen von Security-Anforderungen beziehen.	35
Österreichisches Sicherheitshandbuch	Mit diesem Code werden Aussagen gekennzeichnet mit denen sich die Expert_innen darauf das österreichische Sicherheitshandbuch und dessen Bedeutung beziehen.	8
Ö-Normen	Dieser Code wird verwendet um Expert_innen-Aussagen zur Bedeutung von Ö-Normen zu kennzeichnen.	8
Vertraulichkeit & Integrität	Dieser Code beschreibt jene Abschnitte in denen sich die Expert_innen auf die wichtigsten Anforderungen von kritischen Systemen In Bezug auf Vertraulichkeit und Integrität beziehen.	26
Verfügbarkeit	Mit diesem Code werden Passagen kodiert in denen sich die Expert_innen auf die Erzeugung von Ausfallsicherheit beziehen.	23
Komplexität / Externe Dienste	Diese Code kennzeichnet Abschnitte die sich in den Interviews auf die Komplexität von Systemen beziehen, sowie auf Einflüsse von externen Diensten/Komponenten und Microservices.	23

Security by Design	Mit diesem Code werden jene Abschnitte gekennzeichnet in denen sich die Expert_innen mit der Bedeutung und Umsetzung des Security by Design Prinzips auseinandersetzen.	14
Testing	Mit diesem neuen Code, der induktiv aus den Aussagen der Expert_innen abgeleitet wurde, werden jene Passagen markiert, die sich auf das Testing der Sicherheitsmaßnahmen beziehen.	16
Wirtschaftlichkeit	Mit diesem Code werden Abschnitte gekennzeichnet, die sich auf die Wirtschaftlichkeit von Sicherheitsanforderungen beziehen.	25
ROSI	Mit diesem Code werden Abschnitte mit Bezug auf die Berechnung eines Return on Security Investment (ROSI) markiert.	8
Vertraulichkeit & Integrität vs. Verfügbarkeit	Dieser Code beschreibt Passagen die sich auf die Beziehung von hohen Anforderungen an Vertraulichkeit und Integrität einerseits und einer hohen Verfügbarkeit andererseits beziehen.	29

Tabelle 3: Anhang D - Codesystem