FERDINAND PORSCHE
FERN FH

Quantum Computing: Bedrohungsszenario für die State of the Art Informationssicherheit?

Masterarbeit

Eingereicht von: **Mag. Michael Kirchmair**

Matrikelnummer: 00965825

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. Peter Völkl, BA MA MSc

Linz, Mai 2023

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.

Linz am, 18.05.2023 _____

Unterschrift

Kurzzusammenfassung: Quantum Computing: Bedrohungsszenario für die State of the Art Informationssicherheit?

Quantencomputer haben das Potenzial, durch nie dagewesene Rechenkraft bedeutende mathematische und wirtschaftliche Probleme zu lösen. Gleichzeitig kann diese Rechenkraft dazu verwendet werden, heutzutage in nahezu allen IT-Infrastrukturen tief verankerte asymmetrische Verschlüsselungsverfahren zu knacken.

In dieser Arbeit wird die Funktionsweise von Quantencomputern und deren aktueller technischer Reifestand evaluiert und die Bedrohung durch theoretische Angriffsmodelle dargestellt. Neben Quantencomputern werden auch Ziele und Standards der Informationssicherheit beschrieben und allgemeine sowie spezielle Schutzmaßnahmen wie Post-Quanten-Kryptographie genannt.

Ziel des empirischen Teils dieser Arbeit war es, gemeinsam mit Expert_innen aus den Bereichen IT, IT-Sicherheit und Risikomanagement zu evaluieren, ob sich österreichische Unternehmen der Angriffsszenarien durch Quantencomputer bewusst sind. Darüber hinaus wurden potenzielle Maßnahmen dagegen sowie deren Implementierung diskutiert.

Die Arbeit kommt zu dem Schluss, dass sich facheinschlägige Führungskräfte durchaus mit Quantencomputern befasst haben und sich auch dem Risiko bewusst sind. Da diese aktuell mit dringenderen und wesentlicheren Bedrohungen zu kämpfen haben, sind aktuell noch keine Maßnahmen wie die Implementierung von Post-Quanten-Kryptographie geplant.

Schlagwörter:

Quantencomputer, Informationssicherheit, Kryptographie, Post-Quanten-Kryptographie, Quantenkryptographie, Österreich, Unternehmen

Abstract: Quantum Computing: Threat Scenario for State of the Art Information Security?

Quantum computers have the potential to solve major mathematical and economic problems through their immense computational power. At the same time this computing power can be used to crack asymmetric encryption standards which are deeply integrated in nearly every IT infrastructure today.

In this thesis, the capabilities and the technological level of maturity are evaluated and theoretical attack models are shown. In addition to quantum computers also information security goals and standards are discussed and general as well as specific protective measures like post quantum cryptography are described.

The purpose of the empirical part was to evaluate together with experts in the fields of IT, IT security and risk management whether Austrian companies are aware of the attack scenarios with quantum computers. Additionally, potential measures and their implementation were discussed.

The work concludes that relevant managers are already aware of quantum computers and the risk. As they currently must deal with more urgent and significant threats, there are currently no measures like post-quantum cryptography implementations planned.

Keywords:

Quantum Computing, Information Security, Cryptography, Post-Quantum-Cryptography, Quantum Cryptography, Austria, Companies

Danksagung

Zunächst bedanke ich mich bei Christoph Jungbauer, BA MA MA. Danke, dass du mich während meiner Masterarbeit laufend unterstützt und mir auf effiziente, unkomplizierte Art und Weise mit deinem breiten Fachwissen zur Seite standest.

Zusätzlich danke ich allen Expert_innen, die mich im Zuge des empirischen Teils mit ihrer Expertise unterstützt haben und damit das Ergebnis dieser Arbeit maßgeblich geprägt haben.

Ein weiterer wichtiger Dank gilt meiner Lerngruppe. Ohne Eurer tatkräftigen Unterstützung im gemeinsamen Kampf gegen die vielzähligen Problemstellungen und dem gegenseitigen „in den Arsch treten" wären wir alle wahrscheinlich weniger erfolgreich durchs Studium geschritten.

Gleichzeitig gilt besonderer Dank gilt meinen Eltern. Danke, dass ihr euch (irgendwann im Jahr 1988) die Mühe gemacht habt, mich zu realisieren und zu formen – ohne euch wäre ich heute nicht hier. Wenn ich für diese Arbeit ein sehr gut bekomme, widme ich es euch! Ein mindestens so großer Dank gilt meiner Freundin/ Lebensabschnittspartnerin/Lebensgefährtin Sophia (unzutreffendes kann später gestrichen werden). Danke, dass du mich freiwillig gewählt und nicht innerhalb der 14-tägigen Rückgabefrist reklamiert hast. Danke, dass du mich während meiner exzessiven Abkapselung doch immer wieder in die Realität zurückgeholt und geerdet hast, auch wenn das nicht einfach war. Und danke, dass du diese Arbeit Korrekturlesen wirst, auch wenn du zum Zeitpunkt dieser Danksagung noch nichts von deinem Glück gewusst haben wirst.

Zu guter Letzt danke ich meinen beiden Katzen Frederik und Frida, die mir kontinuierlich von allen Seiten konstruktive Ratschläge unterbreitet und/oder (je nach Tagesverfassung) mich tatkräftig vom Fortschritt dieser Arbeit abgehalten haben.

Inhaltsverzeichnis

1. Einleitung

1.1 Problemstellung und Relevanz

Quantencomputer werden in vielen Bereichen als Disruptoren für bedeutende wirtschaftliche und gesellschaftliche Probleme gesehen: Begonnen mit künstlicher Intelligenz über die Lösung von Simulations- und Optimierungsproblemen bis hin zu neuen Quantensprüngen bei der Bekämpfung des Klimawandels – die Technologie hinter Quantencomputern bringt viele bedeutsame Chancen mit sich (IST Austria, 2021).

Doch gleichzeitig birgt die Technologie auch Risiken: So wird auch vor der Rechenkraft von Quantencomputern gewarnt, weil sie eine Gefahr für State of the Art Verschlüsselungstechnologien darstellt. Diese basieren beispielsweise auf Primfaktorenzerlegung und sind durch gängige Angriffsszenarien praktisch nicht zu knacken. Durch die grundlegend neue Funktionsweise von Quantencomputern ist es deren Recheneinheiten jedoch möglich, mehrere Zustände gleichzeitig einzunehmen und somit mehrere Berechnungen parallel durchzuführen. Auf diese Art und Weise könnte es in naher Zukunft realistisch sein, aktuell als sicher geltende Verschlüsselungstechnologien von Banken, kritischer Infrastruktur, Privatpersonen u.v.m. mit geringem Zeitaufwand zu entschlüsseln (KPMG, 2019).

Genau aus diesem Grund beschäftigen sich Wissenschaftler_innen rund um die Welt mit der Entwicklung von Verschlüsselungstechnologien, die ebenfalls auf Quantenphysik beruhen und sicher gegen Angriffe durch Quantencomputer sind (**Quantenkryptographie**). Gleichzeitig wird an Technologien geforscht, mit denen bereits bestehende Systeme auch ohne Zuhilfenahme von quantenmechanischen Zuständen für die Zeit der Quantencomputer gerüstet werden können (**Post-Quanten-Kryptographie**) (Infineon, 2021).

So haben *Chen et al.* vom amerikanischen *NIST* bereits im Jahr 2016 einen Standardisierungsprozess mit dem Ziel ins Leben gerufen, Algorithmen für die Verschlüsselung bzw. Schlüsselaustausch sowie für digitale Signaturen zu standardisieren (Chen et al., 2016). Dieser Prozess ist aktuell noch im Gange und seit Oktober 2020 in der dritten Runde, wobei ein erster Entwurf des Standards zwischen 2022 und 2024 zu erwarten ist (Computer Security Division, 2017). Auch die europäischen Organisationen *ETSI* (ETSI, 2020) und *ENISA* (ENISA, 2021) sowie das deutsche *BSI* (BSI, 2021a, 2021b) haben in den letzten Jahren laufend wissenschaftliche Paper

veröffentlicht, die die Bedeutung der Post-Quanten-Kryptographie unterstreichen und erste Handlungsempfehlungen festhalten.

Zusätzlich liefert auch die wissenschaftliche Community im Bereich der Post-Quanten-Kryptographie wichtige Erkenntnisse. *Mosca* kam bereits 2018 zu dem Schluss, dass Quantencomputer bedeutende Probleme lösen können, aber die katastrophalen Auswirkungen auf die Cybersecurity noch vor deren Reife gelöst werden müssen (Mosca, 2018). *Yunakovski et al.* analysierten einige Lösungsansätze und schlugen dazu vor, bereits jetzt hybride Lösungen aus schon standardisierten, nicht quantensicheren Verschlüsselungen und Post-Quanten-Lösungen zu verwenden (Yunakovsky et al., 2021). *Tan* et al. gingen einen Schritt weiter und erstellten ein Requirements Framework auf Basis von 14 echten Anwendungsfällen im Bereich von digitalen Signaturen (Tan et al., 2022). *Joseph et al.* ergänzten dazu, dass das Bedrohungsrisiko mit der Entwicklung von Frameworks und Standardisierungen nicht gelöst ist. Schließlich müssen noch Milliarden alter Geräte umgestellt werden, was mehrere Jahrzehnte dauern kann (Joseph et al., 2022).

Quantencomputer sind allerdings kein neues Themengebiet, sondern sie werden in der Literatur schon seit langer Zeit thematisiert. So geht das erste Paper von *Richard Feynman* ins Jahr 1982 zurück (Feynman, 1982). Doch seit diesem Zeitpunkt wurden wesentliche technologische Fortschritte erzielt und die Realisierung überlegener Quantencomputern ist in greifbarer Nähe (BSI, 2020). So wurde die Quantenüberlegenheit bereits im Jahr 2019 von Googles Forschungsteam rund um *Arute et al.* ausgerufen (Arute et al., 2019) und im Jahr 2021 wurden zwei weitere Papers von *Wu et al.* (Wu et al., 2021) und *Zhong et al.* (Zhong et al., 2021) veröffentlicht, die ebenfalls Quantenüberlegenheit behaupten.

Auch wenn es sich um sehr spezielle Experimente handelt und universell einsetzbare Quantencomputer wohl noch in der Ferne liegen (KPMG, 2019), stellt sich bereits jetzt eine bedeutende Frage: Wie rüsten wir uns für den Zeitpunkt, an dem Quantencomputer unsere State of the Art Verschlüsselungsverfahren in Sekundenbruchteilen knacken können und wie sichern wir unsere Daten, Passwörter und Geheimnisse vor dem Post-Quanten-Zeitalter?

1.2 Arbeitsziel

Ziel der vorliegenden Masterarbeit soll sein, das Risiko von Angriffen durch Quantencomputer in den nächsten zehn Jahren einzuschätzen. Darauf aufbauend sollen

weiters geeignete Schutzmechanismen der Quantenkryptographie und der Post-Quanten-Kryptographie identifiziert werden. Wie eingangs erwähnt, existieren aktuell bereits einige potenzielle Verfahren und Standardisierungsprozesse, mit denen das Angriffsrisiko durch Quantencomputer minimiert werden kann. Dabei handelt es sich allerdings noch um sehr generelle Ansätze im Entwurfsstadium. Eine Forschungslücke wurde in der Erhebung von Awareness, Resilienz und Adaption dieser Ansätze von Unternehmen identifiziert. Davon abgeleitet soll im Zuge der Arbeit die Forschungslücke geschlossen werden, ob sich österreichische Unternehmen dem Sicherheitsrisiko Quantencomputer bereits bewusst sind und welche Informationssicherheitsansätze gegen das zu erwartete Sicherheitsrisiko adaptiert wurden. Schlussendlich wird eine Handlungsempfehlung für den Schutz gegen Angriffe durch Quantencomputer erarbeitet und gegebenenfalls weitere noch wenig erforschte Forschungsfelder identifiziert.

Bezogen auf den Lehrplan des Masterstudiums WIMA, wird in dieser Arbeit vorrangig das Wissen aus dem Bereich IT-Security angewandt und vertieft. Hierzu zählen beispielsweise vorangegangene Lehrveranstaltungen wie „Informationssicherheitsmanagement“, „Technische Sicherheitsaspekte“ oder „Kryptographie und Zugriffskontrolle“.

1.3 Forschungsfrage

Aus dem bisher beschriebenen und der Zielsetzung dieser Masterarbeit lässt sich nun folgende Forschungsfrage ableiten:

- Inwieweit sind sich österreichische Unternehmen dem Sicherheitsrisiko durch Angriffe mittels Quantencomputern bewusst?

Ferner leiten sich aus der Forschungsfrage folgende Sub-Forschungsfragen ab:

- Welche Lösungen bieten Quantenkryptographie und Post-Quanten-Kryptographie für die Entwicklung sicherer Verschlüsselungstechnologie?
- Wie hoch ist die Aufmerksamkeit von Unternehmen hinsichtlich dem Sicherheitsrisiko Quantencomputer („Awareness“)?
- Welche Maßnahmen werden gegen das Angriffsszenario durch Quantencomputer getroffen („Adoption“)?
- Wie anpassungsfähig sind Unternehmen in Bezug auf die Implementierung einer quantensicheren IT-Infrastruktur („Resilienz“)?

- Inwieweit sind sich Unternehmen dem Risiko durch Store-now-decrypt-later Angriffe bewusst?

1.4 Methodische Vorgehensweise

1.4.1 Theoretische Vorgehensweise

Die Basis der vorliegenden Masterarbeit liegt in einer Literaturrecherche, auf dessen Grundlage schließlich der empirische Teil aufgebaut wird. Zu Beginn wird die Funktionsweise von Quantencomputern erläutert und der grundlegende Unterschied zur klassischen CPU-Rechenleistung abgegrenzt (Feynman, 1982). Dabei werden einfache Basisgrundlagen aus der Quantenphysik und deren Anwendung bei Quantencomputern beschrieben (Preskill, 2021). Anschließend wird ein kurzer Überblick über die Anbieter und den aktuellen Reifegrad der Technologie gegeben (Arute et al., 2019; Moguel et al., 2022) bevor auf die vielversprechendsten Anwendungsmöglichkeiten (QUTAC et al., 2021) von Quantencomputern eingegangen wird. Darüber hinaus folgt eine kurze Einführung in das IT-Sicherheitsmanagement, dessen Schutzziele und das IT-Risikomanagement, ehe über kryptographische Verfahren (Mavroeidis et al., 2018; Thakkar, 2016) auf die beiden für diese Arbeit vorrangigen Algorithmen von *Shor* (Shor, 1994) und *Grover* (Grover, 1996) und deren Bedrohungsszenarien übergeleitet wird.

Im Kapitel Quantenkryptographie werden dann Verfahren zur sicheren Übertragung wie der *BB84* (Bennett and Brassard, 1984) sowie seine Erweiterungen beschrieben und dabei Wege aufgezeigt, ob und wie Informationen durch Zuhilfenahme von Quantenzuständen abhörsicher ausgetauscht werden können. Anschließend wird der Fokus auf das Feld der Post-Quanten-Kryptographie gelegt (Joseph et al., 2022; Mavroeidis et al., 2018). Dabei wird beleuchtet, welche Lösungen die moderne Kryptographie gegen die Bedrohung durch Quantencomputer entwickelt (BSI, 2021b). Anschließend werden Maßnahmen aus den Konzepten der Quantenkryptographie und der Post-Quanten-Kryptographie abgeleitet und ein kurzer theoretischer Ausblick hinsichtlich Sicherheitsrisiken gegeben (BSI, 2021b; Lau and Lo, 2011). Abschließend wird noch der Store-now-decrypt-later Angriff erläutert und dessen Auswirkungen auf die Informationssicherheit dargestellt (Mosca, 2018).

1.4.2 Empirische Vorgehensweise

Bei der Entscheidung hinsichtlich Forschungsdesign der Masterarbeit wurden der aktuelle Bekanntheitsgrad und die Anzahl an verfügbaren Studien zur Themenstellung

betrachtet. Zum einen existieren zur gewählten Forschungsfrage noch wenige und unklare Thesen in der Fachliteratur, zum anderen handelt es sich bei dem Forschungsinhalt aktuell noch um ein Nischenthema. Es wird daher der qualitative Forschungsansatz gewählt. Dies lässt sich weiterführend dadurch begründen, dass zum gegebenen Zeitpunkt nur ausgewiesene Experten und Führungskräfte aus dem IT-Sicherheits- und Risikomanagementbereich (z.B. CISOs) verwertbare Aussagen diesbezüglich liefern können. Aus diesem Grund wird als Methode für die Datenerhebung das qualitative Expert_inneneninterview herangezogen.

Konkret werden nach Erarbeitung der theoretischen Konzepte mehrere Kategorien gebildet und in einen Interviewleitfaden überführt. Anschließend werden dazu bis zu sieben Expert_innen aus den Funktionsbereichen IT-Sicherheit und Risikomanagement befragt. Um einen validen Querschnitt der betroffenen Bereiche zu finden, werden Personen aus den Branchen Bank, Versicherung, kritische Infrastruktur, Industrie, Politik, Beratung sowie aus einem KMU gewählt. Die Auswahl und Kontaktaufnahme der Interviewpartner erfolgten über das eigene Netzwerk, weshalb sowohl Person als auch Unternehmen aus Sicherheitsgründen anonymisiert werden und lediglich die Branche sowie die Position bekanntgegeben werden. Im nächsten Schritt werden die Interviews mit einer qualitativen Inhaltsanalyse nach *Mayring* ausgewertet. Dabei wird sich der Methode der Zusammenfassung bedient, da damit Überschneidungen und Unterschiede der Interviewpartner_innen gut herausgearbeitet und anschließend diskutiert werden können (Mayring, 2015). Zu guter Letzt werden die Ergebnisse aus der empirischen Untersuchung mit der vorhandenen Literatur diskutiert und in eine Handlungsempfehlung überführt.

2. Quantencomputer

Zu Beginn der Arbeit wird die grundlegende Funktionsweise von Quantencomputern beschrieben und ein Grundwissen zu Quantenmechanik und Qubits vermittelt.

Das Konzept von Quantencomputern geht auf den Physiker Richard Feynman zurück, der diese erstmals in seinem Werk *Simulating Computers with Physics* (Feynman, 1982) im Jahr 1982 erwähnte. Dabei postulierte er, dass sich Computer unter Zuhilfenahme von Quantenzuständen für die Berechnung komplexer Problemstellungen eignen könnten. 40 Jahre später befinden sich die großen Technologiekonzerne im Wettbewerb um Quantencomputer und die erwartete Überlegenheit gegenüber herkömmlichen Computern ist nur noch eine Frage der Zeit (Preskill, 2021).

2.1 Funktionsweise klassischer Computer

Bevor auf die Eigenschaften von Quantencomputern eingegangen werden kann, muss die Funktionsweise klassischer Computer näher betrachtet werden. Im Wesentlichen bestehen Computerchips aus Milliarden mikroskopischer Schaltkreise, die mit Ein- und Ausschaltern, den sogenannten Transistoren, ausgestattet sind. Fließt ein Strom durch einen Schaltkreis hindurch, so nimmt die kleinste Recheneinheit, das sogenannte **Bit** vereinfacht den Wert 1 an, andernfalls den Wert 0 (IST Austria, 2021). Abbildung 1 zeigt ein NAND-Gatter („not and“), das nach folgender Logik funktioniert: Sind alle Eingänge 1, so wird am Ausgang 0 ausgegeben. Sobald einer der Eingänge den Wert 0 hat, gibt das Gatter den Wert 1 für das Bit aus.

x	y	$x \uparrow y$
0	0	1
0	1	1
1	0	1
1	1	0

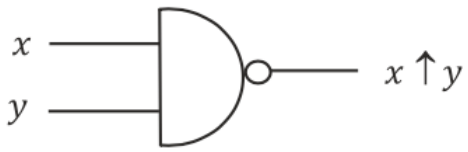

Abbildung 1: NAND-Gatter (Mainzer, 2020, p. 15)

Durch die Aneinanderreihung mehrerer Bits entsteht der sogenannte *Binärcode,* mit dem schließlich Buchstaben, Zahlen und Rechenoperationen kodiert werden. Diese Vorgehensweise bildet die Basis für alle Computerfunktionen. Der *American Standard*

Code for Information Interchange (kurz *ASCII*) kodiert beispielsweise den (Groß-) Buchstaben „A“ als 10000001 *(ASCII, 2022)*.

Abbildung 2 zeigt dazu eine Auflistung der ASCII Zeichen und deren Bedeutung in Dezimal- und Binärcodierung. Das am Ende angefügte Beispiel verdeutlicht, dass es aus Sicht eines Computers bei Wörtern lediglich um eine Aneinanderreihung von Nullen und Einsen handelt.

Binary	Decimal	Glyph
0100000	32	space
0100001	33	!
0100010	34	”
0100011	35	#
0100100	36	$
0100101	37	%
0100110	38	&
0100111	39	’
0101000	40	(
0101001	41	)
0101010	42	*
0101011	43	+
0101100	44	,
0101101	45	-
0101110	46	.
0101111	47	/
0110000	48	0
0110001	49	1
0110010	50	2
0110011	51	3
0110100	52	4
0110101	53	5
0110110	54	6
0110111	55	7
0111000	56	8
0111001	57	9
0111010	58	:
0111011	59	;
0111100	50	<
0111101	61	=
0111110	62	>
0111111	63	?

Binary	Decimal	Glyph
1000000	64	@
1000001	65	A
1000010	66	B
1000011	67	C
1000100	68	D
1000101	69	E
1000110	70	F
1000111	71	G
1001000	72	H
1001001	73	I
1001010	74	J
1001011	75	K
1001100	76	L
1001101	77	M
1001110	78	N
1001111	79	O
1010000	80	P
1010001	81	Q
1010010	82	R
1010011	83	S
1010100	84	T
1010101	85	U
1010110	86	V
1010111	87	W
1011000	88	X
1011001	89	Y
1011010	90	Z
1011011	91	[
1011100	92	\
1011101	93	]
1011110	94	^
1011111	95	_

Binary	Decimal	Glyph
1100000	96	`
1100001	97	a
1100010	98	b
1100011	99	c
1100100	100	d
1100101	101	e
1100110	102	f
1100111	103	g
1101000	104	h
1101001	105	i
1101010	106	j
1101011	107	k
1101100	108	l
1101101	109	m
1101110	110	n
1101111	111	o
1110000	112	p
1110001	113	q
1110010	114	r
1110011	115	s
1110100	116	t
1110101	117	u
1110110	118	v
1110111	119	w
1111000	120	x
1111001	121	y
1111010	122	z
1111011	123	{
1111100	124	|
1111101	125	}
1111110	126	~

$$\underbrace{1010100}_{\text{T}}\underbrace{1101111}_{\text{o}}\underbrace{1101101}_{\text{m}} = \text{Tom}$$

Abbildung 2: ASCII Code (Wong, 2022)

Grundsätzlich erfolgen in einem klassischen Computer alle Berechnungen seriell, also nacheinander. Aus diesem Grund stehen klassische Computer bei zunehmender Komplexität von Rechenaufgaben vor Herausforderungen, wie beispielsweise bei Optimierungsproblemen. Möchte ein Computer die kürzeste Wegstrecke von A nach B berechnen (auch bekannt als **Travelling Salesman Problem**), so muss dieser alle möglichen Wege von A nach B simulieren und nach Beendigung die Ergebnisse miteinander vergleichen. Diese Vorgehensweise wird bei Hinzukommen jeder weiteren Wegvariable komplexer und steigt exponentiell (Infineon, 2021). Warum das so ist, wird in der Disziplin der Komplexitätstheorie behandelt.

Die Komplexitätstheorie stammt aus der theoretischen Informatik und beschäftigt sich mit dem Aufwand, der für die Berechnung spezieller Problemstellungen benötigt wird. Dabei wird nach den Parametern Geschwindigkeit und Speicherbedarf unterschieden, wobei letzterer aufgrund der enormen verfügbaren Speicherkapazitäten bereits an Bedeutung verloren hat. Um die Komplexität zu beschreiben, wird die sogenannte O-Notation verwendet. Bei dem Algorithmus $O(n)$ kann damit beispielsweise von einem linearen Aufwand und bei $O(n^2)$ von einem quadratischen Aufwand gesprochen werden (Dempe and Schreier, 2006, p. 345 f.). Generell wird zwischen zwei Komplexitätsklassen unterschieden:

- Ist der Aufwand zur Lösung eines Problems für gewöhnlich konstant, linear oder quadratisch, so wird von einer polynominalen Komplexität gesprochen. Diese Berechnungen können durch stärkere CPUs beschleunigt werden und die dazugehörigen Probleme sind generell als **Komplexitätsklasse „P“** bekannt (Köbler and Beyersdorff, 2006).
- Steigt der Aufwand der Berechnungen nicht linear oder quadratisch, sondern exponentiell oder fakultativ an, so ist von einer **nichtpolynomen Komplexität** die Rede. Ein Beispiel stellt das bereits beschriebene Travelling Salesman Problem dar: Die Schwierigkeit hinter dieser Berechnung liegt darin, dass eine Steigerung der Rechenleistung aufgrund der hohen Komplexität keine nennenswerten Vorteile bringt und aktuell auch keine effizienten Algorithmen bekannt sind. Alle Probleme, die in nichtpolynominaler Laufzeit lösbar sind, aber deren Lösung in polynominaler Zeit überprüft werden kann, werden in die **Klasse „NP“** eingeordnet. Dabei wird zusätzlich noch in NP und NP-schwere Probleme unterschieden, wobei sich diese beiden Kategorien teilweise überschneiden. Alle Probleme, für die diese Überschneidung zutrifft, werden als NP-vollständig bezeichnet (Nebel and Wild, 2018, p. 467ff.).

Tabelle 1 verdeutlicht den Unterschied zwischen polynominaler und exponentieller Rechenzeit bei 10^9 Elementaroperationen pro Sekunde.

n	20	40	60	80	100
n^2	4.10^{-7} Sek.	2.10^{-6} Sek.	4.10^{-6} Sek.	6.10^{-6} Sek.	1.10^{-5} Sek.
2^n	1.10^{-3} Sek.	18 Minuten	37 Jahre	38.10^6 Jahre	n.V.

Tabelle 1: Unterschied polynominaler zu exponentieller Rechenzeit (Dempe and Schreier, 2006, p. 347)

Eine Besonderheit von NP-vollständigen Problemen liegt darin, dass sich alle Probleme aus NP darauf zurückführen lassen. Gelingt es also, ein NP-vollständiges Problem in polynominaler Laufzeit zu lösen, dann wären alle Probleme aus NP in polynominaler Zeit lösbar. Seit längerer Zeit existiert ein wissenschaftlicher Diskurs zu dem mathematischen Problem, ob P = NP ist oder nicht. Bislang konnte weder bewiesen noch widerlegt werden, ob P = NP bzw. P ≠ NP zutrifft. Dieses Problem ist so populär, das es in die sieben „Millennium Prize Problems“ aufgenommen wurde und für dessen Lösung ein Preisgeld von einer Million Dollar ausgesetzt wurde (Köbler and Beyersdorff, 2006).

2.2 Funktionsweise von Quantencomputern

Im Unterschied zu klassischen Computern basieren Quantencomputer nicht auf Stromflüssen und Bits, sondern auf Quantenbits, den **Qubits**. Bei diesen Qubits handelt es sich meist um Quantenteilchen wie Ionen, Elektronen oder Photonen, deren physikalische Eigenschaften eine grundlegend neue Art der Rechenleistung ermöglichen (Preskill, 2021). Für die Einführung in die Funktionsweise von Quantencomputern ist es zunächst notwendig, die Sonderheiten der Quantenmechanik zu verstehen.

2.2.1 Superposition

Während Bits in herkömmlichen Computern entweder den Wert 1 oder 0 annehmen können, ist der Wert bei Qubits nicht immer eindeutig. Viel mehr ermöglichen es die Gesetze der Quantenmechanik, dass sich die beiden Zustände 1 und 0 überlagern und das Qubit damit auch jeden Wert dazwischen annehmen kann (IST Austria, 2021). Diesen Zustand behält ein Qubit allerdings nur über den Zeitraum bei, in dem das Qubit unbeobachtet bleibt. Findet also eine Messung statt, so entscheidet sich das Qubit für einen Zustand und die jeweilige Berechnung ist damit abgeschlossen (BSI, 2021b). Bekannt ist dieses Phänomen auch unter dem Gedankenspiel von Schrödingers Katze: Wird eine Katze gemeinsam mit einer Giftampulle in eine Kiste gesperrt, ist die Katze bei

unverändertem Zustand gleichzeitig tot und lebendig. Erst wenn die Kiste geöffnet wird, kann die Katze mit Sicherheit als lebendig oder tot bezeichnet werden (BSI, 2021b).

Abbildung 3 zeigt eine **Bloch-Kugel**, mit der sich der Zustand eines Qubits vereinfacht in Richtung Nordpol als 0 und in Richtung Südpol als 1 interpretieren lässt. Befindet sich das Qubit in Superposition, so kann der Vektor in jede andere Richtung im Raum zeigen und die Zustände 0 und 1 befinden sich in Überlagerung. Zur Beschreibung dieser Zustände wird die sogenannte „Ket-Notation" verwendet. Die Schreibweise wird als $|0\rangle$ oder $|1\rangle$ dargestellt und bringt damit zum Ausdruck, dass sich das Qubit nur zu einer gewissen Wahrscheinlichkeit in dieser Position befindet (BSI, 2021b).

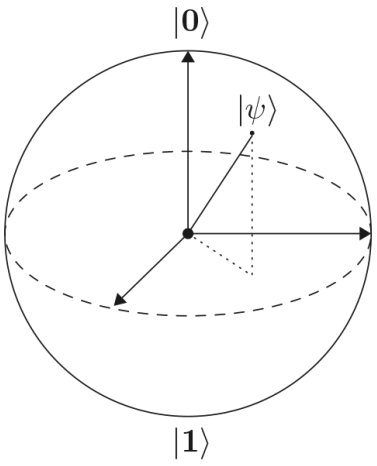

Abbildung 3: Qubit als Bloch-Kugel (BSI, 2021b)

2.2.2 Verschränkung

Eine weitere wesentliche quantenmechanische Besonderheit von Qubits liegt in der Verschränkung. So ermöglicht es die Quantenmechanik, dass sich mehrere Teilchen so verhalten, als wären sie ein einziges (IST Austria, 2021). Befindet sich eines von zwei verschränkten Qubits im Zustand $|1\rangle$, so kann mit Sicherheit gesagt werden, dass sich das andere zum Beispiel im genau gegengesetzten Zustand $|0\rangle$ befindet. Wird nun eines der beiden Qubits manipuliert, so ändert sich unmittelbar auch der Zustand des mit ihm verschränkten Qubits, unabhängig von dessen Entfernung (BSI, 2021b). Albert Einstein bezeichnete das Phänomen der Verschränkung als *Spukhafte Fernwirkung* (Heimann, 1973).

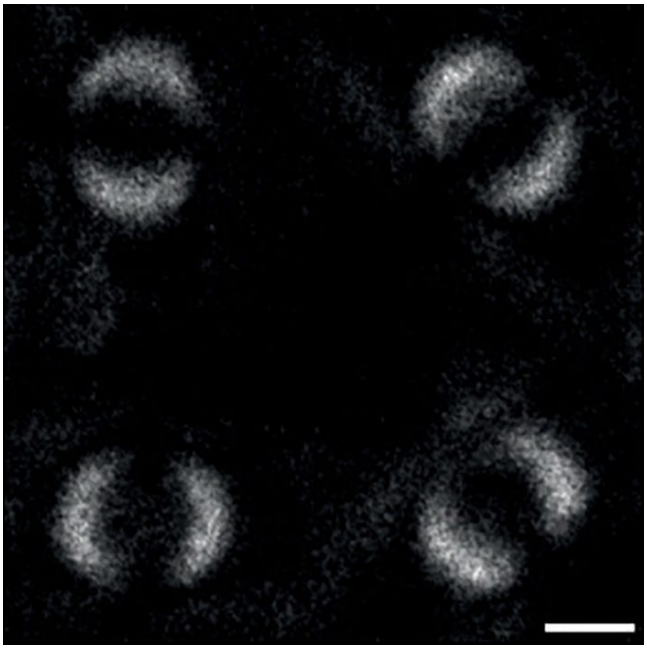

Abbildung 4: Quantenverschränkung (Moreau et al., 2019)

Abbildung 4 zeigt das erste jemals aufgenommene Foto einer Quantenverschränkung von Photonen.

2.2.3 Rechenleistung

Ein Quantencomputer macht sich die Kombination dieser beiden quantenmechanischen Eigenschaften zunutze. Werden beispielsweise zwei Qubits miteinander verschränkt, so können sie aufgrund der Superposition gleichzeitig vier verschiedene Zustände einnehmen. Mithilfe dieser Eigenschaft können Quantencomputer parallele Berechnungen durchführen und die Rechenleistung steigt durch Hinzufügen (bzw. Verschränken) weiterer Qubits exponentiell (Mavroeidis et al., 2018). Somit verarbeitet ein n-Qubit Quantencomputer zu einem Zeitpunkt also nicht einen einzigen Wert, sondern 2^n Werte gleichzeitig. Diese müssen anschließend noch über einen Sortieralgorithmus interpretiert und auf Fehler korrigiert werden, um schlussendlich das gewünschte, korrekte Ergebnis auszugeben (Preskill, 2021). Der Rechenvorteil, der daraus resultiert, wird in Abbildung 5 verdeutlicht.

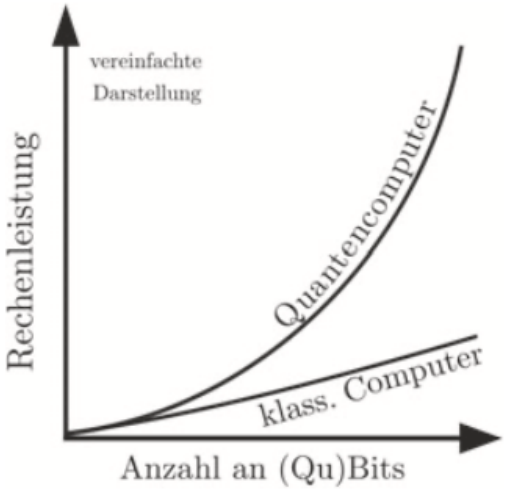

Abbildung 5: Rechenleistung von Quantencomputern (Ellerhoff, 2020, p. 14)

2.2.4 Quantengatter

Genauso wie klassische Computer für die Berechnung von Operationen auf logische Gatter aus Transistoren zurückgreifen, können auch Operationen oder Algorithmen von Quantencomputern durch sogenannten Quantengattern dargestellt werden. Diese unterscheiden sich allerdings dadurch, dass sie keine baulichen Elemente darstellen, sondern eine zeitlich steuerbare Wechselwirkung verschiedener Qubits zueinander (Ellerhoff, 2020, p. 15 f.).

Zunächst werden einfache, unitäre Transformationen erläutert. Eine Gruppe wichtiger Operationen sind die sogenannten Pauli-Matrizen bzw. **Pauli-Gatter**, die weiters in die einzelnen Transformationen X, Y und Z unterteilt werden.

Die **Operation X** kann auch als NOT-Gate bezeichnet werden und wird dazu verwendet, die Amplituden $|0\rangle$ und $|1\rangle$ zu tauschen. Mithilfe der Matrixschreibweise kann das wie folgt ausgedrückt werden:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Bei der **Y-Operation** wird der Zustand $|0\rangle$ zu $i|1\rangle$ und der Zustand $|1\rangle$ zu $-i|0\rangle$ transformiert, was folgender Matrixoperation entspricht:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Schlussendlich wird bei der **Operation Z** die Amplitude der Komponente $|1\rangle$ negiert, was auch als „Phaseflip“ bekannt ist. Der Zustand $|0\rangle$ bleibt von dieser Operation hingegen unberührt. Formal kann diese Operation wie folgt ausgedrückt werden:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Auf Basis dieser drei Operationen können bereits erste Rechenschritte mit Quantencomputer durchgeführt werden (Homeister, 2022, p. 79; Wong, 2022, p. 102). Abbildung 6 zeigt eine Zusammenfassung dieser Operationen sowie der dazugehörigen Pauli-Gatter.

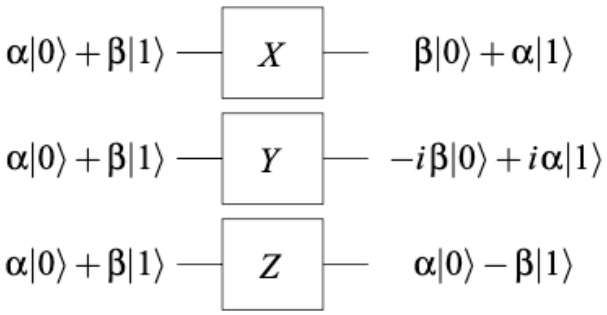

Abbildung 6: Schaltkreis von Pauli-Transformationen (Homeister, 2022, p. 79)

Wird noch einen Schritt tiefer gegangen, so können durch Kombination der nächsten beiden Operationen Qubits miteinander verschränkt werden.

Bei Anwendung eines **Hadamard-Gatters** wird der Zustand eines Qubits von $|0\rangle$ oder $|1\rangle$ auf eine Superposition, also eine Mischung der beiden Zustände verlagert. Auf der Bloch-Kugel befindet sich der Pfeil nun auf dem Äquator. Abbildung 7 zeigt ein Hadamard-Gatter, das die Zustände $|0\rangle$ und $|1\rangle$ in $|+\rangle$ und $|-\rangle$ transformiert.

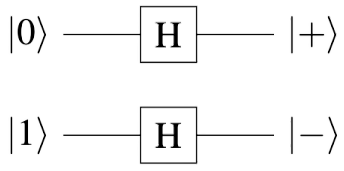

Abbildung 7: Hadamard-Gatter (Ellerhoff, 2020, p. 16)

Ebenfalls für die Verschränkung von Qubits kann das sogenannte **CNOT-Gatter** verwendet werden. Der Unterschied liegt darin, dass es Bedingungen an zwei Qubits stellt und dann entsprechende Manipulationen vornimmt. Befindet sich beispielsweise das Qubit A im Zustand $|0\rangle$, so ändert sich nichts. Befindet sich Qubit A allerdings im Zustand

|1⟩, wird das Qubit B umgedreht und es nimmt den gegenteiligen Wert an, wie Abbildung 8 zeigt.

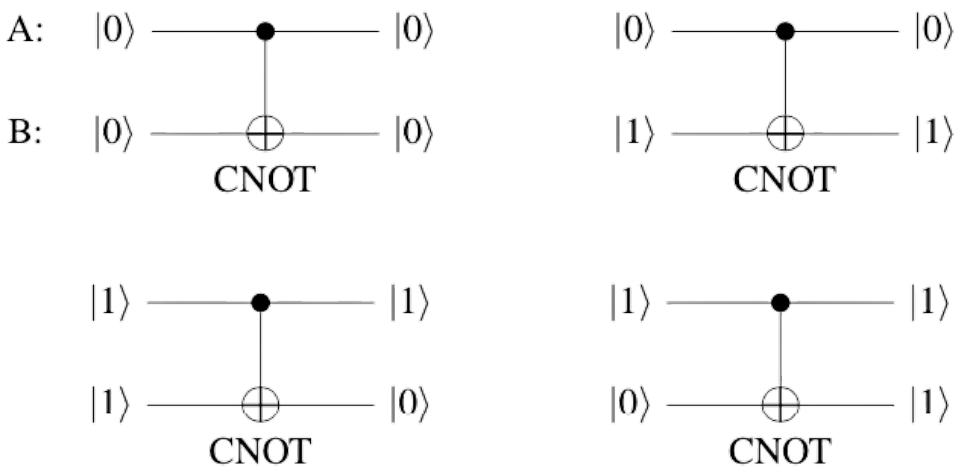

Abbildung 8: CNOT-Gatter (Ellerhoff, 2020, p. 17)

Werden nun diese beiden Operationen miteinander verknüpft, so erfolgt eine Verschränkung der beiden Qubits, die auch als Bell-Zustand bekannt ist (Ellerhoff, 2020, p. 15).

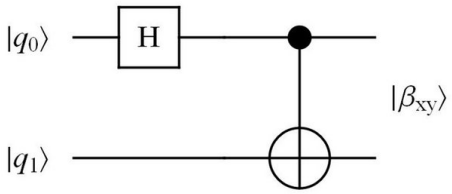

Abbildung 9: Bell-Zustand als Quantengatter (Bovino, 2019)

Mathematisch wird dieser Zustand wie folgt ausgedrückt:

$$|Q_A, Q_A\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$$

2.2.5 Hardwarearchitektur

Auch die Hardware von Quantencomputern unterscheidet sich wesentlich von klassischen Computern, wobei sich noch keine konkrete Architektur durchsetzen konnte. Viel mehr existieren in der aktuellen, experimentellen Phase von Quantencomputern verschiedene physikalische Ansätze, wie Qubits erzeugt und manipuliert werden können (BSI, 2020). Einige der aktuell vielversprechendsten Forschungsansätze werden nun kurz erläutert (IST Austria, 2021):

- Werden in einer Vakuumkammer elektromagnetische Felder erzeugt, so können die Elektronen in sogenannten **Ionenfallen** fixiert werden. Dabei werden die Elektronen, die als Qubits fungieren, mittels Laser manipuliert und in einen hohen oder niedrigen Orbital versetzt. Durch die Wechselwirkung mit benachbarten Ionen und die Lasermanipulation können damit verschiedene Operationen durchgeführt werden.
- Eine weitere Möglichkeit liegt darin, das Qubit mittels eines **supraleitenden Schaltkreises** abzubilden. Der Supraleiter wird dabei auf eine extrem niedrige Temperatur gekühlt, um einen widerstandslosen Stromfluss zu ermöglichen. Der Wert des Qubits wird dabei mithilfe von Mikrowellen ganz einfach durch die Richtung des Stromflusses bestimmt: Fließt der Strom also im Uhrzeigersinn, so kann das Qubit beispielsweise den Wert 0 annehmen und den Wert 1 bei Stromfluss gegen den Uhrzeigersinn. Fließt der Strom in beide Richtungen gleichzeitig, so tritt eine Überlagerung der Zustände und somit eine Superposition auf. Ein großer Vorteil dieser Technik liegt darin, dass die Qubits auf diese Weise in feste Schaltkreise eingebaut werden können.
- In einem weiteren Ansatz werden zwei Laser aufeinander gerichtet und dadurch dazwischenliegende Atome zum Schweben gebracht. Durch die damit entstandenen elektromagnetischen Felder bilden sich sogenannte Potentialtöpfe. Diese **optischen Gitter** können bildhaft mit Eierkartons verglichen werden und die in ihnen ruhenden Atome können als Qubits verwendet werden. Dabei speichert das Qubit die Information in den Energiezuständen der Elektronen. Aktuell wird daran geforscht, wie durch Ergänzung weiterer Laser die Qubitanzahl erhöht werden kann.
- Bei der Methode der **Stickstoff-Fehlstellen-Zentren** werden zwei benachbarte Kohlenstoffatome durch ein einziges Stickstoffatom ersetzt, wodurch eine Fehlstelle entsteht. Genau dorthin werden Elektronen der benachbarten Kohlenstoffatome angezogen. Ihr Drehimpuls bzw. Spin (oben oder unten) stellt schließlich die Information des Qubits dar. Der Vorteil dieser Variante liegt darin, dass sie bei Raumtemperatur funktioniert. Allerdings ist sie noch wenig erforscht.
- Ein sehr fehlertoleranter Ansatz liegt in der Verwendung **topologischer Qubits**. Dabei werden theoretische, physikalische Phänomene bei niedrigen Temperaturen und starken Magnetfeldern vorhergesagt und damit mehrere Quantensysteme zu sogenannten Quasiteilchen kombiniert. Diese Quasiteilchen speichern die Information in ihrem Quantenzustand ab, agieren miteinander und führen damit

Berechnungen durch. Noch ist nicht zweifelsfrei geklärt, ob topologische Quantencomputer überhaupt funktionieren können.

- Zu guter Letzt sind sogenannte **Quanten-Annealer** Quantencomputer, die sich besonders gut für die Optimierung komplexer Probleme eignen. Auch sie basieren auf supraleitenden Schaltkreisen, die Problemstellungen in physikalischer Art und Weise beschreiben. Sie können als imaginäre Landschaften mit Bergen und Tälern vorgestellt werden, wobei sich der Quantenzustand wie Regenwasser verhält, das an den tiefsten Punkt hinunterläuft und damit das Ergebnis herausgibt. Aufgrund ihrer grundlegend unterschiedlichen Funktionsweise können von ihnen nur sehr spezielle Quantenalgorithmen ausgeführt werden (IST Austria, 2021).

2.3 Entwicklungsstand von Quantencomputern

Auch wenn die Möglichkeiten von Quantencomputern ein großes Maß an Euphorie hervorbringen können, so liegen diese Visionen aktuell noch in der Zukunft. So bezeichnet *Preskill* (Preskill, 2021) den aktuellen Entwicklungsstand als die **Noisy Intemediate-Scale Quantum Era** (kurz „NISQ era“). Damit bezieht er sich auf ein wesentliches Problem in der Entwicklung von Quantencomputern: Um komplexe Berechnungen mit Quantencomputern durchzuführen, muss die Superposition über lange Zeit aufrechterhalten werden. Aufgrund ihrer quantenmechanischen Eigenschaften sind Qubits allerdings sehr fehleranfällig, weshalb minimalste Störungen wie z.B. das Rauschen der Elektronik zu Rechenfehlern führen kann. Während diese Rechenfehler in klassischen Computern durch Redundanzen in der Codierung behoben werden, stellt diese Fehlerkorrektur für Quantensysteme große technische Herausforderungen dar.

Somit kann bloß über die Anzahl von Qubits keine klare Aussage zur Leistungsfähigkeit von Quantencomputern getroffen werden. Vielmehr müssen die Fehlerrate und -korrektur berücksichtigt werden, sodass nur ein fehlerfreier, funktionsfähiger Quantencomputer sinnvolle Ergebnisse liefert. Ein Lösungsansatz liegt darin, mehrere Qubits zu sogenannten logischen Qubits zusammenzufassen und damit eine höhere Fehlertoleranz zu schaffen. Bis die ersten fehlerfreien und rechenstarken Quantencomputer auf den Markt kommen, werden allerdings noch einige Jahre vergehen (Preskill, 2021).

2.4 Anbieter von Quantencomputern

In den letzten Jahren hat sich ein regelrechter Wettbewerb um die Entwicklung von Quantencomputern entwickelt. Federführend sind dabei die Akteure Google und IBM, wobei auch zahlreiche andere Technologieunternehmen im Rennen um die technologische Vorherrschaft im Spiel sind (BSI, 2020).

Google war das erste Unternehmen, das 2019 eine Überlegenheit gegenüber klassischen Computern, kurz Quantenüberlegenheit ausrief. Es handelte sich dabei allerdings um ein rein akademisches Problem ohne bekannte praktische Anwendung. Der 53-Qubit Prozessor Sycamore errechnete dieses in 200 Sekunden, wohingegen der schnellste Supercomputer der Welt 10.000 Jahre benötigt hätte (Arute et al., 2019). Google möchte mehrere Milliarden US-Dollar in ihren Quantum-AI-Campus investieren, um bis 2029 die ersten fehlerfreien, kommerziellen Quantencomputer zu realisieren (Petereit, 2021). Zur Programmierung von Quantenalgorithmen hat Google das hauseigene Cirq-Framework im Einsatz, mit dem auch online Quantensimulationen durchgeführt werden können (Google Quantum AI, 2022).

Als aktuell größter Mitbewerber ließ **IBM** mit Kritik an Googles Erfolgsmeldung zur Quantenüberlegenheit nicht lange warten und behauptete, dass die Aufgabe mit Supercomputern in nur 2,5 Tagen gelöst werden könnte. IBM konnte das allerdings nicht beweisen (Pednault et al., 2019). Im Wettlauf um die Vorherrschaft im Markt hat sich IBM ebenfalls eine ehrgeizige Roadmap für die Entwicklung ihrer Quantencomputer gesetzt: Mit IBM Quantum Osprey wurde bis Ende des Jahres 2022 ein 433-Qubit Prozessor und bis Ende 2026 ein fehlerfreier Quantencomputer mit mehreren zehntausenden Qubits ankündigt. Zum aktuellen Zeitraum ist mit IBM Quantum Eagle ein Prozessor mit 127-Qubits im Einsatz (IBM, 2022a). Darüber hinaus bietet IBM mit Qiskit Runtime eine Quantum Computing as a Service Lösung an, mit der der 27-Qubit Falcon und der 127-Qubit Eagle Prozessor über eine Cloud-Lösung verwendet werden können (IBM, 2022b).

Den laut eigenen Angaben aktuell stärksten Quantencomputer produziert der Hersteller **DWAVE** mit dem 5000+ Qubits starken Quantencomputer *Advantage* (D-Wave, 2022), dessen Technologie sich von jener anderer Hersteller stark unterscheidet. Dieser Adiabatic Quantum Computer basiert auf der Technologie des Quantum Annealing. Auch wenn Performancesteigerungen beim Vorgängermodell gegenüber Supercomputern

bewiesen werden konnten, ist die Realisierung einer exponentiellen Leistungssteigerung mit dieser Technologie aktuell umstritten (Gibney, 2017).

Auf der anderen Seite des Globus wurde in China ein Quantencomputer namens **Zuchongzhi 2** gebaut, der mit 66 Lichtphotonen-Qubits rechnet und die Rechenleistung von Googles Sycamore angeblich mit dem Faktor zehn Millionen übertrifft. Nichtsdestotrotz ist auch dieser Computer noch sehr fehleranfällig und nur für sehr beschränkte Aufgaben einsetzbar (Wu et al., 2021).

Zusätzlich zählen beispielsweise noch Honeywell (Honeywell, 2022), Intel (Intel, 2022), IonQ (IonQ, 2022), Rigetti (Rigetti, 2022) und weitere kleinere Unternehmen zu den Wettbewerbern, die leistungsstarke Quantencomputer versprechen. Seit einiger Zeit fördert auch die Europäische Union mit dem EU Flagship Programme (European Commission, 2020) Initiativen wie den Bau des OpenSuperQ (OpenSuperQ, 2022) oder AQTION (AQTION, 2022).

Schließlich haben auch Microsoft und Amazon ihren Platz im Wettbewerb um Quantencomputern gefunden: So positioniert sich **Microsoft** mittlerweile mit *Azure Quantum* (Azure Quantum, 2022) als Dienstleister, der einen Cloudzugang zu Quantencomputern wie Honeywell und IonQ anbietet (Marre, 2021). Passend dazu entwickelte Microsoft mit Q# eine eigene Programmiersprache für Quantencomputer (Bradben, 2022). Ebenso positionierte sich 2020 **Amazon** mit *Amazon Braket* (Amazon Braket, 2022) als Quantencomputer-Cloudanbieter, der über den Clouddienst AWS Zugang zu Quantencomputern von D-Wave, IonQ, Rigetti, OQC und XANADU ermöglicht. 2021 eröffnete Amazon Web Sevices einen gemeinsamen "Hub of Quantum Computing" mit dem California Institute of Technology (Caltech, 2021).

2.5 Anwendungsfälle für Quantencomputer

Nachdem nun die wichtigsten Anbieter von Quantencomputer bekannt sind, stellt sich noch die Frage nach den Anwendungsfeldern, in welchen Quantencomputer effektiv eingesetzt werden können.

Wie im Kapitel 2.1 bereits kurz angeschnitten wurde, stellen Optimierungsprobleme wie das Travelling Salesman Problem klassische Computer vor große Herausforderungen. Da Qubits in Quantencomputern hingegen mehrere Zustände gleichzeitig annehmen, können diese mehrere Lösungswege gleichzeitig simulieren, bis schlussendlich nur der mit hoher Wahrscheinlichkeit kürzeste Weg als Ergebnis errechnet wird. Diese Fähigkeit lässt sich

auf zahlreiche andere Anwendungsmöglichkeiten mit hoher Komplexität ausweiten, wie zum Beispiel (Infineon, 2021; McArdle et al., 2020; QUTAC et al., 2021):

- Simulation und Entwicklung neuartiger chemischer Verbindungen für Medikamente oder Impfstoffe
- Simulation neuer Materialien für nachhaltige Energieproduktion (wie Solarzellen) oder -speicherung (wie Akkus)
- Verbesserung der Wettervorhersage (wie die Früherkennung von Umweltkatastrophen)
- Entwicklung neuer Möglichkeiten der Kohlenstoff- oder Stickstoffbindung zur Förderung der Landwirtschaft und Bekämpfung des Klimawandels
- Suche nach Gemeinsamkeiten von Daten im Bereich der künstlichen Intelligenz (wie Mustererkennung)
- IT-Sicherheit (wie Quantenkryptographie)

Durch Betrachtung all dieser und noch weitaus mehr Möglichkeiten wird klar, welches Potenzial in Quantencomputern steckt. Gleichzeitig wird ein unangenehmer Nebeneffekt dieses technologischen Fortschritts klar, wenn die Funktionsweise gängiger Verschlüsselungsmechanismen betrachtet wird. Diese beruhen beispielsweise auf der Komplexität, Primfaktoren von großen Zahlen zu errechnen, wobei nahezu unendlich viele Möglichkeiten probiert werden müssten. Wird die Parallelisierung der Rechenoperationen eines Quantencomputers nun für die Berechnung von Primfaktoren eingesetzt, so stellt deren Anwendung eine Bedrohung für heute als sicher geltende Verschlüsselungsverfahren dar (de Wolf, 2017).

3. Informationssicherheitsmanagement

Ein weiteres zentrales Element dieser Arbeit liegt in dem Management von Informationssicherheit. Daher wird in diesem Teil ein grober Überblick über wichtige Ansätze, Standards und Schutzmaßnahmen gegeben und das grundlegende Prinzip von Kryptographie erläutert.

Der Begriff IT-Sicherheit wird häufig synonym mit dem Begriff des Informationssicherheitsmanagements verwendet. Dabei ist allerdings zu unterscheiden, dass das Informationssicherheitsmanagement generell die Sicherheit aller Daten betrachtet, unabhängig deren Art der Speicherung. IT-Sicherheit fokussiert sich hingegen auf alle Daten, die elektronisch verarbeitet werden (Wegener et al., 2016, p. 3). Diese Arbeit befasst sich mit der gesamtheitlichen Informationssicherheit, wenngleich ein Hauptaugenmerk auf elektronische Daten gelegt wird.

3.1 Grundwerte

Als zentrales Element des Informationssicherheitsmanagements werden häufig drei Grundwerte genannt. Aufgrund der Zusammensetzung ihrer Anfangsbuchstaben in englischer Sprache hat sich für die Schutzziele der Begriff der CIA-Triade etabliert, der folgende Punkte umfasst (Wegener et al., 2016, p. 3):

- Das Ziel der **Vertraulichkeit** (*confidentiality*) von Daten soll sicherstellen, dass nur Berechtigte über Zugriff zu Informationen verfügen. In der Praxis wird die Vertraulichkeit mittels Zugriffskontrollen sichergestellt.
- Ein weiteres bedeutendes Schutzziel liegt in der **Integrität** (*integrity*) von Informationen. Sie soll sicherstellen, dass Informationen unversehrt bzw. fehlerfrei bleiben bzw. unbemerkte Veränderungen verhindert bzw. erkannt werden. Häufig wird beim Nachweis der Integrität auf digitale Signaturen zurückgegriffen.
- Letztlich soll im Zuge der **Verfügbarkeit** (*availability*) sichergestellt werden, dass Informationen zum benötigten Zeitpunkt auch verfügbar sind.

Darüber hinaus existieren in der Literatur weitere wichtige Schutzziele, die im Laufe der Zeit als Ergänzung zur CIA-Triade häufig genannt werden (Eckert, 2013, p. 7ff.; Wegener et al., 2016, p. 29f.):

- Die **Nichtabstreitbarkeit** *(non-repudiation)* stellt sicher, dass der Absender einer Nachricht eindeutig identifiziert werden und er diese nicht abstreiten kann. Sie wird meist durch digitale Signaturen ermöglicht.
- Bei der **Authentifizierung** *(authentication)* wird die Identität einer Person überprüft. Diese wird häufig über mehrere Faktoren wie Besitz (wie Zugangskarte), Wissen (wie Passwort) oder „etwas sein" (wie biometrische Daten) sichergestellt.
- Im Zuge der **Autorisierung** *(authorization)* wird der Zugriff auf Objekte definiert und festgelegt, welche Person auf welche Information zugreifen darf. Voraussetzung für eine korrekte Autorisierung liegt in einer korrekten Authentifizierung.

3.2 Bedrohungen

In den letzten Jahren wurden durch Innovationen wie dem technologischen Fortschritt und die zunehmende Vernetzung auch die Bedrohungen für Informationssysteme größer. Nachdem die IT zum Alltag wurde, können Angriffe über verschiedenste Wege eingeleitet werden und durch die ständige Konnektivität sind wir bereits rund um die Uhr angreifbar. Folglich erfordern diese Entwicklungen auch einen weitaus höheren Schutzbedarf. Die Liste der möglichen Bedrohungen ist lang und kann aufgrund der Kreativität der Angreifer niemals als vollständig betrachtet werden. Einige wesentliche Bedrohungen sind beispielsweise (Müller, 2018, p. 1ff.):

- **Computerangriffe** werden mittels Viren, Trojaner, Ransomware, Denial-of-Service, Botnetze, Phishing Angriffe, Brute Force Attacken u.v.m. immer komplexer.
- **Sicherheitslücken** wie Programmier- und Anwendungsfehler, menschliches Versagen oder das Fehlen von Softwareupdates führen zu Datendiebstahl und Datenverlusten.
- **Spionagetätigkeiten** durch beispielsweise Abhören von Internetverbindungen und Knotenpunkte sowie ein aufkeimender **Cyberwar** mit Angriffen auf kritische Infrastruktur nehmen laufend zu.
- Auch **äußere Einwirkungen** wie Strom-, IT- oder Mobilnetzausfälle, bzw. -störungen, Unwetter wie Hochwasser, Erbeben, Sturm oder Epidemien bedrohen die Versorgungssicherheit.

- Und zu guter Letzt tragen **technologische Entwicklungen** wie z.B. Quantencomputer dazu bei, dass völlig neuartige Sicherheitsrisiken betrachtet werden müssen.

3.3 ISO/IEC 27000: Standard für die Informationssicherheit

Aufgrund der Vielzahl an Bedrohungen stellt sich die Frage, wie diesen am besten entgegengewirkt und ein Mindestmaß an Informationssicherheit hergestellt werden kann. Dazu existiert eine Reihe an Informationssicherheitsstandards, wobei im deutschsprachen Raum die **BSI-Standards** (BSI, 2022), des deutschen Bundesamts für Sicherheit in der Informationstechnik hervorzuheben sind sowie die **ISO/IEC 27000-Reihe** (ISO/IEC, 2018a), welche sich zu einem internationalen Informationssicherheitsstandard etabliert hat. Genau wegen dieser internationalen Anerkennung, haben die nachfolgenden Ausführungen zum Informationssicherheitsmanagement einen starken Bezug zur ISO/IEC 27000-Reihe.

3.3.1 ISO/IEC 27001: ISMS

Die ISO/IEC 27001 behandelt dabei Großteils die Anforderungen an das Management der Informationssicherheit, dem Informationssicherheits-managementsystem (kurz ISMS). Folgende wichtigen Aufgaben stehen im Vordergrund (Kersten et al., 2020):

- **Formulierung von Sicherheitszielen**: In dieser zentralen Aufgabe werden häufig die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität und auch weitere Geschäftsziele genannt. Sie werden für gewöhnlich in einer Sicherheitsleitlinie dokumentiert.
- **Bestimmung der Assets**: In diesem Schritt werden alle Vermögenswerte einer Organisation definiert und schließlich in einer Datenbank oder Liste inventarisiert. Dabei werden Angaben zum Speicher/Lager-Ort gemacht und der Verantwortliche (Asset Owner) wird definiert.
- **Risikobeurteilung**: Ereignisse, die eine mögliche Auswirkung auf die Sicherheit des Unternehmens haben können, müssen in laufenden Abständen identifiziert und auf Basis von Schadensausmaß und Eintrittswahrscheinlichkeit in einer Risikomatrix bewertet werden.
- **Risikobehandlung**: Anschließend werden alle Risiken in die Klassen der Risikobehandlung unterteilt:
    - Risikoakzeptanz

- Risikoverlagerung (z.B. Outsourcing oder Versicherung)
- Risikoreduktion (mittels Sicherheitsmaßnahmen)
- Risikovermeidung (durch Änderung des Prozesses)

Für gewöhnlich werden die höchsten Risiken priorisiert und geringe Risiken einfach toleriert.

- **Kontinuierliche Verbesserung**: Zu guter Letzt wird die Organisation dazu veranlasst, laufende Verbesserungen im ISMS vorzunehmen. Hierbei wird häufig nach dem sogenannten Plan-Do-Check-Act (kurz PDCA) Modell vorgegangen. Zuerst wird das ISMS konzipiert (Plan), dann umgesetzt (Do), anschließend kontinuierlich überprüft (Check) und im Zuge der Ergebnisse schlussendlich verbessert (Act).

3.3.2 ISO/IEC 27002: Best Practice & Maßnahmenkatalog

Mit der ISO/IEC 27002 (ISO/IEC, 2018b) bietet die ISO/IEC 27000-Reihe auch einen Best-Practice-Ansatz zur Anwendung der ISO/IEC 27001 mit praktischen Steuerungsmaßnahmen. Sie kann damit gleichzeitig als eine Art Leitfaden und Katalog für Informationssicherheit gesehen werden. Darin enthalten sind insgesamt 18 Bausteine zum Aufbau eines ISMS, wobei 14 davon konkrete Maßnahmen zur Stärkung des internen ISMS enthalten, die sogenannten „control objectives“ (ISO/IEC, 2018c)*:*

- **A.5 Information security policies**: Die Informationssicherheitspolitik beinhaltet alle sicherheitsrelevanten Unternehmensrichtlinien im Hinblick auf die Geschäftsziele, Gesetze und Regulatorien sowie die Kontrollzyklen.
- **A.6 Organization of information security**: In der Sicherheits-organisationsrichtlinie wird das Management der IT-Sicherheit im Unternehmen verankert und geregelt, wie dieses erhalten werden kann. Dazu gehören z.B. Rollentrennung, Kontakte mit Behörden und der Umgang mit mobilen Geräten.
- **A.7 Human resource security**: Viele Sicherheitsrisiken gehen vom Faktor Mensch aus, wie menschliche Fehler, Fehlverhalten oder auch Diebstahl bzw. Betrug. Dieser Baustein beinhaltet Maßnahmen zur Vermeidung dieser Bedrohungen mittels Backgroundchecks, Personalrichtlinien und Disziplinierungsmaßnahmen bis hin zum Offboarding.
- **A.8 Asset management**: Ziel dieses Bausteins ist der Schutz von materiellen und immateriellen Unternehmenswerten. Dazu gehört z.B. die Inventarisierung, die Zuteilung von Verantwortungen, die Klassifizierung von Informationen und der Umgang mit Medien.

- **A.9 Access control**: Der Zugriff zu Informationen des Unternehmens muss ausreichend kontrolliert werden. Dazu gehören Daten, Netzwerke, physische Geräte, Passwortmanagement und die regelmäßige Überprüfung der Rechteverwaltung.
- **A.10 Cryptography**: Dieser Baustein regelt den Umgang, den Lebenszyklus und den Schutz mit kryptographischen Schlüsseln und digitalen Signaturen und sichert damit die Vertraulichkeit, Integrität und Authentizität der Unternehmensdaten.
- **A.11 Physical and environmental security**: Der physische Schutz verhindert unerlaubten Zugang zu Unternehmensgebäuden, Büros, Netzwerken, etc. durch effektive Zugangskontrollen und schützt damit vor Sabotagen, Verlusten oder Diebstahl.
- **A.12 Operations security**: Die Betriebssicherheit sorgt für die ordnungsgemäße Funktionsweise aller benötigten Systeme und regelt die dazugehörigen Prozesse und Verantwortungen. Sie behandelt beispielsweise Backups, Aktivitäten-Logging, Antivirensoftware und weitere Applikationen.
- **A.13 Communications security:** Die Kommunikationssicherheit von Netzwerken und dem internen Informationsfluss schützt die Vertraulichkeit und Integrität von Daten. Beispiel dafür sind Netzwerksicherheit und -segmentierungen sowie ein angemessener Schutz der Informationsübertragung, wie z.B. die Verwendung von VPN-Tunnels.
- **A.14 System acquisition, development and maintenance:** In diesem Abschnitt wird der sichere Softwareentwicklungsprozess geregelt – von Anforderungen, über Entwicklung bis hin zu Tests. Mögliche Maßnahmen in diesem Bereich sind die Anwendung sicherer Entwicklungspraktiken, Qualitätskontrollen und -tests, Outsourcing sowie Schutz dieser Daten.
- **A.15 Supplier relationships:** Werden externe Lieferanten mit Leistungen betraut, so ist dabei besondere Sorgfalt zu wahren. Zu den Schutzmaßnahmen gehören Vereinbarungen zur Informationsübergabe, Service Level Agreements, Geheimhaltungserklärungen oder Beendigungsprozesse.
- **A.16 Information security incident management:** Informations-sicherheitsvorfälle (Incidents) können für Unternehmen existenzbedrohlich sein. Aus diesem Grund muss bei Bekanntwerden schnell gehandelt werden, wie z.B. durch Incident Response Maßnahmen und vordefinierte Managementprozesse. Hierzu zählen auch die Beweissicherung und das Lernen aus solchen Vorfällen.

- **A.17 Information security aspects of business continuity management:** Nach Eintritt eines Incidents muss der Geschäftsbetrieb wieder aufgenommen werden. Wie das geschieht, ist im Business Continuity Management geregelt. Es beinhaltet für gewöhnlich zahlreiche Desaster Recovery Maßnahmen.
- **A.18 Compliance:** Schlussendlich stellt die Compliance sicher, dass im gesamten Unternehmen alle sowie internen als auch externen Gesetze, Regulatorien und Richtlinien eingehalten werden. Dazu zählen auch Maßnahmen zum Schutz intellektuellen Eigentums, der Datenschutz und natürlich regelmäßige Kontrollen der internen Regelungen oder Audits.

Der Vollständigkeit sei noch zu erwähnen, dass die Bausteine A.1 bis A.4 („Scope", „Normative references", „Terms and defitions" und „Structure of this standard") keine Maßnahmen enthalten und daher nicht näher darauf eingegangen wurde (ISO/IEC, 2018b).

Die für diese Arbeit wohl zentralste Maßnahmenkategorie liegt in der Verwendung sicherer und verlässlicher kryptographischer Systeme. Sie sind wie beschrieben ein wesentliches Element in jedem Informationssicherheitsmanagement. Aus diesem Grund werden im kommenden Kapitel grundlegende kryptographische Ansätze näher erläutert.

3.4 Kryptographie

Kryptographie ist aus unserem Alltag kaum wegzudenken, auch wenn sie von Anwendern nur selten wahrgenommen wird. Ohne der Möglichkeit, Nachrichten, Mails, Finanztransaktionen oder ähnliches zu verschlüsseln, wären unsere gesamte digitale Kommunikation rund um die Uhr offen und die Nutzer wären ungeschützt gegen Cyberangriffe (Yunakovsky et al., 2021).

Dieses Problem wird in der Praxis durch kryptographische Verfahren gelöst, die im Wesentlichen in die symmetrische und asymmetrische Kryptographie unterteilt werden können (Mavroeidis et al., 2018).

3.4.1 Symmetrische Kryptographie

Bei der symmetrischen Kryptographie wird der gleiche Schlüssel zur Verschlüsselung und Entschlüsselung einer Information oder Nachricht verwendet. Das bedeutet, dass sowohl Sender als auch Empfänger einer Nachricht den Schlüssel kennen und einen effizienten Weg zum geheimen Austausch dieses Schlüssels finden müssen. Der Austausch einer

Nachricht würde mithilfe der symmetrischen Kryptographie wie folgt aussehen (Thakkar, 2016):

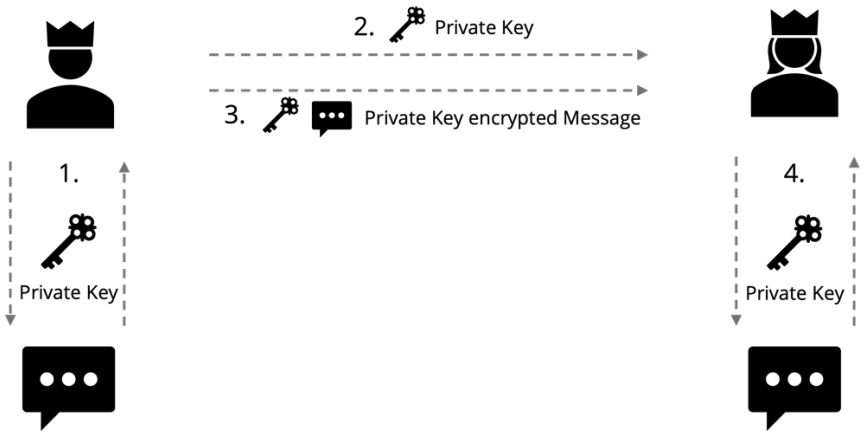

Abbildung 10: Symmetrische Kryptographie (Eigene Darstellung)

Abbildung 10 zeigt die typischen Schritte einer Informationsübertragung mittels symmetrischer Verfahren, die in folgende Schritte gegliedert werden:

1. Bob verschlüsselt eine Nachricht mit ihrem geheimen Schlüssel.
2. Bob übermittelt den geheimen Schlüssel an Alice.
3. Bob übermittelt die verschlüsselte Nachricht an Alice.
4. Alice verwendet den geheimen Schlüssel zur Entschlüsselung der Nachricht.

Das größte Problem bei symmetrischen Verschlüsselungsmethoden liegt in der Schlüsselübertragung: Sobald jemand über den geheimen Schlüssel verfügt, könnte er die Informationen entschlüsseln und somit den Informationsaustausch belauschen (Mavroeidis et al., 2018). Zu den bekanntesten symmetrische Verschlüsselungsmechanismen zählen der Advanced Encyrption Standard (AES), DES, 3DES und BLOWFISH (Sharma and Ketti Ramachandran, 2021).

3.4.2 Asymmetrische Kryptographie

Aufgrund des Problems der Schlüsselübertragung wurde die asymmetrische Kryptographie, auch als **Public Key Kryptographie** bekannt, entwickelt. Bei diesem Verfahren werden Informationen nicht mit dem gleichen Schlüssel ver- und entschlüsselt, sondern ein Schlüsselpaar übernimmt diese Aufgaben. Dabei besitzen Sender und Empfänger jeweils einen geheimen Schlüssel (**Private Key***)* sowie einen daraus errechneten öffentlichen (**Public Key**) (Thakkar, 2016).

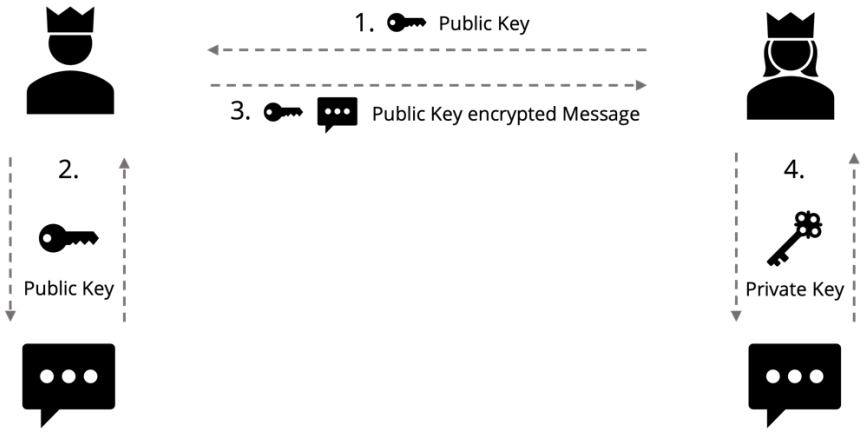

Abbildung 11: Asymmetrische Kryptographie (Eigene Darstellung)

Abbildung 11 zeigt die Informationsübertragung mithilfe von asymmetrischer Kryptographie, die ebenfalls in 4 Schritten geschieht (Thakkar, 2016):

1. Alice übermittelt ihren Public Key an Bob.
2. Bob verschlüsselt die Nachricht mit Alices Public Key.
3. Bob übermittelt die verschlüsselte Nachricht an Alice.
4. Alice entschlüsselt die Nachricht mit ihrem Private Key.

Auf diese Art und Weise kann eine Nachricht sicher übertragen und nur vom Empfänger, der den Private Key besitzt, entschlüsselt werden. Aus diesem Grund eignet sich dieses Verfahren besonders gut für digitale Signaturen. Der große Vorteil der Public Key Kryptographie liegt darin, dass die Ableitung des Public Keys vom Private Key auf komplexen mathematischen Problemen basiert und vom Public Key praktisch nicht auf den Private Key rückgerechnet werden kann (Mavroeidis et al., 2018).

Zu den bekanntesten asymmetrischen Verschlüsselungsmechanismen zählen der RSA, Elliptic Curve Cryptography (ECC), Diffie-Hellman und Algorithmen zur digitalen Signatur (Sharma and Ketti Ramachandran, 2021).

4. Quantencomputer als Bedrohung für die Informationssicherheit?

Wie in den vorherigen Kapiteln bereits beschrieben wurde, sind Quantencomputer klassischen Computern in gewissen Berechnungen theoretisch weit voraus. Dazu gehören auch mathematische Probleme, auf deren Basis die heutige Kryptographie basiert und die mit klassischen Computern der Kategorie der NP-Probleme entsprechen.

4.1 Bedrohungsszenarien für Kryptographie

Schon im vergangenen Jahrhundert wurden Algorithmen entwickelt, die mithilfe eines Quantencomputers zu einem Quantensprung in der IT-Sicherheit führen können (Sharma and Ketti Ramachandran, 2021). Die nächsten beiden Kapitel geben einen kurzen Überblick über deren Funktionsweise.

4.1.1 Shor's Algorithmus

Die Sicherheit klassischer Computersysteme geht zu einem großen Teil auf die Komplexität mathematischer Probleme zurück, die für klassische Rechner praktisch nicht zu lösen sind. Dazu gehören beispielsweise die Faktorisierung von Primzahlen sowie das Problem diskreter Logarithmen. Der Mathematiker *Peter Shor* entwickelte im Jahr 1994 je einen Algorithmus, der durch Zuhilfenahme der Superposition auf einem effizienten Quantencomputer beide Probleme in polynominaler Laufzeit lösen kann. Bei der Berechnung wird nicht sofort das korrekte, konkrete Ergebnis geliefert, sondern der Algorithmus erfordert einige wenige Durchläufe, in denen er jeweils mit hoher Wahrscheinlichkeit das richtige Ergebnis ermittelt (Shor, 1994).

Da das weit verbreitete RSA-Schema auf dem Problem der Fakturierung von Primzahlen basiert und ein Großteil der heute verwendeten asymmetrischen Public Key Verfahren mit dem Problem des diskreten Logarithmus gesichert sind, stellt Shor's Algorithmus eine Bedrohung für die Sicherheit vieler heute verwendeter Computersysteme dar (BSI, 2021b).

4.1.2 Grover's Algorithmus

Etwas später entwickelte *Lov Grover* einen Suchalgorithmus, der die Suche nach einem Element in einer unsortierten Datenbank stark verkürzen kann. Dies geschieht für gewöhnlich über eine Abfragefunktion, die die Datenbank Element für Element

durchsucht und jeweils den Wert korrekt oder falsch zurückgibt. Ist der Wert falsch, wird zum nächsten Element gesprungen. In einer Datenbank mit n Elementen werden bei einer zufälligen Suche im schlechtesten Fall n Versuche benötigt, um das gesuchte Element zu finden. Der Grover Algorithmus hingegen bedient sich der sogenannten Grover-Transformation, bei der die Wahrscheinlichkeitsamplitude so erhöht wird, dass der gesuchte Eintrag mit einer hohen Wahrscheinlichkeit bereits nach $\sqrt{n}$ Schritten gefunden wird. Die Leistungssteigerung des Algorithmus ist dabei zwar nicht exponentiell, aber quadratisch (Grover, 1996).

Die Anwendung des Grover-Algorithmus ist grundsätzlich problematisch, da der Schlüsselraum von symmetrischen Verschlüsselungsalgorithmen mit seiner Hilfe schneller gefunden werden kann. So kann eine Schlüssellänge von 128 Bit durch Anwendung des Grover-Algorithmus theoretisch mit 264 Quantenoperationen geknackt werden. Da aber eine bloße Verdoppelung der Schlüssellänge auf 256 Bits bereits 2128 Quantenoperationen erfordern würde und dies aktuell als unpraktikabel gilt, stellt der Grover-Algorithmus verglichen zum Shor-Algorithmus ein geringeres Risiko für gängige Verschlüsselungsverfahren dar (BSI, 2021b).

4.2 Maßnahmen gegen Quantencomputer

Aufgrund der neuartigen Bedrohung sind Forschung, Regierungen und folglich auch die Wirtschaft gefordert, neuartige kryptographische Ansätze zu finden, die auch Angriffen durch Quantencomputer standhalten und gleichzeitig aktuelle Sicherheitsstandards erfüllen.

4.2.1 Quantenkryptographie

Die Disziplin der Quantenkryptographie geht im Wesentlichen auf *Bennett und Brassard* zurück, die im Jahr 1984 das nach ihnen benannte BB84 Protokoll entwickelten. Das Verfahren der **Quantum Key Distribution** (QKD) wurde entwickelt, um einen kryptographischen Schlüssel über einen unsicheren Informationskanal zwischen 2 Parteien zu übermitteln. Dabei bedient sich das Verfahren direkt quantenmechanischen Zuständen und ist somit im Wesentlichen auch sicher gegenüber Angriffen mit Quantencomputern (Bennett and Brassard, 1984).

Seither wurden viele weitere Protokolle entwickelt, die den Austausch von Informationen im Zeitalter vom Quantencomputern sichern sollen. Dabei bedienen sich sogenannte „Prepare-and-measure Protokolle“ der Heisenberg‘schen Unschärferelation, wonach die

Beobachtung des Quantenzustands zum Verlust dieses Zustands führt. „Entanglement-based Protokolle“ hingegen bedienen sich zweier verschränkter Partikel. Wird eines davon manipuliert, so ändert sich auch das andere verschränkte Teilchen. Da bei beiden Protokollen ein Lauschangriff einen Einfluss auf die Informationsübertragung der beiden Parteien hat, wird ein Angreifer schnell erkannt und kann mit den abgefangenen Informationen nichts anfangen (Mavroeidis et al., 2018).

4.2.1.1 BB84-Protokoll

Beim BB84-Protokoll wird durch die Polarisierung von Licht eine zufällige Anzahl an Qubits übertragen. Dabei werden jeweils eine horizontale und eine vertikale Basis verwendet. Bei der horizontalen Basis resultiert eine Polarisierung von 0° in einem Wert des Qubits von 0 und eine Polarisierung von 90° den Wert 1. Bei der vertikalen Basis entspricht eine Polarisierung von 45° dem Wert 0 und 135° dem Wert 1. Der Prozess folgt dabei dem Ablauf (Bennett and Brassard, 1984):

1. Alice sendet eine Sequenz von Photonen an Bob, die ausreicht, um einen Schlüssel zu generieren. Sowohl die Basis als auch die Polarisierung der Photonen erfolgt zufällig.
2. Bob wählt für jedes Photon eine geheime und zufällige Basis, mit der er die empfangenen Photonen misst.
3. Bob teilt Alice anschließend mit, welche Basis er für welches Photon gewählt hat.
4. Alice beantwortet Bob nur, ob die jeweilige Basis korrekt oder falsch war.
5. War die Basis korrekt, so wurde ein korrektes Bit übertragen. War die Basis falsch, so wird dieses Photon verworfen.
6. Alle korrekten Bits sind nun beiden Seiten bekannt und können als Schlüssel für die Nachricht verwendet werden.
7. Alice kodiert also die Nachricht mit dem Schlüssel und überträgt diese an Bob.
8. Bob entschlüsselt die Nachricht von Alice.

Insgesamt existieren somit folgende Möglichkeiten, wie die Übertragung der Photonen gesendet und gemessen werden kann:

Alices Photon	Bobs Basis	Bobs Messung	Bobs Ergebnis	Korrektheit	Schlüssel
↔	+	↔	0	✓	0
↔	×	⤢,⤡	0,1	✗	-
↕	+	↕	1	✓	1
↕	×	⤢,⤡	0,1	✗	-
⤢	+	↔,↕	0,1	✗	-
⤢	×	⤢	1	✓	1
⤡	+	↔,↕	0,1	✗	-
⤡	×	⤡	0	✓	0

Tabelle 2: Möglichkeiten BB84 (Eigene Darstellung)

Das für den Schlüsselaustausch selbst verwendete BB84-Protokoll wird zwar als sicher angesehen (Mavroeidis et al., 2018), dennoch hat sich die für die Kommunikation verwendete Hardware auch mit Erweiterungen noch als unsicher z.B. gegen „Blinding Attacks“ herausgestellt (Lydersen et al., 2010).

4.2.1.2 Weitere Protokolle

Insgesamt existieren vielzählige Weiterentwicklungen des BB84-Protokolls wie auch Varianten, die eine andere Art der Messung verwenden (Mavroeidis et al., 2018).

Das **B92-Protokoll** stellt eine Vereinfachung von *Bennett* gegenüber dem BB84-Protokoll dar. Der Unterschied liegt darin, dass nur die beiden Zustände 0° (Wert = 0) und 45° (Wert = 1) existieren. Ansonsten ist der Prozess dem des BB84-Protokolls sehr ähnlich (Bennett, 1992).

Bei dem **E91-Protokoll** oder auch *Ekert Encoding Scheme* wird die Verschränkung der Teilchen zur Messung herangezogen. Dabei wurde ebenfalls das BB84-Protokoll als Basis genommen und um den Effekt der Quantenverschränkung ergänzt, indem ein Photon mithilfe eines Lasers gesplittet wird und eines dieser beiden Photonen an den Empfänger gesendet wird. Wird dieses Photon beispielsweise beobachtet, so hat das einen direkten Einfluss auf das andere Photon (Ekert, 1991).

Ebenfalls eine Abwandlung des BB84-Protokolls stellt das **SARG04-Protokoll** dar. Es verwendet ebenfalls die vier Varianten der Phontonen bei der Codierung. Doch im Gegensatz zu BB84 nicht die Polarisierung, sondern die Basis zur Codierung der Nachricht verwendet. Dadurch ist SARG04 weniger anfällig gegen Photon Number Splitting Angriffe (Scarani et al., 2004).

Darüber hinaus existieren viele weitere Ansätze, die entweder ebenfalls Ähnlichkeiten mit den beschriebenen Modellen aufweisen oder deren praktischer Einsatz sich als weniger praktikabel darstellt (Mavroeidis et al., 2018; Sharma and Ketti Ramachandran, 2021). Generell ist die Disziplin der Quantenkryptographie noch unzureichend erforscht und ein Einsatz auf breiter Basis wird noch dauern (BSI, 2021b).

4.2.2 Post-Quanten-Kryptographie

Nachdem die NSA (National Security Agency, USA) im Jahr 2015 eine offizielle Warnung zum Sicherheitsrisiko durch Quantencomputer aussprach, wurde von dem *NIST* 2016 ein Standardisierungsverfahren für quantensichere Verschlüsselungstechnologien ins Leben gerufen. Bereits in der Vergangenheit haben ähnliche Ausschreibungen vom *NIST* zur Entwicklung der weit verbreiteten Algorithmen AES oder SHA-3 geführt (BSI, 2021b; Chen et al., 2016).

Wie der Name schon sagt, handelt es sich bei Post-Quanten-Kryptographie um kryptographische Verfahren, die auf komplexen mathematischen Problemen basieren und durch Quantencomputer nicht gebrochen werden können. Dabei haben sich aktuell fünf Forschungsrichtungen entwickelt (BSI, 2021b):

- **Codebasierte Verfahren** (Code-based cryptography) basieren auf der Komplexität, Fehlerkorrekturcodes zu dekodieren. Fehlerkorrekturcodes ermöglichen generell, Fehler in codierten Daten zu vermeiden. Eine der einfachsten Möglichkeiten ist die einfache Wiederholung von Bits: Die Sequenz 000 stellt in diesem Fall den Wert 0 dar. Passiert ein Bit-Flip, so kann in der Codierung 010 immer noch erkannt werden, dass der Wert 0 korrekt ist. Dabei wird das allgemeine Dekodierungsproblem zur Hilfe genommen, in dem eine Nachricht mittels unstrukturierten Codes decodiert wird und als NP-hard gilt.
- Bei **gatterbasierten Verfahren** (Lattice-based cryptography) wird die Schwierigkeit von Berechnungsproblemen in mathematischen Gattern als Basis genommen. Dabei sind mathematische Gatter als n-dimensionaler Vektorraum zu verstehen. Ein schwieriges Berechnungsproblem stellt das Problem des kürzesten Vektors dar, in dem der kürzeste Vektor in einem mehrdimensionalen Raum gefunden werden muss. Es existieren weder klassische noch Quantenalgorithmen, die dieses Problem in effizienter Zeit lösen können.
- **Hashbasierte Verfahren** (Hash-based cryptography) beruhen auf der Sicherheit von Hashfunktionen. Diese sind im Grunde Komprimierungsfunktionen, die aus

einem Input mittels kryptographischer Funktion einen Hashwert generieren. Diese Funktion kann nicht revidiert werden und es ist praktisch nicht möglich, dass entweder zwei unterschiedlich Inputs den gleichen Hashwert ergeben oder ein Input mehrere verschiedene Hashwerte generiert.

- Die Sicherheit von **isogeniebasierten Verfahren** (Isogeny-based cryptography) beruht auf der Schwierigkeit, eine Isogenie zwischen zwei super-singulären elliptischen Kurven zu finden.
- Schlussendlich basiert die Sicherheit der **multivariaten Kryptographie** (Multivariate cryptography) auf dem Problem, multivariate polynominale Systeme von Gleichungen über endliche Felder zu lösen.

Im Juli 2022 wurde die dritte Runde des Standardisierungsverfahrens am *NIST* beendet und bereits erste Algorithmen zur Standardisierung vorgeschlagen. Dabei evaluierte das NIST alle aus den vorigen Runden übrig gebliebenen Kandidaten anhand der Kriterien Sicherheit, Kosten bzw. Performance und Implementierungscharakteristiken. Da das NIST auf der Suche nach langfristigen Lösungen in den Bereichen von Public Key Verfahren und digitalen Signaturen ist, ist das gesamte Standardisierungsverfahren in die beiden Kategorien **Public Key Encryption** und **Digital Signatures** unterteilt (Moody, 2022).

4.2.2.1 Public Key Encryption

In der Kategorie Public Key Encryption wurde der gatterbasierte *CRYSTALS-Kyber* (Bos et al., 2018) Algorithmus vom *NIST* zur Standardisierung vorgeschlagen. Das Verfahren basiert auf dem Gatterproblem „Lernen mit Fehlern“ und weist signifikante Effizienzvorteile gegenüber anderen Verfahren auf. Zusätzlich überzeugte die jahrzehntelang erforschte theoretische Sicherheitsgrundlage von gatterbasierten kryptographischen Verfahren. CRYSTALS-Kyber setzte sich dabei gegen die Verfahren *NTRU* und *Saber* durch, die ebenfalls auf Gattern basieren und nicht in die vierte Runde mit aufgenommen werden (Moody, 2022).

Grund dafür liegt darin, dass das NIST auch einen codebasierten Algorithmus als alternativen Standard anbieten möchte. Zu diesen Verfahren gehören *BIKE* (Misoczki et al., 2013), *Classic McEliece* (McEliece, 1978), *HQC* (Aragon et al., 2020) und *Sike* (Jao and De Feo, 2011). Sie alle werden in einer vierten Runde weiteren Tests unterzogen, ehe sich das *NIST* für die Standardisierung eines oder mehrerer dieser Verfahren entscheidet (Moody, 2022). Allerdings gilt die Standardisierung des *Sike*-Algorithmus mittlerweile als

unwahrscheinlich, nachdem dieser im August 2022 von einem 10 Jahre alten Computer gehackt wurde (Choi, 2022).

4.2.2.2 Digital Signatures

In der Kategorie der Signaturen wurden gleich drei Verfahren standardisiert (Moody, 2022):

- *CRYSTALS-Dilithium* ist ein gatterbasierter Signaturalgorithmus, der durch seine hohe Effizienz, eine starke theoretische Sicherheit, einer einfachen Implementierung sowie einer guten kryptoanalytischen Vergangenheit überzeugte. Aufgrund der breiten Einsetzbarkeit wird dieser Algorithmus als primäres Signaturverfahren vom NIST standardisiert (Ducas et al., 2018).
- Ebenso liegt dem *FALCON* Verfahren ein gatterbasierter Ansatz, verbunden mit dem hash-and-sign Paradigma, zugrunde. Das NIST wählte FALCON aufgrund der hohen Sicherheit und der geringen benötigten Bandbreite aus. Nichtsdestotrotz ist der FALCON Algorithmus schwierig zu implementieren und das NIST empfiehlt weitere Forschung in Best Practices, wie FALCON am besten zu implementieren ist (Fouque, Pierre-Alain et al., 2020).
- Zu guter Letzt wurde mit *SPHINCS+* ein hash-basiertes Signaturverfahren standardisiert, welches verschiedene Signaturen, Merkle Trees, Hypertrees u.v.m. vereint. Zwar könnten theoretisch aufgrund der hohen Komplexität und der vielzähligen verwendeten Verfahren bei der Implementierung Sicherheitsprobleme auftreten, dennoch wurde das Signaturverfahren als sehr solide angesehen. Ein wichtiger Grund für die Standardisierung lag darin, dass sich das Signaturverfahren auch grundlegend von allen anderen vom NIST standardisierten Verfahren unterscheidet (Bernstein et al., 2019).

4.2.2.3 Weitere Standardisierungsbestrebungen

Auch wenn sich das *NIST* bei einigen Verfahren für eine Standardisierung entschloss, werden in der vierten Runde weitere Verfahren weiteren Tests unterzogen (Moody, 2022). Darüber hinaus hat das NIST einen weiteren Call for Proposals ausgeschrieben, zu dem neue Ansätze eingereicht werden können. Grund dafür liegt darin, dass bis auf SPHINCS+ alle Algorithmen auf dem gatterbasierten Ansätzen beruhen und das *NIST* eine breitere Palette an Verfahren standardisieren möchte (NIST, 2022).

Schlussendlich bleibt noch anzumerken, dass auch die „Chinese Association for Cryptologic Research“ (CAGR) sowie das „Russian Technical Committee for Standardisation“ von ROSSTANDARD an der Standardisierung arbeiten. Das deutsche BSI orientiert sich dabei stark an den Ergebnissen des NIST und wird keine eigene und auch keine europäische Standardisierung forcieren, da aus dessen Sicht ein gemeinsamer internationaler Standard vom NIST die generelle Interoperabilität fördert (BSI, 2021b).

4.2.3 Migration der Kryptographie als Zeitfrage

Nach einer Studie des *BSI* benötigt ein voll funktionsfähiger Quantencomputer (mit einer Fehlerrate von 1:10.000) zum Entschlüsseln des 2048-Bit RSA rund 100 Tage mit ca. einer Million Qubits und nur eine Stunde mit ca. einer Milliarde Qubits. Angesichts des in Kapitel 2.4 beschriebenen technologischen Entwicklungsstands könnte die Gefahr schnell vernachlässigt werden, da Quantencomputer aktuell nicht mehr als 50 bis 5000 (fehlerhafte) Qubits aufweisen. Allerdings ist gerade durch hohe Forschungsetats vieler führender Technologieunternehmen und die Förderung durch US-Militär und Heimatschutzministerium mit einer beschleunigten Entwicklung in den nächsten Jahren zu rechnen (BSI, 2020). Verschiedene Studien schätzen, dass irgendwann in den nächsten fünf bis 15 Jahren der Zeitpunkt erreicht sein wird, an dem fehlerkorrigierte, leistungsstarke Quantencomputer Realität werden und ein beachtliches Sicherheitsrisiko darstellen (Kießling, 2021; KPMG, 2019).

Dazu gilt es zu beachten, dass auch die Implementierung von Post-Quanten-Kryptographie eine gewisse Zeit benötigen wird. Daher muss diese Implementierungsdauer bereits jetzt bei allen Überlegungen zur Rüstung gegen Quantencomputer miteinkalkuliert werden (BSI, 2021b). So besagt *Mosca's Theorem*, dass die Zeit, die gewissen Daten geschützt werden müssen (X) und die Dauer der Implementierung (Y) und nicht länger sein darf als die restliche Zeitspanne bis zu dem Punkt, an dem Quantencomputer gängige Kryptographie knacken können (Z).

Andernfalls ist das System angreifbar und die Vertraulichkeit der Daten kann nicht mehr gewährleistet werden (Mosca, 2018).

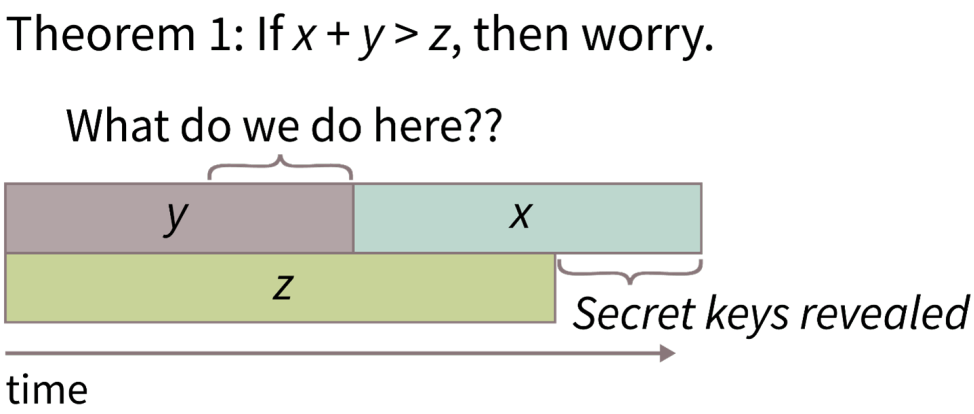

Abbildung 12: Mosca's Theorem (Poeppelmann, 2021)

Ebenso in *Mosca's Theorem* behandelt wird das große Sicherheitsrisiko des *Store- now-decrypt-later* Angriffs. Dieser beruht auf der Annahme, dass Angreifer bereits jetzt im großen Stil verschlüsselte Daten der Opfer abfangen und speichern. Dabei spekulieren sie darauf, dass sie eines Tages in der Lage sein werden, die gesammelten Daten mit der Hilfe von Quantencomputern zu entschlüsseln. Dieser Angriff stellt daher ein großes Risiko für Daten dar, die sensibel sind und für lange Zeit geheim gehalten werden müssen, wie beispielsweise wirtschaftliche oder politische Geheimnisse, Patente, Gesundheitsdaten u.v.m. (Yunakovsky et al., 2021).

4.2.4 Handlungsempfehlungen und Umsetzung

Somit stellt sich schlussendlich noch die Frage, wie Public Key Infrastrukturen und Digitale Signaturen für das Zeitalter von Quantencomputern umgerüstet werden können. In Kapitel 4.2.2. wurde dazu erläutert, welche kryptographischen Verfahren bereits am NIST standardisiert wurden und welche in einer vierten Runde noch weiter analysiert werden. Doch durch die bloße Empfehlung geeigneter quantensicherer Algorithmen ist noch keine Gefahr gebannt, schließlich steht deren Implementierung noch in Milliarden von Geräten bevor (Joseph et al., 2022). Dieser Prozess wird Organisationen noch vor wesentliche Herausforderungen hinsichtlich Kosten, Ressourcen und neuen Sicherheitsrisiken stellen. Das *BSI* empfiehlt dazu eine Reihe von Handlungen, mit denen sich Organisationen bereits jetzt rüsten können (BSI, 2021b), (BSI, 2020):

- **Vorbereitung**: Zuerst sollte ein Migrationsplan erstellt werden, der eine Inventarisierung der verwendeten kryptographischen Verfahren und der verschlüsselten Daten enthält.

- **Kryptoagilität**: Werden kryptographische Algorithmen durch neue Entwicklungen als nicht mehr sicher angesehen, so sollten sie schnellstmöglich durch sichere Varianten ausgetauscht und neue Standards schnell adaptiert werden können. Diese Agilität sollte über die gesamte Lebenszeit von Produkten garantiert werden.
- **Kurzfristige Schutzmaßnahmen**: Es ist auch möglich, zusätzliche symmetrische Schlüssel als Basis zur die asymmetrischen Schlüsselgenerierung hinzuzuziehen. Dabei stellt sich allerdings die Frage nach dem sicheren Transfer.
- **Hybride Lösungen**: Die vom NIST zur Standardisierung vorgeschlagenen Post-Quanten-Kryptographie sind noch nicht so gut erforscht wie beispielsweise RSA oder ECC und sind daher möglicherweise anfälliger auf Side-Channel Attacken oder Implementierungsfehler. Daher sollten diese Algorithmen nur als Hybridlösungen mit bereits erprobten, nicht-quantensicheren Verfahren verwendet werden. Das Gleiche gilt für Signaturverfahren, wobei hier vonseiten des BSI die Verwendung der Verfahren CRYSTALS-Dilithium und FALCON empfohlen wird.
- **Hash-basierte Signaturverfahren**: Zur Signatur von Firmware-Updates könnten sich Hash-basierte Verfahren eignen. Zwar sind sie von der Anzahl der möglichen Signaturen limitiert, allerdings werden in diesem speziellen Fall auch nur wenige benötigt. Zusätzlich leisten sie einen wichtigen Beitrag zur Förderung von Kryptoagilität.
- **Kryptographische Protokolle**: Da die Ergänzung von Post-Quanten-Kryptographie die Funktionsweise klassischer Protokolle verändert, sind auch Adaptierungen an diesen Protokollen selbst nötig.
- **Quantenkryptographie**: Eine weitere Maßnahme könnte darin liegen, einen sicheren AES-256 Schlüssel über Quantenschlüsselaustausch (siehe Kapitel 4.2.1) zu übertragen. Allerdings wird dies nur in Kombination mit einer hybriden Lösung aus klassischen und Post-Quanten-Verfahren empfohlen, da diese Methode noch zu wenig erprobt ist und noch keine zertifizierten Produkte existieren.
- **Weitere Forschung**: Zu guter Letzt empfiehlt das BSI, weitere Forschung zu betreiben. Dies ist darin begründet, dass nicht nur der der Fortschritt der Entwicklung von Quantencomputern einen Einfluss auf die Sicherheit von Public Key Infrastrukturen hat, sondern auch die Entwicklung neuer Algorithmen. Zudem wurden die Post-Quanten-Verfahren noch kaum auf bekannte Probleme wie Side-Channel Angriffe oder Implementierungsfehler untersucht.

Schlussendlich gehört auch der Methode des Quantenschlüsselaustauschs weitere Aufmerksamkeit gewidmet.

Während am *NIST* noch an einem Migrationsfahrplan gearbeitet wird (Barker et al., 2021), hat das *ETSI* bereits einen erarbeitet, der eine detaillierte Vorgehensweise zur Umsetzung dieser Maßnahmen bietet. Im Folgenden werden die drei darin beschriebenen Phasen kurz erläutert (ETSI, 2020):

1. **Bestandsaufnahme**: Zu Beginn muss überhaupt erst identifiziert werden, in welchen Bereichen in einer Organisation kryptographische Verfahren eingesetzt werden. Um keine Angriffspunkte offen zu lassen, sollten daher alle Anwendungsfälle inventarisiert werden, was sehr aufwändig und schwierig ist.
2. **Migrationsplan**: Auf Basis der Inventarliste wird nun entschieden, ob die Migration eines Gerätes durchgeführt oder ein Austausch erfolgen soll. Da in einer Organisation meistens Abhängigkeiten zwischen den Applikationen oder Maschinen bestehen, ist hier auch eine Abfolge und die Abschätzung von Konsequenzen durch den Austausch zu berücksichtigen. Dazu gehören z.B. Stillstände der Produktion.
3. **Umsetzung**: Zu guter Letzt wird die Migration durchgeführt. Dabei sollten Deadlines eingehalten werden und Metriken zur Erfolgsmessung laufend überprüft werden. Dabei muss ständig auf Fehler getestet werden, die die Funktion der jeweiligen Elemente stören könnten. Es ist also ein hohes Augenmerk darauf zu legen, dass die Wertschöpfungskette auch nach Migration noch voll funktionsfähig ist und das gesamte Inventar umgestellt wird.

Im Anhang der Empfehlungen findet sich zusätzlich eine nützliche Checkliste, anhand derer viele wichtige Schritte der Migration strukturiert geplant und umgesetzt werden können (ETSI, 2020).

5. Qualitative Forschung & Inhaltsanalyse

Auf Basis des bereits erarbeiten Theorieteils dieser Arbeit wurden qualitative Expert_inneninterviews durchgeführt und in den nächsten Abschnitten eine qualitative Inhaltsanalyse nach *Mayring* (Mayring, 2015) unterzogen. Nachfolgend werden die in dieser Methodik beinhalteten Schritte kurz beschrieben, bevor abschließend die Ergebnisse der Interviews zusammengefasst bzw. diskutiert werden und eine Conclusio daraus gebildet wird. Die übergeordnete Zielsetzung der Expert_innennterviews liegt darin, mithilfe qualitativer Forschungsmethoden Antworten auf die in Kapitel 1.3 definierten Forschungsfragen zu finden.

5.1 Bestimmung des Ausgangsmaterials

Zu Beginn der Inhaltsanalyse ist es notwendig, das benötigte Ausgangsmaterial festzulegen. Dazu wurden im Zuge dieser Masterthesis im Studiengang Wirtschaftsinformatik fünf Interviews mit Expert_innen aus verschiedenen Branchen durchgeführt, um die Auswirkungen von Quantencomputern auf die Informationssicherheit der Zukunft zu erforschen. Dabei wurden auf Basis der Literaturrecherche Inhalte wie aktuelle Sicherheitsmaßnahmen gegen Cyberangriffe, die Entwicklung von Quantencomputern, aktuelle Adaptionsbemühungen, Post-Quanten-Kryptographie und die damit verbundenen Standardisierungsverfahren, Implementierungsdauer sowie Store-now-decrypt-later Angriffe abgefragt. Die Bestimmung des Ausgangsmaterials gliedert sich nach *Mayring* in die Schritte Festlegung des Materials, die Analyse der Entstehungssituation und abschließend der formalen Charakteristika des Materials (Mayring, 2015, p. 54 ff.).

5.1.1 Festlegung des Materials

Wie eingangs erwähnt, wurden in dieser Arbeit Interviews mit insgesamt fünf Expert_innen aus den Bereichen Informationssicherheit & Risikomanagement durchgeführt. Der Kontakt zu den Expert_innen wurde über das eigene Netzwerk und weitere persönliche Kontakte der Interviewpartner_innen hergestellt. Generell wurden die Interviewpartner_innen unter der Voraussetzung ausgewählt, dass sie auch an einer hierarchischen Position angesiedelt sind, in der sie für diese Vorgänge Verantwortung tragen und über Entscheidungsbefugnisse verfügen.

Da die Arbeit einen Aufschluss über das Bewusstsein österreichischer Unternehmen hinsichtlich des IT-Sicherheitsrisikos durch Quantencomputer geben soll, wurde ein Querschnitt aus verschiedenen Branchen gewählt. Sowohl die Person als auch das Unternehmen wurden anonymisiert, die Position der Person im Unternehmen soll jedoch aus Transparenzgründen bekannt sein. Somit sieht die Zusammenstellung der Interviewpartner_innen wie folgt aus:

Interviewpartner_in	Branche	Position
1L	KMU	CISO
2K	Beratung und Wirtschafts-prüfung	Partner/Geschäftsführer
3H	Industrie	IT-Security Manager
4P	Kritische Infrastruktur	Leiter IT
5W	Beratung und Wirtschafts-prüfung	Geschäftsführer & Auditor

Tabelle 3: Überblick Interviewteilnehmer_innen (Eigene Darstellung)

Anfänglich wurden sieben Interviews geplant, wobei noch weitere Branchen wie Politik, Versicherung oder Bank angedacht waren. Da bereits nach vier Interviews keine wesentlichen neuen Erkenntnisse mehr gezogen wurden, wurde als fünfte Person noch eine weitere Person aus dem Beratungsumfeld hinzugezogen, da diese Personen meist über einen tiefen Blick in verschiedene Unternehmen verfügen. Da sich auch nach diesem Interview keine weiteren Erkenntnisse mehr ziehen ließen, wurde mit fünf Expert_innen eine ausreichende Sättigung erreicht und mit einem Probedurchlauf der Auswertung der Interviews begonnen. Dieser ergab, dass mit dem vorliegenden Material bereits alle Forschungsfragen beantwortet werden konnten und somit keine weiteren Interviews benötigt wurden.

5.1.2 Analyse der Entstehungssituation

Die Interviews wurden gänzlich online via Microsoft Teams Meetings durchgeführt. Es wurden jeder Expert_in die gleichen Fragen gestellt, sodass eine Vergleichbarkeit der Inhalte in der weiteren Auswertung gegeben ist. Der Interviewer behielt sich zudem vor, gewisse Rückfragen zu stellen, um bei schwammigen Auskünften dennoch aussagekräftige Aussagen zu erzielen.

5.1.3 Formale Charakteristika des Materials

Die Interviews wurden mithilfe MS Teams auf dem Notebook des Interviewers aufgenommen. Alle Teilnehmer wurden vorab auf die Aufnahme, Transkription sowie die Anonymisierung der Interviews hingewiesen. Anschließend wurde zur Transkription der Interviews auf die Transkriptionsfunktion von Microsoft Teams zurückgegriffen, die bei der Verschriftlichung unterstützte. Dem folgten je Interview drei Qualitätssicherungszyklen, in denen Interpretationsfehler der Software ausgebessert wurden.

Dabei wurde wie von *Mayring* (Mayring, 2015, p. 57) empfohlen eine vollständige und wörtliche Transkription durchgeführt, lediglich auf Füllwörter wie „äh“ wurde verzichtet, Auffälligkeiten wie Lachen oder Räuspern werden in Klammern gesetzt und Dialektfärbungen wurden eingedeutscht. Eine Frage des Interviewers wurde immer durch das Symbol „F“ und einen nachfolgenden Doppelpunkt dargestellt, die Antworten mit dem Symbol „E“.

5.2 Fragestellung der Analyse

In den beiden nachfolgenden Kapiteln werden die Aussagen bestimmt, die auf Basis des Ausgangsmaterials interpretiert werden sollen. Um eine qualitative Inhaltsanalyse durchzuführen, muss die Fragestellung der Interpretation festgelegt werden. Dazu wird nun zuerst die Richtung der Analyse festgelegt und anschließend eine theoriegeleitete Differenzierung der Fragestellung durchgeführt.

5.2.1 Richtung der Analyse

Zur Strukturierung der Interviews wurde ein Interviewleitfaden erstellt, durch den ein roter Faden gezogen wurde. Zu Beginn wurde sehr allgemein in das Themengebiet Informationssicherheit eingestiegen und von Frage zu Frage tiefer in die Bedrohungen

durch Quantencomputer eingetaucht. Zur zielgerichteten Beantwortung der Forschungsfragen wurden in jedem Interview die gleichen Fragen gestellt. Auf Basis der in Kapitel 1.3 erarbeiteten Forschungsfrage und Subfragen umfasst der Interviewleitfaden folgende Themenbereiche:

- Einstiegsfrage zum Tätigkeitsfeld und zur Erfahrung
- Allgemeine Einschätzung hinsichtlich Bedrohungen der Informations-sicherheit in den nächsten Jahren
- Stellenwert von Informationssicherheit im Unternehmen
- Verwendete kryptographische Verfahren im Unternehmen
- Wissensstand zu Quantencomputern
- Auswirkungen von Quantencomputern auf die Informationssicherheit
- Einschätzung der technologischen Entwicklung von Quantencomputern in den nächsten Jahren
- Vorbereitungsmaßnahmen für das Post-Quanten-Zeitalter
- Adaptierungsfähigkeit der Unternehmen zur Umstellung auf Post-Quanten-Kryptographie
- Risikoeinschätzung hinsichtlich Store-now-decrypt-later Angriffe
- Offene Frage mit Raum für sonstiges Feedback

5.2.2 Theoriegeleitete Differenzierung der Fragestellung

Die Transkription der Expert_inneneinschätzungen beinhaltet insgesamt fünf Personen aus verschiedenen Bereichen. Auf Basis der eben angeführten, im Theorieteil ausgearbeiteten Themenbereiche wurde anschließend eine Analyse durchgeführt, in der Übereinstimmungen und Unterschiede der Interviewteilnehmer_innen herausgearbeitet wurden.

5.3 Technik der qualitativen Inhaltsanalyse: Zusammenfassung

Im Zuge der qualitativen Inhaltsanalyse nach *Mayring* kann grundsätzlich zwischen drei verschiedenen Techniken unterschieden werden. Dabei handelt es sich um die Explikation, die Strukturierung und die Zusammenfassung (Mayring, 2015, p. 67). Auf Basis der Forschungsfrage und der theoretischen Grundlage wird die Technik der Zusammenfassung verwendet, um die qualitativen Expert_inneninterviews auf einen gemeinsamen Nenner zu bringen und die Gemeinsamkeiten sowie Gegensätze der Gespräche zu analysieren.

Dabei wurden vorab auf Basis der Interviewfragen folgende Kategorien gebildet, in die die Aussagen der Expert_innen eingeordnet und anschließend weiterverarbeitet wurden:

Kategorie	Inhalt
1B	Bedrohung durch Cyberangriffe in nächsten Jahren
2I	Stellenwert von Informationssicherheit in Unternehmen
3K	Einsatz von Kryptographie
4Q	Bedrohungen durch Quantencomputer
5M	Maßnahmen gegen die Bedrohung durch Quantencomputer
6I	Geschätzte Implementierungsdauer von Maßnahmen
7S	Risikoeinschätzung von Store-now-decrypt-later Angriffen

Tabelle 4: Kategorien der Inhaltsanalyse (Eigene Darstellung)

Sämtliche Fragen zur Person (Tätigkeitsfeld, Erfahrung & Kenntnisse zu Quantencomputern) sowie die offene Frage am Ende des Interviews wurden nicht in die Inhaltsanalyse übernommen, da diese nur Randinformationen zum eigentlichen Themengebiet darstellen. Die beiden Fragestellungen zum Kenntnisstand zu Quantencomputer und der jeweiligen Einschätzung der Bedrohung wurde im Kapitel 4Q zusammengefasst, da einige Teilnehmer_innen bereits vorgriffen.

Bei der Auswertung wurden in einem ersten Schritt alle Interviewprotokolle gedruckt, analysiert und mit Kommentaren bzw. Notizen versehen. Anschließend wurden die Inhalte der Interviews in eine neu erstellte Microsoft Excel Liste übertragen und mit der Paraphrasierung begonnen. Anschließend wurden alle Paraphrasen generalisiert. Abschließend wurde eine Reduktion unter Zuhilfenahme der Interpretationsregeln von *Mayring* durchgeführt (Mayring, 2015, p. 70 ff.). Um auch sichergehen zu können, dass die Ausarbeitungen dem Ausgangsmaterial entsprechen, wurden die Paraphrasierung und Generalisierung mehreren Iterationen unterzogen.

Die Reduktion wurde schließlich mit dem anonymisierten Kürzel der Interviewpartner_in und der jeweiligen Kategorie codiert. Das Ergebnis der Interviewpartner_in 1L zur Kategorie 1B wurde somit unter dem Kürzel 1L1B zusammengefasst, wie in den Tabellen 5 und 6 zu erkennen ist.

Fall	Kat.	Nr.	Paraphrasierung	Generalisierung	Reduktion
1L	1B	1	Die Bedrohung durch Cyber Angriffe in den nächsten Jahren wird sehr hoch eingeschätzt.	Die Bedrohung steigt.	1L1B Bedrohung steigt: - Telefonnummern und Mails werden gefälscht - Credentials tauchen im Darknet auf - Angriffe wirden professioneller und organisierter - Wird nicht zurückgehen
1L	1B	2	Wir sehen dass Telefonnummern gefälscht werden damit bei uns angerufen wird.	Telefonnummern werden gefälscht	
1L	1B	3	Wir sehen auch, dass Partner, Kunden und Lieferanten gefälschte Mails von uns bekommen.	Partner bekommen gefälschte Mails	
1L	1B	4	Wir sehen auch, dass Credentials von uns im Darknet auftauchen.	Credentials tauchen im Darknet auf	
1L	1B	5	Ich glaube generell, dass die Angriffe professioneller und organisierter werden. Das Niveau wird noch steigen.	Angriffe werden professioneller und organisierter. Niveau steigt	
1L	1B	6	Ich glaube nicht, dass das irgendwann wieder normal wird. Das ist eher das neue normal.	Wird nicht wieder normal	
1L	1B	7	Wir werden uns daran gwöhnen müssen, dass wir alle 3 Monate wo lesen, dass eine größere Firma gehackt wurde.	~~Alle 3 Monate wird große Firma gehackt~~	

Tabelle 5: Auszug der Reduktion (Eigene Darstellung, siehe Anhang)

Nach erfolgter Zusammenfassung der Kategorien wurden die Aussagen der jeweiligen Expert_innen in Tabelle 6 neu strukturiert, sodass die reduzierten Aussagen je Expert_in und Kategorie auf einem Blick miteinander verglichen werden konnten.

Kat.	1L	2K	3H	4P	5W
1	1L1B Bedrohung steigt: - Telefonnummern und Mails werden gefälscht - Credentials tauchen im Darknet auf - Angriffe wirden professioneller und organisierter - Wird nicht zurückgehen	2K1B Bedrohungen steigen stark: - virtueller Raum und mehr potenzielle Opfer - Bedrohung wird bleiben, außer starke Reglementierung	3H1B Bedrohungen steigen: - neue Möglichkeiten durch Cloud-Rechenleistung - Angriffe aus internationalem Umfeld - monetär motiviert	4P1B Bedrohungen steigen laufend: - Abbild politischen Verfalls - Geheimdienste schaffen Backdoors - Kriminelle nutzen Backdoors	5W1B Bedrohungen steigen stark: - neue Angriffsvektoren - stärkere Technologien wie Cloud - Anleitungen leicht zu finden - Home Office als Türöffner
2	1L2I Informationssicherheit strategisches Thema: - Ressourcen zugunsten Informationssicherheit - Maßnahmen günstiger als Kosten bei Ausfall - Orientierung stark an ISO 27001, auch BSI und NIST - ISO 27001 Zertifizierung aktuell nicht rentabel, überlegen aber manchmal - IATF 16494 zertifiziert	2K2I - hoher Stellenwert - Kunden vertrauen mit Daten darauf - arbeiten nach ISO 27001 - BSI-Grundschutz wird auch berücksichtigt - laufende Weiterentwicklung und Schulungen	3H2I - ISMS wird aufgebaut - ISO 27001 Zertifizierung geplant - Tisax auch berücksichtigt - externe Schutzschicht für Monitoring & rasche Threat/Incident Detection - dadurch für Angreifer unattraktiv machen	4P2B - hoher Wert auf Informationssicherheit - Kunden erwarten mehr, laufende Investments - Bedrohungen steigen im gleichen Ausmaß Zertifizierungen: - ISO 27001 - DIN EN 50600	5W2I - sehr hoher Stellenwert - selbst Auditor - eigenes Gerät je Projekt - nur State of the Art Infrastruktur - Budgets für IT-Security steigend

Tabelle 6: Auszug der Gegenüberstellung (Eigene Darstellung, siehe Anhang)

Zu guter Letzt wurden die reduzierten Inhalte jenen des Ausgangsmaterials nochmals gegenübergestellt, um die Validität der Reduzierung zu bestätigen. Die zusammengefassten Ergebnisse der Auswertung werden im nachfolgenden Kapitel erläutert.

5.4 Zusammenfassung der Expert_inneninterviews

Insgesamt wurden fünf Personen aus den Branchen KMU, Industrie, kritische Infrastruktur sowie Beratung und Wirtschaftsprüfung befragt. Die Erfahrung der Teilnehmer liegt jeweils zwischen sieben und 30 Jahren in der IT, Informationssicherheits- oder Risikomanagement. Jede der gewählten Interviewteilnehmer_innen ist in einer Managementposition tätig und trägt sowohl ausreichend Entscheidungsbefugnis als auch Verantwortung für sein Handeln.

Nachfolgend werden die Kernaussagen der Expert_innen anhand der in Kapitel 5.3 definierten Kategorien zusammengefasst.

5.4.1 Kategorie 1B: Bedrohung durch Cyberangriffe in nächsten Jahren

Alle Expert_innen gaben an, dass sie die Bedrohung durch Cyberangriffe in den nächsten Jahren als steigend sehen. Dabei wurde auch mehrfach genannt, dass kein Rückgang von Cyberangriffen erwartet wird. Neben der Anzahl der Angriffe nehmen auch die Möglichkeiten der Angreifer neue Ausmaße an. Diese reichen vom Kauf von On-Demand-Rechenleistung bei Cloudprovidern über Schritt für Schritt Anleitungen bis hin zu international organisierten, monetär motivierten Hackergruppen. Mehrere Personen gaben an, dass sie in letzter Zeit aktiv attackiert wurden. Durch die verstärkte Nutzung von Remote-Work und Home-Office wurden Angreifern neue Tore geöffnet. Als weiterer Grund wurden der politische Verfall und die stärkere Involvierung von Geheimdiensten genannt.

5.4.2 Kategorie 2I: Stellenwert von Informationssicherheit in Unternehmen

Generell nimmt die Informationssicherheit bei allen Expert_innen einen hohen Stellenwert im Unternehmen ein. Alle Teilnehmer_innen arbeiten entweder nach dem ISO/IEC 27001 Standard, sind zertifiziert oder führen selbst Zertifizierungen durch. So wurde die ISO/IEC 27001 auch als „der Standard“ für Informationssicherheit genannt. Daneben wurden noch weitere verwendete Frameworks wie vom BSI (Grundschutz, Cybersecurity-Handbuch), NIST, IATF 16494 sowie die DIN EN 50600 genannt. Der Großteil der Auskunftspersonen gab an, in den letzten Jahren viel in Informationssicherheit investiert zu haben und das auch über die nächsten Jahre beizubehalten. Das liegt daran, dass Informationssicherheit stärker bei den Kunden ankommt und auch verstärkt von Lieferanten gefordert wird.

So werden beispielsweise andere Ressourcen zurückgefahren, die Kosten von Ausfällen berechnet und über die Durchführung von Zertifizierungen nachgedacht. Eine Expert_in gab an, sich durch weitgehende Maßnahmen und Schutzschichten bei Angreifern möglichst unattraktiv machen zu wollen.

5.4.3 Kategorie 3K: Einsatz von Kryptographie

Alle Expert_innen gaben an, sowohl symmetrische als auch asymmetrische Verfahren für die Verschlüsselung von Daten und Kommunikation zu verwenden. Festplatten von

Endgeräten werden häufig mittels AES bzw. Bitlocker verschlüsselt, wohingegen bei digitalen Zertifikaten, Kommunikation, Signaturen bzw. Authentifizierung auf asymmetrische Verfahren zurückgegriffen wird. Teilweise wird die Schlüssellänge noch laufend erweitert. Eine Person gab an, Verschlüsselung sogar als Produkt (unverschlüsselbares Backup vom Backup) zur Ransomware Protection anzubieten.

5.4.4 Kategorie 4Q: Bedrohungen durch Quantencomputer

Alle Expert_innen gaben an, sich zumindest privat mit dem Thema Quantencomputer bereits auseinandergesetzt zu haben bzw. sich für die Technologie zu interessieren. Gleichzeitig kam jeweils die Ergänzung, dass die Auskunftspersonen ihren Wissensstand zu dem Thema als eher gering ansehen. Ebenfalls wurden Quantencomputer bei der Mehrheit der Expert_innen im Unternehmen bereits intern thematisiert. Alle Teilnehmer sehen Quantencomputer als zukünftige Bedrohung für die Informationssicherheit.

Die funktionelle Reife von Quantencomputern und die damit einhergehende Bedrohung für die State of the Art Kryptographie wird von der Mehrheit der Expert_innen in den nächsten fünf bis zehn Jahren erwartet. Die Expert_innen sind sich dabei alle bewusst, dass die Zuverlässigkeit gängiger asymmetrischer Kryptographie durch die Performance von Quantencomputern langfristig sehr stark in Gefahr ist. Die laufenden Forschungsansätze und Standardisierungen im Bereich der Post-Quanten-Kryptographie sind dem Großteil der Expert_innen bekannt. Außerdem wurde auch mehrmals angemerkt, dass ein früher Zugang zu der Technologie von Quantencomputern Wettbewerbsvorteile erschaffen kann und zuerst entweder Tech-Riesen, Geheimdienste, Militär oder regierungsnahe Organisationen Zugriff auf leistungsstarke Quantencomputer bekommen werden.

Eine Expert_in gab dazu an, dass es sich bei dem Hype um das Sicherheitsrisiko Quantencomputer auch um ein großes Ablenkungsmanöver von viel wesentlicheren Bedrohungen handeln könnte. So ist das Top Management vieler Unternehmen im Bereich Informationssicherheit häufig überfordert und lässt sich zu voreiligen Maßnahmen verleiten. Also sind nach dieser Ansicht Quantencomputer nur ein Teil einer weitaus größeren Bedrohung.

5.4.5 Kategorie 5M: Maßnahmen gegen die Bedrohung durch Quantencomputer

Keine der Expert_innen gab an, bereits aktiv an Maßnahmen gegen die Bedrohung durch Quantencomputer zu arbeiten. Das wird dadurch begründet, dass aus Sicht der

Expert_innen die Bedrohung noch zu weit in der Zukunft liegt und aktuell akutere Bedrohungen vorhanden sind. Post-Quanten-Kryptographie ist zudem auch noch nicht ausreichend erforscht bzw. standardisiert und kann laut einer Expert_in Backdoors beinhalten, die schwer evaluierbar sind.

Gleichzeitig gab die Mehrheit an, dass sie das Thema laufend beobachten und evaluieren. So wurde auch mehrmals angemerkt, dass Zertifizierungen wie die ISO/IEC 27001 eine Chance sind, in regelmäßigen Abständen neue Risiken zu identifizieren und auch die eingesetzte Technologie laufend zu evaluieren. Weiters gaben auch mehrere Expert_innen an, dass es „schnell gehen kann", die Technologie plötzlich Reife erlangen kann und sie das Thema daher beobachten.

5.4.6 Kategorie 6I: Geschätzte Implementierungsdauer von Maßnahmen

Bei der Frage nach der geschätzten Implementierungsdauer für Maßnahmen wie Post-Quanten-Kryptographie gingen die Meinungen auseinander. Eine Person konnte keine Aussage tätigen, die weiteren Expert_innen schätzten bis auf eine Ausnahme eine mehrjährige Implementierungsdauer (im Schnitt 3 Jahre) mit hohem Aufwand. Eine Expert_in gab an, dass bei einer akuten Gefahrenlage die Implementierung in maximal einem Quartal umgesetzt sein sollte. Wie die Implementierung umgesetzt werden soll, ist nach aktuellen Auskünften der Expert_innen unklar.

5.4.7 Kategorie 7S: Risikoeinschätzung von Store-now-decrypt-later Angriffen

Schlussendlich wurde noch die Risikoeinschätzung zum Store-now-decrypt-later Angriff abgefragt, wobei die Meinungen dazu sehr unterschiedlich waren. Die Mehrheit der Expert_innen gab an, dass Daten mit der Dauer massiv an Wert verlieren und das Risiko daher zu vernachlässigen ist bzw. sich kein monetärer Wert aus diesen Angriffen erzielen lässt.

Dennoch gaben Expert_innen an, dass ein Leck bei gewissen vertraulichen Daten wie Krankenakten, Unternehmensdaten, interner Kommunikation, Geschäftsführer- oder Prozessdaten sehr schmerzhaft sein kann. Eine Person gab an, dass das der Worst Case schlechthin wäre, da das Vertrauen der Kunden in das Unternehmen damit verletzt werden würde. Auch bei dieser Fragestellung wurden nochmals Geheimdienste, Regierungen, Wissenschaft sowie Tech-Riesen als potenzielle Angreifer genannt, die gleichzeitig gewisse Schlüsse aus den gesammelten Daten ziehen. Eine Person gab an, dass der Angriff de facto nichts Neues ist und veraltete Verschlüsselungen in der Zukunft

sehr häufig geknackt werden können. Für einen Angriff der heimischen Industrie benötigt es laut Auskunft einer Expert_in in einem Großteil der Fälle keinen Store-now-decrypt-later Angriff, da Produktionsdaten ohnedies nur schwach oder überhaupt nicht verschlüsselt sind.

5.4.8 Abschließende Aussagen

Abschließend dankte der Großteil der Expert_innen für den Mut, ein Thema wie dieses zu wählen und Awareness im Bereich Informationssicherheit und im speziellen auf das Sicherheitsrisiko Quantencomputer zu schaffen. Es wurde dabei mehrmals angegeben, dass die IT bzw. IT-Security in heimischen Unternehmen noch häufig als Kostenfaktor und Showstopper angesehen wird. Dennoch ist es wichtig, sich schon heute Gedanken über Morgen zu machen und Informationssicherheit proaktiv zu betrachten. Es muss noch eine Kultur für Informationssicherheit geschaffen werden.

Die Bedrohung durch Quantencomputer wird laut Aussagen entweder noch nicht erkannt oder noch nicht als kritisch gesehen. Es wird gehofft, in diesem Fall einen Schritt vor den Angreifern zu sein und, dass die Chancen von Quantencomputern, die Risiken künftig überschatten.

6. Zusammenfassung

In dieser Masterarbeit wurden insgesamt fünf qualitative Interviews durchgeführt, die auf Basis des Theorieteils zu sieben Kategorien zusammengefasst wurden. Ziel des empirischen Teils war herauszufinden, inwieweit sich österreichische Unternehmen dem Sicherheitsrisiko durch Quantencomputer bewusst sind und welche Maßnahmen bereits geplant sind. Nach Auswertung der Ergebnisse gilt es nun, diese entsprechend mit der Theorie zu diskutieren und die richtigen Schlüsse daraus zu ziehen. Dabei wird die Struktur der Interviews verfolgt und von generellen Bedrohungen und Informationssicherheit hin zu den konkreten Bedrohungen durch Quantencomputer übergeleitet.

Als theoretische Basis für diese Arbeit wurden neben einigen Papers aus der wissenschaftlichen Community auch einige Ausführungen von öffentlichen Informationssicherheitsbehörden wie dem NIST, ENISA, ETSI und dem BSI gewählt, welche den aktuellen Forschungsstand in der benötigten Tiefe abbilden.

6.1 Diskussion der Ergebnisse

Zunächst wurde sowohl im theoretischen als auch im empirischen Teil eine stark ansteigende Bedrohungslage durch Cyberangriffe festgestellt. Die von *Müller* im Theorieteil genannten allgemeinen Bedrohungen (Müller, 2018, p. 1 ff.) wurden durch die Expert_innen noch konkretisiert und eine stärker werdende Involvierung von Geheimdiensten im Cyberspace festgestellt. Ein wesentlicher Grund dazu lässt sich in einer aktuell global sehr angespannten Situation finden, in der der Westen an Dominanz verliert und parallel dazu ein Aufstieg neuer Weltmächte in Asien zu beobachten ist.

Ein steigendes staatliches Interesse an der digitalen Sicherheit ist auch durch Ausführungen des *BSI* erkennbar, seit der amerikanische Geheimdienst NSA im Jahr 2015 eine offizielle Warnung vor der Bedrohung durch Quantencomputer ausgesprochen hat (BSI, 2021a) und die Technologie von staatlichen Organisationen wie dem Heimatschutzministerium und Militär stark gefördert wird (BSI, 2020).

Ein genereller Schutz vor neuen Cyberangriffen existiert nicht. Was jedoch zur Erhöhung des Sicherheitsniveaus in Unternehmen beiträgt, ist die Anwendung von Informationssicherheitsstandards wie der ISO/IEC 27000 oder dem BSI-Grundschutz. Während diese in der verwendeten Literatur zwar nicht direkt als Maßnahmen gegen

Quantencomputer vom *BSI* oder *ENISA* genannt wurden, zwingen sie nach Angaben der Expert_innen Unternehmen allerdings dazu, regelmäßig Risiken neu zu bewerten und eingesetzte technologische Standards wie kryptographische Verfahren auf deren Aktualität zu überprüfen. Somit können sie zumindest als Basis der Maßnahmenplanung gegen die Bedrohung durch Quantencomputer gesehen werden (BSI, 2021b; ENISA, 2021).

Wie einleitend von *Joseph et al.* und *Mosca* beschrieben wurde, entsteht durch Quantencomputer eine generell Bedrohungslage für IT-Systeme (Joseph et al., 2022; Mosca, 2018). Dies zeigt auch der empirische Teil, da sämtliche Infrastrukturen der Auskunftspersonen asymmetrische Kryptographie zur Verschlüsselung von Daten und Kommunikation verwenden und damit früher oder später anfällig auf Angriffe mit leistungsfähigen Quantencomputern sein werden. Dadurch wird bestätigt, dass bis zu einer entsprechenden technologischen Reife von Quantencomputern ein langer Weg der Umrüstung vor uns liegt. Wird dieser technologische Übergang verabsäumt, so können wie *Yunakovsky et al.* festhalten, die Vertraulichkeit und Integrität von Daten ab einem gewissen Zeitpunkt nicht mehr sichergestellt werden und damit auch digitale Kommunikation von Dritten entschlüsselt bzw. mitgehört werden (Yunakovsky et al., 2021).

Hierzu ist weiters anzumerken, dass der empirische Teil selbst bei ausgewiesenen ein IT-Expert_innen ein Wissensdefizit zum Thema Quantencomputer aufzeigt. Zwar ist ein privates Interesse an dem Themengebiet vorhanden und auch unternehmensintern wurden diese Gefahren zwar thematisiert, allerdings nicht tiefer darauf eingegangen. Das mag daran liegen, dass aktuell weitaus akutere Gefahren lauern und Informationssicherheit häufig immer noch als Kostenfaktor gesehen wird. Darüber hinaus ist die Bedrohung durch Quantencomputer noch viel zu weit in der Ferne, als dass bereits mit der Planung von Maßnahmen begonnen werden würde. Was dabei möglicherweise unterschätzt wird, ist der Aufwand und die Dauer, die mit der gänzlichen Implementierung quantensicherer Kryptographie und der Quarantäne unsicherer Geräte verbunden ist. Schließlich stellt jedes vernetzte, aber nicht quantensichere Gerät ein Einfallstor für Angreifer dar (ETSI, 2020). Wird den Ausführungen von *Mosca* Beachtung geschenkt, so liegt die Chance einer akuten Bedrohung bis 2027 bei 1:6, bis 2032 jedoch schon bei 1:2 (Mosca, 2018). Während im empirischen Teil aufkam, dass mit einem frühen Zugang zu leistungsstarken Quantencomputern massive Wettbewerbsvorteile erzielt werden können, wurde dieser Aspekt in der behandelten Literatur nicht erwähnt. In

diesem Bereich könnte möglicherweise eine Forschungslücke identifiziert werden, die Potenzial für weitere Arbeiten in sich trägt.

Genau umgekehrt verhält sich der Erkenntnisgewinn bei der Identifikation von Maßnahmen zum Schutz vor Quantencomputern. In diesem Bereich liefern das *BSI* und die *ENISA* eine Reihe von Empfehlungen. Hierzu zählen die hybride Verwendung Post-Quanten-Kryptographie in Verbindung mit bereits standardisierten, nicht quantenresistenten Verschlüsselungsverfahren wie z.B. dem RSA. Alternativ kann auch ein symmetrischer, vorab geteilter Schlüssel als Basis für Public Key Infrastrukturen verwendet werden. Es wird aber auch generell empfohlen, bei der Einführung neuer Systeme den Faktor Kryptoagilität miteinzubeziehen. Eine weitere betrachtete Maßnahme der sogenannten Quantenkryptographie erwies sich bereits im Theorieteil als aktuell rein wissenschaftlicher Ansatz, da dessen praktische Umsetzung bislang nur in ein paar Experimenten unter kontrollierten Bedingungen realisiert werden konnte. Schlussendlich bedarf allerdings bei sämtlichen Maßnahmen und der darauffolgenden Implementierung noch tieferer Forschung (BSI, 2021b; ENISA, 2021). Aufgrund der noch spärlichen Auseinandersetzung mit der Thematik konnten im empirischen Teil somit keine Planungsansätze der in der Literatur beschriebenen Maßnahmen identifiziert werden. Dies mag auch daran liegen, dass ein gewisser Respekt vor den zu standardisierenden Post-Quanten-Algorithmen gegeben ist. Einerseits könnten nach Ansicht von Expert_innen Backdoors eingebaut werden, andererseits unterstreicht auch *Mosca* die Gefahr von neuen Sicherheitslücken durch überhastete Implementierung (Mosca, 2018). Das *BSI* ergänzt zu diesem Aspekt, dass Post-Quanten-Kryptographie aufgrund fehlender Erfahrungen im Hinblick auf Implementierungssicherheit noch schwer zu bewerten ist und gleichzeitig anfällig für Side-Channel Angriffe sein kann (BSI, 2021b). Dieser Aspekt muss besonders kritisch gesehen werden, da sich mittlerweile mit SIKE (Choi, 2022) und CRYSTALS-Kyber (Dubrova et al., 2022) zwei durch das *NIST* zur Standardisierung ausgewählten Post-Quanten-Algorithmen (Moody, 2022) als anfällig gegen Angriffe durch klassische Computer erwiesen haben. Auch wenn dies keine generelle Ablehnung dieser Verfahren zur Konsequenz haben wird, müssen gewisse Detailoperationen noch verbessert werden und als Folge daraus, wird der Standardisierungsprozess des NIST noch weitere Zeit und Forschung in Anspruch nehmen. Dieser Aspekt kann auch als Henne-Ei-Problem gesehen werden: Unternehmen implementieren keine Post-Quanten-Algorithmen, weil sie auf eine Standardisierung warten. Diese Standardisierung verzögert sich allerdings, da praktische Anwendungen

auf sich warten lassen und damit zu wenig Angriffs- sowie Verbesserungsmöglichkeiten aufgezeigt werden.

Somit wird auf Unternehmensseite aller Voraussicht nach in den nächsten Jahren weiterhin beobachtet, bis ein wesentlicher Durchbruch in der Entwicklung von Quantencomputern verkündet wird oder zumindest absehbar ist. Ab diesem Zeitpunkt wird die von Expert_innen geschätzte rund dreijährige Implementierungsdauer starten und damit ein Wettlauf gegen Angreifer ins Leben gerufen. Wie *Joseph et al.* festhalten, müssen ab diesem Zeitpunkt Milliarden von Geräten auf quantenresistente Verschlüsselungsverfahren umgestellt werden (Joseph et al., 2022), was zu einer generellen, globalen Herausforderung in einer digitalen Welt führen wird. Deshalb empfiehlt die *ENISA* bereits jetzt, schwer zugängliche Geräte, bei denen sich Upgrades als schwierig gestalten, zu identifizieren und deren Auswirkung auf eine künftige Umrüstung zu berücksichtigen (ENISA, 2021). Schließlich könnten es im zukünftigen Ernstfall genau diese Geräte sein, die sehr unangenehmen Verzögerungen in der Migration ins Post-Quanten-Zeitalter führen.

Schließlich bleibt noch offen, inwieweit die Vertraulichkeit von Daten gegenüber einem Store-now-decrypt-later Angriff aufrechterhalten werden kann. Zwar waren die Erkenntnisse aus dem empirischen Teil sehr unterschiedlich und teilweise widersprüchlich. Dennoch wurde eine Gefahr durch diesen Angriff erkannt, insbesondere im Hinblick auf vertrauliche und sensible Daten von Kunden oder Prozessen. *Mosca* stellte dazu ein sehr einfaches und klares Modell auf: Die Zeitspanne, die gewisse Daten geschützt werden müssen plus jener, der Implementierung von Post-Quanten-Kryptographie benötigt, darf nicht länger sein als die verbleibende Zeitspanne bis zum Eintritt des Post-Quanten-Zeitalters. So könnte der Zeitpunkt zum Beginn der rechtzeitigen Implementierung von Post-Quantum-Algorithmen bereits in der Vergangenheit liegen und schon heute könnten Angreifer vertrauliche Daten sammeln, die sie in ein paar Jahren mithilfe von effektiven Quantencomputern entschlüsseln können (Mosca, 2018). Inwieweit solche Angriffe schon heute ausgeführt werden, kann auf Basis der vorliegenden Informationen nicht beantwortet werden. Einerseits wird nicht davon ausgegangen, dass die jeweiligen Unternehmen der Expert_innen Ziele solcher Angriffe sind. Andererseits schätzen die Expert_innen den Einsatz dieser Technik bei Geheimdiensten bzw. regierungsnahen Organisationen als hochrelevant ein.

6.2 Beantwortung der Forschungsfrage

Während die Sub-Forschungsfragen bereits im vorhergehenden Kapitel diskutiert wurden, gilt es nun, die allgemeine Forschungsfrage noch konkret zu beantworten. Diese wurde im Einleitungsteil folgendermaßen formuliert:

Inwieweit sind sich österreichische Unternehmen dem Sicherheitsrisiko durch Angriffe mittels Quantencomputern bewusst?

Grundsätzlich kann diese Forschungsfrage insoweit beantwortet werden, als dass ein grundlegendes Bewusstsein des Sicherheitsrisikos gegeben ist. Dieses Problembewusstsein ist allerdings vorrangig zu den Verantwortlichen aus Bereichen wie IT, IT-Sicherheit und Risikomanagement vorgedrungen. Der technische Fortschritt von Quantencomputern und damit die Bedrohungslage wird außerdem laufend beobachtet. Schlussendlich werden die Standardisierung und eine gewisse Reife von Post-Quanten-Kryptographie abgewartet, bevor mit der Planung von Maßnahmen begonnen wird.

6.3 Fazit & Ausblick

Quantencomputer werden durch ihre (noch) theoretische Rechenkraft nicht nur revolutionäre Möglichkeiten für Forschung, Wirtschaft und Gesellschaft mit sich bringen, sondern auch noch nie dagewesene Angriffsszenarien auf digitale Infrastrukturen ermöglichen.

Zwar ist der erste wichtige Schritt gegangen und zumindest bei den IT-Verantwortlichen ist das Angriffsrisiko durch Quantencomputer angekommen. Aktuell wird auf dieses Bedrohungsszenario allerdings noch kaum aktiv eingegangen geschweige denn Maßnahmen geplant, da Bedrohungen in der Informationssicherheit generell sehr stark steigen. Damit wird der Fokus auf weitaus wesentlichere, größere bzw. dringendere Bedrohungen gelegt und die Reife von Quantencomputer noch zu weit am Horizont entfernt gesehen. Da kaum mit einem Rückgang des Trends zu rechnen ist, werden in den nächsten Jahren große Summen in die Informationssicherheit von österreichischen Unternehmen gesteckt, auch wenn einige Unternehmen IT und IT-Sicherheit noch als Kostenfaktor und Showstopper sehen.

Die wohl am stärksten verbreitete und weitreichendste Schutzmaßnahme ist das Arbeiten nach dem Informationssicherheitsstandard ISO/IEC 27000. Diese zwingt im Zuge der Zertifizierungswellen Unternehmen dazu, sich ihre technische Umwelt genau anzusehen,

neue Risiken zu identifizieren und veraltete Technologien zu ersetzen. Damit kann auch mehr oder weniger sichergestellt werden, dass das Risiko Quantencomputer laufend beobachtet wird und bei absehbaren technologischen Durchbrüchen einigermaßen rasch mit der Evaluierung von Maßnahmen begonnen wird.

Dazu stellt sich auch abschließend nochmal die Frage, wie weit das Post-Quanten-Zeitalter noch weit in der Zukunft liegt, da zwischenzeitlich laufend technologische Durchbrüche verkündet werden. Einer davon ist jener von *Google Quantum AI et al.* im Bereich der Fehlerkorrektur: So resultierte die Erhöhung der Anzahl physischer Qubits auf 49 in einer wesentlich niedrigerer Fehlerrate und erzielte damit eine wesentliche Performancesteigerung der Rechenleistung (Google Quantum AI et al., 2023). Gleichzeitig wird auch laufend an neuen Algorithmen geforscht: *Yan et al.* zeigten eine Methode auf, den RSA-2048 mit einem 372 Qubit-Quantencomputer zu entschlüsseln, allerdings ohne eine Dauer für diese Operation nennen zu können (Yan et al., 2022). Auf der anderen Seite könnten auch die als weniger kritisch angesehenen, symmetrischen Verschlüsselungsverfahren zum Ziel neuer Algorithmen werden. So entwickelten *Wang et al.* eine Methode, mit der Angriffszeiten auf symmetrische Verschlüsselungen stark variieren und teilweise bessere Ergebnisse als Grover's Algorithmus liefern (Wang et al., 2022).

Schlussendlich ist es absehbar, dass in den nächsten Jahren zu einem gewissen Zeitpunkt die Dringlichkeit von Post-Quanten-Kryptographie erkannt und der Druck auf rasche Implementierungsmöglichkeiten steigen wird. Genau dadurch können aber Implementierungsfehler entstehen oder Sicherheitslücken übersehen werden, die erst recht neue Einfallstore für Angreifer öffnen. Es bleibt also noch unklar, ob die Chancen von Quantencomputern eines Tages die Bedrohungen überschatten. Gleichzeitig legen sowohl aktuelle Forschungsansätze als auch Expertenmeinungen nahe, dass in den nächsten Jahren wohl ein Wettlauf zwischen „Angreifern" mit Quantencomputern und „Beschützern" mit Post-Quanten-Kryptographie aufkeimen wird. Ob zu diesem Zeitpunkt ein großes Chaos ausbricht oder die IT-Sicherheit bereits einen Schritt voraus ist und die Sicherheit von Informationen weiterhin gewährleisten kann, bleibt abzuwarten. Der technologische Fortschritt von Quantencomputern wird weiter mit Spannung beobachtet.

Literaturverzeichnis

Amazon Braket, 2022. Quantum Computing Service—Amazon Braket–Amazon Web Services [WWW Document]. URL https://aws.amazon.com/de/braket/ (accessed 8.20.22).

AQTION, 2022. AQTION Quantum Computer. URL https://www.aqtion.eu/ (accessed 8.20.22).

Aragon, N., Gaborit, P., Zémor, G., 2020. HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code. https://doi.org/10.48550/ARXIV.2005.10741

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G.S.L., Buell, D.A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., Fowler, A., Gidney, C., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M.P., Hartmann, M.J., Ho, A., Hoffmann, M., Huang, T., Humble, T.S., Isakov, S.V., Jeffrey, E., Jiang, Z., Kafri, D., Kechedzhi, K., Kelly, J., Klimov, P.V., Knysh, S., Korotkov, A., Kostritsa, F., Landhuis, D., Lindmark, M., Lucero, E., Lyakh, D., Mandrà, S., McClean, J.R., McEwen, M., Megrant, A., Mi, X., Michielsen, K., Mohseni, M., Mutus, J., Naaman, O., Neeley, M., Neill, C., Niu, M.Y., Ostby, E., Petukhov, A., Platt, J.C., Quintana, C., Rieffel, E.G., Roushan, P., Rubin, N.C., Sank, D., Satzinger, K.J., Smelyanskiy, V., Sung, K.J., Trevithick, M.D., Vainsencher, A., Villalonga, B., White, T., Yao, Z.J., Yeh, P., Zalcman, A., Neven, H., Martinis, J.M., 2019. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510. https://doi.org/10.1038/s41586-019-1666-5

ASCII, 2022. ASCII Code - The extended ASCII table [WWW Document]. URL https://www.ascii-code.com/ (accessed 8.15.22).

Azure Quantum, 2022. Azure Quantum: Quantum-Dienst | Microsoft Azure [WWW Document]. URL https://azure.microsoft.com/de-de/services/quantum/ (accessed 3.11.22).

Barker et al., 2021. MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.

Bennett, C.H., 1992. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121–3124. https://doi.org/10.1103/PhysRevLett.68.3121

Bennett, C.H., Brassard, G., 1984. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science 560, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Bernstein, D.J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., Schwabe, P., 2019. The SPHINCS+ Signature Framework, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. Presented at the CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security, ACM, London United Kingdom, pp. 2129–2146. https://doi.org/10.1145/3319535.3363229

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehle, D., 2018. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM, in: 2018 IEEE European Symposium on Security and Privacy

(EuroS&P). Presented at the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, London, pp. 353–367. https://doi.org/10.1109/EuroSP.2018.00032

Bovino, F.A., 2019. Intrasystem Entanglement Generator and Unambiguos Bell States Discriminator on Chip, in: ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Presented at the ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Brighton, United Kingdom, pp. 7993–7997. https://doi.org/10.1109/ICASSP.2019.8683820

Bradben, 2022. What are the Q# programming language & QDK? - Azure Quantum [WWW Document]. URL https://docs.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk (accessed 8.20.22).

BSI, 2022. BSI-Standards [WWW Document]. URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html (accessed 10.13.22).

BSI, 2021a. Migration to Post Quantum Cryptography.

BSI, 2021b. Quantum-safe cryptography – fundamentals, current developments and recommendations.

BSI, 2020. Entwicklungsstand Quantencomputer. BSI.

Caltech, 2021. Caltech and Amazon Partner to Create New Hub of Quantum Computing [WWW Document]. California Institute of Technology. URL https://www.caltech.edu/about/news/caltech-and-amazon-partner-to-create-new-hub-of-quantum-computing (accessed 8.20.22).

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., 2016. Report on Post-Quantum Cryptography (No. NIST IR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Choi, C.Q., 2022. "Quantum-Safe" Crypto Hacked by 10-Year-Old PC [WWW Document]. IEEE Spectrum. URL https://spectrum.ieee.org/quantum-safe-encryption-hacked (accessed 10.6.22).

Computer Security Division, I.T.L., 2017. Workshops and Timeline - Post-Quantum Cryptography | CSRC | CSRC [WWW Document]. CSRC | NIST. URL https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (accessed 6.26.22).

de Wolf, R., 2017. The potential impact of quantum computers on society. Ethics Inf Technol 19, 271–276. https://doi.org/10.1007/s10676-017-9439-z

Dempe, S., Schreier, H., 2006. Operations Research: deterministische Modelle und Methoden, 1. Aufl. ed, Teubner Studienbücher Wirtschaftsmathematik. Teubner, Wiesbaden.

Dubrova, E., Ngo, K., Gärtner, J., 2022. Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste.

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D., 2018. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. TCHES 238–268. https://doi.org/10.46586/tches.v2018.i1.238-268

D-Wave, 2022. The Advantage™ Quantum Computer | D-Wave [WWW Document]. URL https://www.dwavesys.com/solutions-and-products/systems/ (accessed 8.20.22).

Eckert, C., 2013. IT-Sicherheit: Konzepte - Verfahren - Protokolle, 8., aktualisierte und korr. Aufl. ed. Oldenbourg, München.

Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67, 661–663. https://doi.org/10.1103/PhysRevLett.67.661

Ellerhoff, B.M., 2020. Mit Quanten rechnen: Quantencomputer für Neugierige, essentials. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-31222-0

ENISA, 2021. Post-quantum cryptography: current state and quantum mitigation. Publications Office, LU.

ETSI, 2020. Migration strategies and recommendations to Quantum Safe schemes.

European Commission, 2020. European Commission: "Midterm Report of the Quantum Technologies Flagship."

Feynman, R.P., 1982. Simulating physics with computers. Int J Theor Phys 21, 467–488. https://doi.org/10.1007/BF02650179

Fouque, Pierre-Alain, Hoffstein, Jeffrey, Kirchner, Paul, 2020. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU.

Gibney, E., 2017. D-Wave: Scientists Line Up for World's Most Controversial Quantum Computer [WWW Document]. Scientific American. URL https://www.scientificamerican.com/article/d-wave-scientists-line-up-for-world-rsquo-s-most-controversial-quantum-computer/ (accessed 8.20.22).

Google Quantum AI, 2022. Cirq [WWW Document]. Google Quantum AI. URL https://quantumai.google/cirq (accessed 8.20.22).

Google Quantum AI, Acharya, R., Aleiner, I., Allen, R., Andersen, T.I., Ansmann, M., Arute, F., Arya, K., Asfaw, A., Atalaya, J., Babbush, R., Bacon, D., Bardin, J.C., Basso, J., Bengtsson, A., Boixo, S., Bortoli, G., Bourassa, A., Bovaird, J., Brill, L., Broughton, M., Buckley, B.B., Buell, D.A., Burger, T., Burkett, B., Bushnell, N., Chen, Y., Chen, Z., Chiaro, B., Cogan, J., Collins, R., Conner, P., Courtney, W., Crook, A.L., Curtin, B., Debroy, D.M., Del Toro Barba, A., Demura, S., Dunsworth, A., Eppens, D., Erickson, C., Faoro, L., Farhi, E., Fatemi, R., Flores Burgos, L., Forati, E., Fowler, A.G., Foxen, B., Giang, W., Gidney, C., Gilboa, D., Giustina, M., Grajales Dau, A., Gross, J.A., Habegger, S., Hamilton, M.C., Harrigan, M.P., Harrington, S.D., Higgott, O., Hilton, J., Hoffmann, M., Hong, S., Huang, T., Huff, A., Huggins, W.J., Ioffe, L.B., Isakov, S.V., Iveland, J., Jeffrey, E., Jiang, Z., Jones, C., Juhas, P., Kafri, D., Kechedzhi, K., Kelly, J., Khattar, T., Khezri, M., Kieferová, M., Kim, S., Kitaev, A., Klimov, P.V., Klots, A.R., Korotkov, A.N., Kostritsa, F., Kreikebaum, J.M., Landhuis, D., Laptev, P., Lau, K.-M., Laws, L., Lee, J., Lee, K., Lester, B.J., Lill, A., Liu, W., Locharla, A., Lucero, E., Malone, F.D., Marshall, J., Martin, O., McClean, J.R., McCourt, T., McEwen, M., Megrant, A., Meurer Costa,

B., Mi, X., Miao, K.C., Mohseni, M., Montazeri, S., Morvan, A., Mount, E., Mruczkiewicz, W., Naaman, O., Neeley, M., Neill, C., Nersisyan, A., Neven, H., Newman, M., Ng, J.H., Nguyen, A., Nguyen, M., Niu, M.Y., O'Brien, T.E., Opremcak, A., Platt, J., Petukhov, A., Potter, R., Pryadko, L.P., Quintana, C., Roushan, P., Rubin, N.C., Saei, N., Sank, D., Sankaragomathi, K., Satzinger, K.J., Schurkus, H.F., Schuster, C., Shearn, M.J., Shorter, A., Shvarts, V., Skruzny, J., Smelyanskiy, V., Smith, W.C., Sterling, G., Strain, D., Szalay, M., Torres, A., Vidal, G., Villalonga, B., Vollgraff Heidweiller, C., White, T., Xing, C., Yao, Z.J., Yeh, P., Yoo, J., Young, G., Zalcman, A., Zhang, Y., Zhu, N., 2023. Suppressing quantum errors by scaling a surface code logical qubit. Nature 614, 676–681. https://doi.org/10.1038/s41586-022-05434-1

Grover, L.K., 1996. A fast quantum mechanical algorithm for database search, in: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96. Presented at the the twenty-eighth annual ACM symposium, ACM Press, Philadelphia, Pennsylvania, United States, pp. 212–219. https://doi.org/10.1145/237814.237866

Heimann, P.M., 1973. Reviews : The Born-Einstein Letters. Correspondence between Albert Einstein and Max and Hedwig Born from 1916 to 1955 with commentaries by Max Born. Translated by Irene Born. London, Macmillan, I970. 320 pp. £3.85. European Studies Review 3, 198–199. https://doi.org/10.1177/026569147300300214

Homeister, M., 2022. Quantum Computing verstehen: Grundlagen – Anwendungen – Perspektiven, Computational Intelligence. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-36434-2

Honeywell, 2022. Honeywell Quantum Computing [WWW Document]. URL https://www.honeywell.com/us/en/company/quantum (accessed 8.20.22).

IBM, 2022a. IBM Quantum Computing Roadmap [WWW Document]. URL https://www.ibm.com/quantum/www.ibm.com/quantum/roadmap (accessed 8.20.22).

IBM, 2022b. IBM Qiskit Runtime [WWW Document]. URL https://www.ibm.com/quantum/qiskit-runtime (accessed 8.20.22).

Infineon, 2021. Quantencomputing: Schlüsseltechnologie des 21. Jahrhunderts - Infineon Technologies [WWW Document]. URL https://www.infineon.com/cms/de/discoveries/quantum-computing/ (accessed 3.11.22).

Intel, 2022. Intel Quantum Computing [WWW Document]. Intel. URL https://www.intel.com/content/www/us/en/research/quantum-computing.html (accessed 8.20.22).

IonQ, 2022. IonQ Quantum Computing [WWW Document]. IonQ. URL https://ionq.com/ (accessed 8.20.22).

ISO/IEC, 2018a. ISO/IEC 27000:2018 [WWW Document]. ISO. URL https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73906.html (accessed 9.16.22).

ISO/IEC, 2018b. ISO/IEC 27002 - 2013-10 - Beuth.de [WWW Document]. URL https://www.beuth.de/de/norm/iso-iec-27002/194462674 (accessed 9.23.22).

ISO/IEC, 2018c. ISO/IEC 27001 - 2013-10 - Beuth.de [WWW Document]. URL https://www.beuth.de/de/norm/iso-iec-27001/194462684 (accessed 9.23.22).

IST Austria, 2021. Dossier - Quantencomputer.

Jao, D., De Feo, L., 2011. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, in: Yang, B.-Y. (Ed.), Post-Quantum Cryptography, Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 19–34. https://doi.org/10.1007/978-3-642-25405-5_2

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., Hansen, R., 2022. Transitioning organizations to post-quantum cryptography. Nature 605, 237–243. https://doi.org/10.1038/s41586-022-04623-2

Kersten, H., Klett, G., Reuter, J., Schröder, K.-W., 2020. IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, Edition <kes>. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-27692-8

Kießling, C., 2021. Das IT-Sicherheitsrisiko Quantencomputer.

Köbler, J., Beyersdorff, O., 2006. Von der Turingmaschine zum Quantencomputer — ein Gang durch die Geschichte der Komplexitätstheorie, in: Reisig, W., Freytag, J.-C. (Eds.), Informatik. Springer Berlin Heidelberg, pp. 165–195. https://doi.org/10.1007/3-540-32743-6_8

KPMG, 2019. Sicherheitsrisiko Quantencomputer. KPMG.

Lau, H.-K., Lo, H.-K., 2011. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Phys. Rev. A 83, 012322. https://doi.org/10.1103/PhysRevA.83.012322

Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V., 2010. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon 4, 686–689. https://doi.org/10.1038/nphoton.2010.214

Mainzer, K., 2020. Quantencomputer: Von der Quantenwelt zur Künstlichen Intelligenz. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-61998-8

Marre, A.J., 2021. Welche Quantencomputer gibt es jetzt schon? URL http://www.quantencomputer-info.de/quantencomputer/welche-quantencomputer-gibt-es-jetzt-schon/ (accessed 8.20.22).

Mavroeidis, V., Vishi, K., Zych, M.D., Jøsang, A., 2018. The Impact of Quantum Computing on Present Cryptography. ijacsa 9. https://doi.org/10.14569/IJACSA.2018.090354

Mayring, P., 2015. Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12., überarb. Aufl. ed. Beltz, Weinheim Basel.

McArdle, S., Endo, S., Aspuru-Guzik, A., Benjamin, S.C., Yuan, X., 2020. Quantum computational chemistry. Rev. Mod. Phys. 92, 015003. https://doi.org/10.1103/RevModPhys.92.015003

McEliece, R.J., 1978. A public-key cryptosystem based on algebraic. Coding Thv 4244 114–116.

Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P.S.L.M., 2013. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes, in: 2013 IEEE International Symposium on Information Theory. Presented at the 2013 IEEE International Symposium on Information Theory (ISIT), IEEE, Istanbul, Turkey, pp. 2069–2073. https://doi.org/10.1109/ISIT.2013.6620590

Moguel, E., Rojo, J., Valencia, D., Berrocal, J., Garcia-Alonso, J., Murillo, J.M., 2022. Quantum service-oriented computing: current landscape and challenges. Software Qual J. https://doi.org/10.1007/s11219-022-09589-y

Moody, D., 2022. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process (No. NIST IR 8413). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8413

Moreau, P.-A., Toninelli, E., Gregory, T., Aspden, R.S., Morris, P.A., Padgett, M.J., 2019. Imaging Bell-type nonlocal behavior. Sci. Adv. 5, eaaw2563. https://doi.org/10.1126/sciadv.aaw2563

Mosca, M., 2018. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy 16, 38–41. https://doi.org/10.1109/MSP.2018.3761723

Müller, K.-R., 2018. IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-22065-5

Nebel, M., Wild, S., 2018. Entwurf und Analyse von Algorithmen, Studienbücher Informatik. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-21155-4

NIST, 2022. Draft Call for Additional Digital Signature Schemes for the PostQuantum Cryptography Standardization Process.

OpenSuperQ, 2022. OpenSuperQ Quantum Computer [WWW Document]. URL https://opensuperq.eu/ (accessed 8.20.22).

Pednault et al., 2019. On “Quantum Supremacy” [WWW Document]. IBM Research Blog. URL https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/ (accessed 8.20.22).

Petereit, D., 2021. Google: Kommerzieller Quantencomputer soll 2029 einsatzbereit sein [WWW Document]. t3n Magazin. URL https://t3n.de/news/google-quantencomputer-2029-1379872/ (accessed 8.20.22).

Poeppelmann, T., 2021. The Battle For Post-Quantum Security Will Be Won By Agility [WWW Document]. Semiconductor Engineering. URL

https://semiengineering.com/the-battle-for-post-quantum-security-will-be-won-by-agility/ (accessed 10.2.22).

Preskill, J., 2021. Quantum computing 40 years later. https://doi.org/10.48550/ARXIV.2106.10522

QUTAC, Bayerstadler, A., Becquin, G., Binder, J., Botter, T., Ehm, H., Ehmer, T., Erdmann, M., Gaus, N., Harbach, P., Hess, M., Klepsch, J., Leib, M., Luber, S., Luckow, A., Mansky, M., Mauerer, W., Neukart, F., Niedermeier, C., Palackal, L., Pfeiffer, R., Polenz, C., Sepulveda, J., Sievers, T., Standen, B., Streif, M., Strohm, T., Utschig-Utschig, C., Volz, D., Weiss, H., Winter, F., 2021. Industry quantum computing applications. EPJ Quantum Technol. 8, 25. https://doi.org/10.1140/epjqt/s40507-021-00114-x

Rigetti, 2022. Rigetti Quantum Computing [WWW Document]. Rigetti Computing. URL https://www.rigetti.com/ (accessed 8.20.22).

Scarani, V., Acín, A., Ribordy, G., Gisin, N., 2004. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. Phys. Rev. Lett. 92, 057901. https://doi.org/10.1103/PhysRevLett.92.057901

Sharma, N., Ketti Ramachandran, R., 2021. The Emerging Trends of Quantum Computing Towards Data Security and Key Management. Arch Computat Methods Eng 28, 5021–5034. https://doi.org/10.1007/s11831-021-09578-7

Shor, P.W., 1994. Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science. Presented at the 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press, Santa Fe, NM, USA, pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700

Tan, T.G., Szalachowski, P., Zhou, J., 2022. Challenges of post-quantum digital signing in real-world applications: a survey. Int. J. Inf. Secur. https://doi.org/10.1007/s10207-022-00587-6

Thakkar, J.K., 2016. Quantum Cryptography – A Quantum leap in Security. IJETT 41, 15–18. https://doi.org/10.14445/22315381/IJETT-V41P203

Wang, Z., Wei, S., Long, G.-L., Hanzo, L., 2022. Variational quantum attacks threaten advanced encryption standard based symmetric cryptography. Sci. China Inf. Sci. 65, 200503. https://doi.org/10.1007/s11432-022-3511-5

Wegener, C., Milde, T., Dolle, W., 2016. Informationssicherheits-Management: Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung, Xpert.press. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49167-6

Wong, T.G., 2022. Introduction to classical and quantum computing. Rooted Grove, Omaha, Nebraska.

Wu, Y., Bao, W.-S., Cao, S., Chen, F., Chen, M.-C., Chen, X., Chung, T.-H., Deng, H., Du, Y., Fan, D., Gong, M., Guo, Cheng, Guo, Chu, Guo, S., Han, L., Hong, L., Huang, H.-L., Huo, Y.-H., Li, L., Li, N., Li, S., Li, Y., Liang, F., Lin, C., Lin, J., Qian, H., Qiao, D., Rong, H., Su, H., Sun, L., Wang, L., Wang, S., Wu, D., Xu, Y., Yan, K., Yang, W., Yang, Y., Ye, Y., Yin, J., Ying, C., Yu, J., Zha, C., Zhang, C., Zhang, H.,

Zhang, K., Zhang, Y., Zhao, H., Zhao, Y., Zhou, L., Zhu, Q., Lu, C.-Y., Peng, C.-Z., Zhu, X., Pan, J.-W., 2021. Strong Quantum Computational Advantage Using a Superconducting Quantum Processor. Phys. Rev. Lett. 127, 180501. https://doi.org/10.1103/PhysRevLett.127.180501

Yan, B., Tan, Z., Wei, S., Jiang, H., Wang, W., Wang, Hong, Luo, L., Duan, Q., Liu, Y., Shi, W., Fei, Y., Meng, X., Han, Y., Shan, Z., Chen, J., Zhu, X., Zhang, C., Jin, F., Li, H., Song, C., Wang, Z., Ma, Z., Wang, H., Long, G.-L., 2022. Factoring integers with sublinear resources on a superconducting quantum processor.

Yunakovsky, S.E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., Kiktenko, E.O., Kolycheva, E., Borisov, A., Fedorov, A.K., 2021. Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. EPJ Quantum Technol. 8, 14. https://doi.org/10.1140/epjqt/s40507-021-00104-z

Zhong, H.-S., Deng, Y.-H., Qin, J., Wang, H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Wu, D., Gong, S.-Q., Su, H., Hu, Y., Hu, P., Yang, X.-Y., Zhang, W.-J., Li, H., Li, Y., Jiang, X., Gan, L., Yang, G., You, L., Wang, Z., Li, L., Liu, N.-L., Renema, J.J., Lu, C.-Y., Pan, J.-W., 2021. Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light. Phys. Rev. Lett. 127, 180502. https://doi.org/10.1103/PhysRevLett.127.180502

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang A – Interviewleitfaden

Zur Durchführung der Interviews wurde ein Interviewleitfaden erstellt, der einen Rahmen während des Gesprächs bildet. Er dient vorrangig der Beantwortung der Forschungsfragen und wurde daher von diesen sowie den Erkenntnissen des Theorieteils abgeleitet. Sofern der/die Interviewteilnehmer_in in beratender Funktion tätig ist, können die folgenden Fragen auf Partnerunternehmen/Kund_innen umformuliert werden.

Nach einer kurzen Einleitung zum Hintergrund und zur Zielsetzung der Masterarbeit wird mit einer Eisbrecherfrage begonnen, die dann auf das Thema Informationssicherheit weiterführt. Der Fragebogen beinhaltet folgende Fragestellungen:

1. Was ist Ihr aktuelles Tätigkeitsfeld und wie lange sind Sie schon in dieser Branche/diesem Bereich (IT-Sicherheit/Risikomanagement) tätig?

2. Wie schätzen Sie die Bedrohung durch Cyberangriffe allgemein für die nächsten Jahren ein?

3. Welchen Stellenwert legt Ihr Unternehmen auf Informationssicherheit bzw. arbeitet Ihr Unternehmen nach gewissen Informationssicherheitsstandards (ISMS)?

4. Welche kryptographischen Verfahren haben Sie in Ihrem Unternehmen zur Verschlüsselung von Daten sowie Kommunikation im Einsatz (symmetrisch, asymmetrisch)?

5. Inwieweit haben Sie sich bereits mit Quantencomputer auseinandergesetzt bzw. wie würden Sie Ihren Wissensstand zu diesem Thema einschätzen?

6. Welche Risiken sehen Sie durch Quantencomputer in Bezug auf die IT-Sicherheit als kritisch und ab welchem Zeitpunkt schätzen Sie, dass Quantencomputer ein wirkliches Problem für die IT-Landschaft darstellen wird?

7. Welche Maßnahmen haben Sie bereits geplant? (Alternativ: Wann werden Sie mit der Planung von Maßnahmen beginnen?)

8. Wie lange schätzen Sie, dass Ihr Unternehmen für die Implementierung von Post-Quanten-Kryptographie benötigen wird?

9. Beim sogenannten „Store-now-decrypt-later Angriff“ werden verschlüsselte Daten bereits heute abgehört und gesammelt, in der Hoffnung, diese mittels Quantencomputern in einigen Jahren zu entschlüsseln. Wie gravierend wäre solch ein Angriff für Ihr Unternehmen hinsichtlich Datenschutzes, Geschäftsgeheimnissen, interne Kommunikation oder Ähnlichem?

10. Vielen Dank für Ihre Einblicke! Haben Sie noch sonstiges Feedback zu diesem Thema oder möchten Sie sonst noch etwas ergänzen?

Anhang B – Kategorisierung der Interviews

Fall	Kategorie	Nr.	Paraphrasierung	Generalisierung	Reduktion
1L	1B	1	Die Bedrohung durch Cyber Angriffe in den nächsten Jahren wird sehr hoch eingeschätzt.	Die Bedrohung steigt.	1L1B Bedrohung steigt: - Telefonnummern und Mails werden gefälscht - Credentials tauchen im Darknet auf - Angriffe wirden professioneller und organisierter - Wird nicht zurückgehen
1L	1B	2	Wir sehen dass Telefonnummern gefälscht werden damit bei uns angerufen wird.	Telefonnummern werden gefälscht	
1L	1B	3	Wir sehen auch, dass Partner, Kunden und Lieferanten gefälschte Mails von uns bekommen.	Partner bekommen gefälschte Mails	
1L	1B	4	Wir sehen auch, dass Credentials von uns im Darknet auftauchen.	Credentials tauchen im Darknet auf	
1L	1B	5	Ich glaube generell, dass die Angriffe professioneller und organisierter werden. Das Niveau wird noch steigen.	Angriffe werden professioneller und organisierter. Niveau steigt	
1L	1B	6	Ich glaube nicht, dass das irgendwann wieder normal wird. Das ist eher das neue normal.	Wird nicht wieder normal	
1L	1B	7	Wir werden uns daran gwöhnen müssen, dass wir alle 3 Monate wo lesen, dass eine größere Firma gehackt wurde.	~~Alle 3 Monate wird große Firma gehackt~~	
1L	2I	8	Bei uns ist Informationssicherheit ein strategisches Thema und bekommt viel Management Attention.	Informationssicherheit ist strategisches Thema und bekommt viel Management Attention	1L2I Informationssicherheit strategisches Thema: - Ressourcen zugunsten Informationssicherheit - Maßnahmen günstiger als Kosten bei Ausfall - Orientierung stark an ISO/IEC 27001, auch BSI und NIST - ISO/IEC 27001 Zertifizierung
1L	2I	9	Es werden Projekte zurückgefahren, zugunsten von Informationssicherheitsmaßnahmen.	Ressourcen zugunsten Informationssicherheit	
1L	2I	10	Wir haben die Kosten eines typischen Ausfalls von 10 Tagen berechnet und die Mahnahmen dagegen sind kostengünstiger.	Kosten eines Ausfalls übersteigen die von Maßnahmen	

1L	2I	11	Wir haben aktuell keine Zertifizierung, da wir noch keinen kaufmännischen Vorteil sehen.	Aktuell keine Zertifizierung aus kaufmännischen Gründen	aktuell nicht rentabel, überlegen aber manchmal - IATF 16494 zertifiziert
1L	2I	12	Wir orientieren uns an ISO/IEC 27001.	Orientierung an ISO/IEC 27001	
1L	2I	13	Wir sind IATF 16949 zertifiziert, wo Cybersicherheit eine immer größere Rolle spielt.	IATF 16949 zertifiiziert	
1L	2I	14	Wir bekommen viele Fragebögen von Kunden und Partnern, wo Informationssicherheit abgefragt wird. Mit einer ISO/IEC 27001 Zertifizierung würden wir uns die restlichen Fragen ersparen. Daher überlegen wir doch manchmal nach einer Zertifizierung.	Überlegen manchmal Zertifizierung	
1L	2I	15	Wir orientieren uns auch noch an BSI-Standards, BSI Cybersecurity Handbuch und NIST Standards.	Orientierung an BSI-Standards, BSI Cybersecurity Handbuch und NIST Standards.	
1L	3K	16	Wir haben unterschiedliche Verschlüsselungsmechanismen im Einsatz wie VPN, TLS, verschiedene Zertifikate, eine PKI, die Verschlüsselung der Cloud etc.	symmetrische (Cloud, SAP) und asymmetrische Verfahren (TLS, PKI, Zertfikate)	K1L.3 - symmetrisch (Cloud, SAP) - asymmetrisch (TLS, PKI, Zertifikate)
1L	4Q	17	Als Unternehmen haben wir uns noch nicht mit Quantencomputern beschäftigt, ich als Person sehr wohl. Ich verfolge die Nachrichten dazu.	Im Unternehmen noch kein Thema, privates Interesse	1L4Q - privates Interesse - im Unternehmen noch kein Thema - wird neue Security Modelle benötigen - in Architektur eingreifen - im Darknet schon angeboten - Reife in 5-10 Jahren (große Unternehmen)
1L	4Q	18	Wenn jeder Quantencomputer im Einsatz hat, haben wir ein immenses Problem. Dann können wir 90% der bisherigen Security Modelle verwerfen und alles neu gestalten. Je nachdem, welche Practices es dann gibt.	Bei Reife der Technologie Security Modelle verwerfen und neu gestalten, in Architektur eingreifen	

1L	4Q	19	Angeblich kann man sich Quantencomputer schon im Darknet kaufen.	Im Darknet schon vorhanden	
1L	4Q	20	Meistens kommen diese Trends schneller, als einem lieb ist. Ich schätze, in 5-10 Jahren könnte große Unternehmen Quantencomputer zur Verfügung haben.	In 5-10 Jahren für große Unternehmen im Einsatz	
1L	5M	21	Wir schützen uns momentan vor organisiertem Verbrechen und nicht vor Geheimdiensten und staatlichen Akteuren. Meiner Meinung nach werden diese als erste Quantencomputer im Einsatz haben, um andere Regierungen und anzugreifen und Rüstungsgeheimnisse in Erfahrung zu bringen.	Schutz vor organisiertem Verbrechen; Angriffe eher durch Geheimdiensten und staatlichen Akteuren	1L5M - Schutzmaßnahmen vor organisiertem Verbrechen, in nächsten 3-4 Jahren unwahrscheinlich - Use Case eher bei Geheimdiensten / Staaten - vorbereiten, darüber nachdenken, aber keine Vorbereitungen - muss erst etwas passieren - nächste Jahr thematisieren
1L	5M	22	Ich glaube nicht, dass das organisiserte Verbrechen in den nächsten 3-4 Jahren Quantencomputer zur Verfügung haben wird.	Organisiertes Verbrechen keinen Zugang in den nächsten 3-4 Jahren	
1L	5M	23	Nichtsdestotrotz muss man sich bereits jetzt darauf vorbereiten oder zumindest darüber nachdenken.	vorbereiten, darüber nachdenken	
1L	5M	24	Wir haben keine Vorbereitungen gemacht und sehen das noch zu weit weg am Horizont.	keine Vorbereitungen, zu weit am Hoizont	
1L	5M	25	Es muss zuerst wo etwas passieren, vor man sich Gedanken über dieses Risiko macht.	warten auf Vorfall	
1L	5M	26	Wir werden das Thema spätestens nächstes Jahr ansprechen, dass wir da einen Trend sehen und dann stellt sich heraus, wie man damit umgeht	Nächstes Jahr ansprechen	

1L	6I	27	Wenn die bisherigen Verschlüsselungsmechanismen nicht mehr sinnvoll sind, wird man Neues brauchen. Ich weiß zumindest jetzt nicht, wie das aussehen wird.	vorhandene Verschlüsselungsmechanismen ersetzen; wie ist noch unklar	1L6I - aktuelle Verschlüsselungen ersetzen - wie ist unklar - hoher Aufwand, mehrjährig
1L	6I	28	Das wird durchaus sehr viel Aufwand sein und eine mehrjährige Reise, um das umzusetzen.	viel Aufwand, mehrjährige Reise	
1L	7S	29	Ich schätze das Risiko als eher gering ein,	Risiko gering	1L7S geringes Risiko weil, - Know-How in Patenten öffentlich - Daten eher wertlos in 10 Jahren - Keine rechtliche Aufmerksamkeit (Datenschutz)
1L	7S	30	Unser Know-How steckt in Patenten und ist öffentlich einsehbar. Die Forschung wird mit dem Ziel betrieben, sie patentieren zu lassen.	Know-How in Patenten, öffentlich einsehbar	
1L	7S	31	Ich habe keine Angst, dass etwas abgehört und in 10 Jahren entschlüsselt werden könnte und dem Mitbewerb einen wesentlichen Vorteil gibt.	Daten haben in 10 Jahren keinen großen Wert mehr.	
1L	7S	32	Im Hinblick auf Datenschutz denke ich nicht, dass die momentane Rechssprechung auf das Problem aufmerksam ist, also sehe ich kein riesen Risiko.	Datenschutz kein Thema, keine Aufmerksamkeit	
2K	1B	33	Seit die Covid Pandemie gekommen ist, sind die Cyberangriffe exponentiell gestiegen.	Bedrohungen steigen stark	2K1B Bedrohungen steigen stark: - virtueller Raum und mehr potenzielle Opfer - Bedrohung wird bleiben, außer starke Reglementierung
2K	1B	34	Das kann sein, weil wir uns sehr stark in den virtuellen Raum zurückgezogen haben oder weil seither mehr virtuelle Teilnehmer und damit auch mehr potenzielle Opfer existieren.	Gründe: Rückzug in virtuellen Raum und mehr potenzielle Opfer	
2K	1B	35	Das ist ein Zeichen der Zeit und wird auch ganz normal so weiterlaufen.	wird nicht wieder normal	

2K	1B	36	Das wird es immer geben, es sei denn, wir beginnen den virtuellen Raum sehr stark zu reglementieren. Das ist aber nicht im Sinne des Erfinders und will auch keiner in dem Zusammenhang.	immer geben, außer starker Regelmentierung	
2K	2I	37	Wir legen einen sehr hohen Stellenwert auf Informationssicherheit, nachdem wir mit Daten von Kunden arbeiten und uns ein hohes Vertrauen entgegengebracht wird.	hoher Stellenwert auf Informationssicherheit aufgrund von Kundendaten und Vertrauen	2K2I - hoher Stellenwert - Kunden vertrauen mit Daten darauf - arbeiten nach ISO/IEC 27001 - BSI-Grundschutz wird auch berücksichtigt - laufende Weiterentwicklung und Schulungen
2K	2I	38	Wir arbeiteten nach dem eigentlich Standard der Informationssicherheit, der ISO/IEC 27001, aber auch der BSI-Grundschutz wird berücksichtigt.	arbeiten nach ISO/IEC 27001, aber auch BSI-Grundschutz	
2K	2I	39	Es gibt immer Weiterentwicklungen in der Hauseigenen IT. Zur Zeit führen wir ein hauseigenes SOX SIEM ein.	ständige Weiterentwicklungen intern	
2K	2I	40	Das ist ein ständiges Thema und wir führen auch viele Schulungsmaßnahmen durch.	viele Schulungsmaßnahmen	
2K	2I	41	Wir haben eine Phishing-Kampagne auf unserer Mitarbeiter gefahren und seitdem hat sich das Thema exponentiell gebessert.	Schulungsmaßnahme Phishing	
2K	2I	42	Wenn jemand eine Email oder App nicht kennt, wird das sofort an eine Sandbox gschickt und dementsprechend gescreened.	Awareness geschaffen intern	
2K	3K	43	Auf Exchange haben wir TLS im Einsatz, ein asymmetrisches Verfahren.	asymmetrisch (TLS)	2K3K - asymmetrisch (TLS) - symmetrisch (AES, Bitlocker)
2K	3K	44	Die Daten werden mit AES, also einem symmetrischen Verfahren verschlüsselt. Bei den Clients verwenden wir Bitlocker.	symmetrisch (AES, Bitlocker)	

2K	4Q	45	Mein Kenntnisstand ist rudimentär. Intern und im Beratungsumfeld haben wir uns nicht damit auseinandergesetzt.	privat damit auseinandergesetzt, im Unternehmen nicht	2K4Q - privates Interesse - beruflich kein Thema, keine Beratung - Chance durch Rechenleistung - Risiko bei Kryptographie - neue Möglichkeiten für Angreifer - Einsatz zuerst durch regierungsnahe Organisationen und Tech-Riesen - kommerzielle Nutzung in 5-10 Jahren
2K	4Q	46	Ich glaub Quantencomputing ist eine irrsinnige Chance, wenn es um dieses Thema und um das Thema Rechenleistung geht.	Chance im Thema Rechenleistung	
2K	4Q	47	Quantencomputer bringen das hohe Risiko mit sich, durch die hohe Rechenleistung entsprechende kryptologische Schutverfahren auszuhebeln.	Risiko im Bereich kryptologische Schutzverfahren aushebeln	
2K	4Q	48	Es stellt sich auch die Frage, wer Zugang zu dieser Technologie hat. Die dunkle Seite hat viel mehr Möglichkeiten, seine Machenschaften durchzuziehen.	bietet dunkler seite mehr Möglichkeiten	
2K	4Q	49	Quantencomputer werden schon eingesetzt. Aktuell sind sie sehr teuer und werden von Regierungen und regierungsnahmen Organisationen eingesetzt.	Quantencomputer werden schon eingesetzt, aktuell aber sehr teuer und regierungsnahen Organisationen vorbehalten	
2K	4Q	50	Eine Gefahr wird es sein, wenn es kommerzielle wird und die Tech-Riesen haben dann schon einen exponentiellen Vorteil.	Gefahr durch kommerzielle Nutzung; Tech-Riesen haben einen exponentiellen Vorteil	
2K	4Q	51	Die technische Entwicklung steigt exponentiell und daher kann es recht schnell gehen, sodass ich in den nächsten 5-10 Jahren eine kommerzielle Nutzung schätze.	Kommerzielle Nutzung in 5-10 Jahren	
2K	5M	52	Ich habe keine Maßnahmen geplant, da ich die Kommerzialität erst in den nächsten 5-10 Jahren sehe.	Keine Maßnahmen geplant, zu weit weg	2K5M keine Maßnahmen, weil - zu weit entfernt - keine Nachfrage am Markt

2K	5M	53	Ich merke nicht, dass Quantumcomputing am Markt ein großes Thema wäre.	Am Markt kein großes Thema	- dringendere Bedrohungen - kann sich rasch ändern
2K	5M	54	Ich glaub das Thema Quantencomputer ist bei uns und Unternehmen die ich berate noch nicht angekommen oder aufgekommen.	~~Am Markt kein großes Thema~~	
2K	5M	55	Das Thema ist bei österreichischen Unternehmen nicht auf der Agenda, da es auch andere Bedrohungen in unserem Bereich gibt.	Andere Bedrohungen bei österreischen Unternehmen	
2K	5M	56	Es könnte aber dann im weiteren Vorgehen rasch gehen, wenn Quantencomputer funktionieren und kommerzieller umgesetzt werden.	Könnte rasch gehen, wenn kommerzielle Nutzung in Sichtweite	
2K	6I	57	Es hängt davon ab, wann diese verfügbar sind.	Noch nichts verfügbar	2K6I - wenn verfügbar, 3-5 Jahre für Implementierung
2K	6I	58	Wenn zum Datum X kommerzielle Quantencomputer zur Verfügung stehen, dann wird die Implementierung Schutzmaßnahmen dazu von diesem Zeitpunkt an meistens 3-5 Jahre benötigen.	Nach Verfügbarkeit 3-5 Jahre für Implementierung	
2K	7S	59	Das ist der worst Case schlechthin.	Worst Case	2K7S - worst case, weil Vertrauen der Kunden verletzt - Use Case für Wissenschaft, Regierungen & Nachrichtendienste - keine monetäre Motivation - Google oder Techriesen ziehen Schlüsse daraus; äußerst kritisch
2K	7S	60	Der worst Case bei einem Ransomwareangriff ist nicht nur verschlüsselt zu sein, sondern auch, dass vertrauliche Daten abgezogen werden.	~~Datenleck auch Problem bei Ransomware größtes Problem~~	
2K	7S	61	Wir arbeiten ja mit den Kundendaten und dem Vertrauen, damit vertrauensvoll umzugehen.	Datenleck größtes Problem, weil Vertrauen verletzt	
2K	7S	62	Daten zu sammeln und später auszuwerten ist eigentlich ein Use Case für Regierungen und Nachrichtendienste.	Use Case ist eher bei Regierungen und Nachrichtendiensten	

2K	7S	63	Aus monetärer Sicht sehe ich bei Hackern kaum Motivation für so einen Angriff.	Keine monetäre Motivation bei Hackern	
2K	7S	64	Wenn Google oder Tech-Riesen auf die Idee kommen, Unmengen an Daten zu speichern und auszuwerten, dann werden die gewisse Schlüsse daraus ziehen. Das sehe ich äußerst kritisch.	Aus Daten können Schlüsse gezogen werden, wenn diese von Tech-Riesen gesammelt werden. Äußerst kritisch	
2K	7S	65	Diese Thema ist in der Wissenschaft, bei Regierungen und Tech-Riesen unterwegs.	~~Thema eher bei Wissenschaft, Regierungen & Tech-Riesen~~	
3H	1B	66	Die Bedrohungen schätze ich als sehr stark ein und vor allem steigend. Nicht nur in der Anzahl, sondern auch in den Möglichkeiten	Bedrohungen steigen stark, auch in Möglichkeiten	3H1B Bedrohungen steigen, - neue Möglichkeiten durch Cloud-Rechenleistung - Angriffe aus internationalem Umfeld - monetär motiviert
3H	1B	67	Es sind nicht mehr nur Botnetze oder Script Kiddies, die auch Schaden verursachen können.	~~Neue Angriffe tauchen auf~~	
3H	1B	68	Mittlerweile kann sich jeder beim Standard Cloudanbieter extreme Rechenpower für einen Angriff mieten. Wir reagieren schon auf dieses Thema, auch wenn es noch nicht so sehr in die Breite getragen wurde.	Bedrohung durch Cloud-Rechenpower on demand für Angriffe	
3H	1B	69	Wir sehen in unseren Auswertungen schon internationale Hacking Groups, die auf das große Geld aus sind.	Internationale Groups greifen an und sind auf Geld aus	
3H	2I	70	Wir bauen gerade im Hintergrund ein ISMS auf, in Richtung Tisax und ISO/IEC 27001 und streben auch die entsprechende Zertifizierung an.	ISMS wird aufgebaut, Tisax und ISO/IEC 27001 Zertifizierung	3H2I - ISMS wird aufgebaut - ISO/IEC 27001 Zertifizierung geplant - Tisax auch berücksichtigt - externe Schutzschicht für Monitoring & rasche Threat/Incident Detection
3H	2I	71	Aktuell bauen wir eine externe Schutzschicht inklusive Darknet Scanning. Eine externe Firma scannt 70-100% unseres Traffics mit und kann unser internes SOC Team sofort alarmieren.	Externe Schutzschicht wird aufgebaut inkl. Scanning & Monitoring	

3H	2I	72	Ich möchte so schnell wie möglich mitbekommen, wenn ich angegriffen werde, um entsprechende Maßnahmen im Incident- und Krisenmanagement einleiten zu können.	Schnelle Threat & Incident Detection im Aufbau	- dadurch für Angreifer unattraktiv machen
3H	2I	73	Es ist nur eine Frage der Zeit, bis es uns erwischt. Deshalb machen wir uns mit Sicherheitsmaßnahmen so unattraktiv wie möglich.	Durch Maßnahmen unattraktiv machen.	
3H	3K	74	Für die Festplattenverschlüsselung verwenden wir Bitlocker, also symmetrisch.	symmetrisch (Bitlocker)	3H3K - symmetrisch (AES) - asymmetrisch für Authentifizierung - Hashing (SHA256) - Schlüssellänge wird ausgebaut
3H	3K	75	Wir haben AES256 für die Verschlüsselung und für die Authentifizierung SHA256 im Einsatz.	symmetrisch (AES256), asymmetrisch für Authentifizierung, Hashing (SHA256)	
3H	3K	76	Wir schauen, dass unsere Schlüssel lange sind, sind aber noch nicht im Endausbau.	Lange Schlüssel, aber noch nicht Endausbau	
3H	4Q	77	Ich schätze meinen Wissensstand zu Quantencomputer als gering ein. Ich habe mich damit beschäftigt und es spannend gefunden, im Detail ist das Thema aber schwieriger nachzuvollziehen.	Geringer Wissenstand zu Quantencomputern, spannend aber komplex	3H4Q - spannendes, aber komplexes Thema - geringer Wissensstand - intern thematisiert - Angriffe werden in Zukunft erwartet - Risiko moderat durch Post-Quanten-Kryptographie - symmetrische Verfahren nicht betroffen - Anwenung asysmmetrischer Verfahren neu überdenken - Angreifer schneller als Schutzmaßnahmen
3H	4Q	78	Wir haben uns bereits Gedanken gemacht. Ab dem Zeitpunkt, an dem Quantencomputer das erste Mal richtig funktionieren, werden wir Angriffe damit sehen.	Quantencomputer wurden thematisiert, zukünftige Angriffe damit werden erwartet	
3H	4Q	79	Ich sehe das Risiko aktuell noch nicht so tragisch, weil auch die Securityseite reagiert und an Post-Quanten-Kryptographie arbeitet.	Risiko moderat, weil an Post-Quanten-Kryptographie gearbeitet wird.	

3H	4Q	80	Symmetrische Verfahren wären ohnedies nicht wirklich angreifbar. Bei asymmetrischen Verfahren muss man sich überlegen, was man damit verschlüsselt.	Keine Gefahr für symmetrische Verfahren; Daten hinter asymmetrische Verfahren überdenken	
3H	4Q	81	Wir rüsten uns generell viel durch Trennung, laufende Bewertung und Monitoring. Ich möchte schnell mitbekommen, wenn wir angegriffen werden.	~~Rüsten uns generell gegen Bedrohungen~~	
3H	4Q	82	Das Schwert wird dem Schild ein bisschen voraus sein und es wird Angriffe mit Quantencomputern geben.	Angreifer werden Schutzmaßnahmen voraus sein	
3H	5M	83	Spezfisch gegen Quantencomputer haben wir noch keine Maßnahmen geplant.	keine Maßnahmen geplant	3H5M - aktuell keine Maßnahmen - laufende Beobachtung und Evaluierung - bei Fortschritten startet Maßnahmenplanung
3H	5M	84	Mit der Planung von Maßnahmen beginnen wir, sobald wir technologische Fortschritte bemerken. Das ist dem geschuldet, dass wir das Ganze aktuell noch aufbauen und wir bereits aktuelle Bedrohungen haben.	laufende Beobachtung, Maßnhamen starten bei technologischen Fortschritten	
3H	5M	85	Bei einer IT-Security Strategie von 3-5 Jahren sollte es zumindest thematisiert und bewertet werden.	sollte zumindest thematisiert/bewertet werden	
3H	6I	86	Wir sind noch sehr reaktiv und als produzierendes Gewerbe wird die IT-Security als Bremse gesehen.	reaktiv, IT-Security wird als Bremse gesehen	3H6I - reaktives Verhalten - IT-Security als Bremse in Produktion - generell schnelle Umsetzung von Maßnahmen - maximal ein Quartal, eher kürzer durch War Room
3H	6I	87	Bei uns werden Maßnahmen sehr schnell implementiert. Nach einem kompromittierten Handy war die MFA-Authenfifizierung 2 Wochen später implementiert.	sehr schnell in der Implementierung von Maßnahmen	

3H	6I	88	Für die Implementierung von Maßnahmen würden wir maximal ein Quartal benötigen, tendenziell aber weniger. Es würde in einen War Room gehen und umgesetzt werden.	maximal ein Quartal, tendenziell schneller durch Errichtung von War Room	
3H	7S	89	Dieser Angriff ist nicht zu unterschätzen.	Nicht zu unterschätzen	3H7S Gefahr nicht zu unterschätzen, teilweise 30 Jahre Aufbewahrungsfristen kritisch: - interne Kommunkation (Teams) - Geschäftsführer (Kommunikation, Festplatte) - Krankenakten - Prozessdaten eher unkritisch: - Geschäftsgeheimnisse
3H	7S	90	Geschäftsgeheimnisse sehe ich nicht so kritisch, unser Gewerbe ist nicht das große Ding.	Geschäftsgeheimnisse nicht kritisch	
3H	7S	91	Wird die interne Kommunikation mitgeschnitten, hätten wir schon ein Thema, besonders bei Geschäftsführern.	interne Kommunikation kritischer	
3H	7S	92	Prozessdaten könnten der Konkurrenz vielleicht das Eine oder Andere verraten.	Prozessdaten kritisch	
3H	7S	93	Es kommt darauf an, was geknackt wird. Eine Geschäftsführerfestplatte oder ein Teams-Channel wäre unangenehm.	Geschäftsführerfestplatte unangenehm	
3H	7S	94	Wir haben teilweise Aufbewahrungsfristen von 30 Jahren, revisisionssicher. Das könnte ein wirklicher Schmerz sein, wenn diese Daten jemand bekommt.	teilweise Aufbewahrungsfristen 30 Jahre	
3H	7S	95	Nicht jeder Breach löst automatisch einen Datenschutzvorfall aus. Bei irgendwelchen Krankenakten von Mitarbeitern hätten wir natürlich ein Thema.	Krankenakten von Mitarbeitern kritisch	
4P	1B	96	Die Bedrohungen werden laufend stiegen, immer größer werden und nicht zurückgehen.	Bedrohungen steigen laufend	4P1B Bedrohungen steigen laufend: - Abbild politischen Verfalls

4P	1B	97	Sie sind ein Abbild des politischen Verfalls in verschiedene Machtsphären. Sichere Systeme werden bewusst kompromittiert und Backdoors am Leben gehalten, um geheimdienstliche Aktivitäten aufrechtzuerhalten. Die Backdoors werden dann von kriminellen Organisationen bewirtschaftet.	Abbild politischen Verfalls, geheimdienste schaffen Backdoors und Kriminelle nützen diese	- Geheimdienste schaffen Backdoors - Kriminelle nutzen Backdoors
4P	2I	98	Wir legen einen hohen Wert auf Informationssicherheit. Unsere Kunden schrauben ihre Erwartungen laufend nach oben.	hoher Wert auf Informationssicherheit, Kundenerwartungen steigen	4P2I - hoher Wert auf Informationssicherheit - Kunden erwarten mehr, laufende Investments - Bedrohungen steigen im gleichen Ausmaß Zertifizierungen: - ISO/IEC 27001 - DIN EN 50600
4P	2I	99	Wir sind seit 10 Jahren ISO/IEC 27001 zertifiziert.	ISO/IEC 27001 zertifiziert seit 10 Jahren	
4P	2I	100	Wir investieren laufend mehr Geld in Cyber Security und müssen erkennen, dass in mindestens gleichem Ausmaß die Bedrohungen steigen.	Laufende Investments in Cyber Security, Bedrohungen steigen im gleichen Ausmaß	
4P	2I	101	Wir sind auch nach DIN EN 50600 zertifiziert, einer Infrastrukturrichtlinie für Data Center.	DIN EN 50600 zertifiziert	
4P	3K	102	Wir haben die klassischen Verschlüsselungsverfahren im Einsatz und kündigen die unsicheren ab. Das passiert in enger Koordination mit den Kunden, weil diese immer stark mit Applikationen verwoben sind.	klassische Verschlüsselungsverfahren, kündigen die unsicheren ab	4P3K - symmetrische - asymmetrische - laufende Updates - Verschlüsselung als Produkt
4P	3K	103	Wir haben also symmetrische und asymmetrische Verfahren im Einsatz.	symmetrische und asymmetrische Verfahren im Einsatz	
4P	3K	104	Wir haben auch ein Produkt, das ein Backup vom Backup symmetrisch verschlüsselt. Dieses Backup kann dann nicht weiter verschlüsselt werden und geht Richtung Ransomware Protection.	Verschlüsselung wird als Produkt angeboten (Backups)	

4P	4Q	105	Ich bin laufend interessiert am Thema Quantencomputer, mein Wissensstand ist dennoch ein sehr minimaler.	~~privates Interesse, jedoch geringer Wissensstand~~	4P4Q - privates Interesse - geringer Wissensstand - Quantencomputer als Ablenkungsmanöver - nur Teil der großen Bedrohung - einfachere, logischere Angriffe - Top Management überfordert, voreilige Maßnahmen - Verschlüsselung verändert sich - neue Angriffsvektoren - Militär-, Verteidigungs- und IT-Industrie federführend - in 8 Jahren möglich
4P	4Q	106	Als Informatiker habe ich nicht die geistigen Fähigkeiten, um die Idee hinter Quanten und Quantencomputer zu verstehen.	~~Eher für Physiker geeignet~~	
4P	4Q	107	Ich habe eine ungefähre Vorstellung, wie Quantencomputer das N=NP Problem lösen könnte. Ich weiß aber, dass das in der Praxis extrem schwierig sein wird.	Kennt Lösungsweg für N=NP Problem	
4P	4Q	108	Ich bin der Meinung, dass das Thema Quantencomputer ein großes Ablenkungsmanöver ist. Die größeren Bedrohungen kommen von ganz anderen Ecken.	Quantencomputer sind ein Ablenkungsmanöver von echten Bedrohungen	
4P	4Q	109	Die Aufmerksamkeitsspanne des Top Managements ist sehr gering und die sind sehr dünn besetzt, sodass es viel einfachere Wege gibt, um an kritische Daten zu kommen.	Top Management wird damit Aufmerksamkeit entzogen	
4P	4Q	110	Es gibt viel einfachere und logischere Angriffsvektoren wie Standard-Bibliotheken zu kompromittieren, mit einem Patchkabel in einem Data Center einen Port zu spiegeln oder anderes.	Einfachere und logischere Angriffsvektoren verfügbar	
4P	4Q	111	Viele sind von der Komplexität so überfordert, dass sie die nötigsten Maßnahmen umsetzen, um ein bisschen besser als der Branchendurchschnitt zu sein.	~~Komplexität verursacht voreilige Maßnahmen~~	

4P	4Q	112	Viele verwenden dann Microsoft Azure, weil sie damit keine grundlgegenden Fehler machen und nicht alleine auf der Anklagebank sitzen.	~~Microsoft Azure profitiert von Angst~~	
4P	4Q	113	Wenn wir in der Post-Quaum-Ära sind, wird die Verschlüsselung auch wieder verändertn und angepassst werden. Das ist ein Katz und Maus Spiel.	Verschlüsselung wird sich verändern und erneuern, wie auch Angreifer	
4P	4Q	114	Es gibt gewisse Industrien, die diese Landschaft bewirtschaften, ihre Interessen durchsetzen oder ihre Profite maximieren. Dazu gehört die Militärindustrie, die Verteidigungsindustrie oder die IT-Industrie.	Militär-, Verteidigungs- und IT-Industrie profitieren davon.	
4P	4Q	115	Quantencomputer werden sich in das ganze Bild einfügen und nicht die ganze Welt auf den Kopf stellen.	Quantencomputer als Teil der Bedrohung.	
4P	4Q	116	Ich rechne in Technologiezyklen von 4 Jahren. In 4 Jahren werden sie noch nicht in der Lage sein, aktuelle Schlüsseln zu knacken. Also dauert es noch weitere 4 Jahre, bis ein Angriffsvektor als Bedrohung auftaucht, also 8 Jahre.	Erste Bedrohungen in ca. 8 Jahren, 2 Zyklen a 4 Jahre	
4P	5M	117	Wir beschäftigen uns damit, welche quantensichere Verschlüsselung es gibt. Aber man weiß da auch noch nicht, welche tatsächlich quantensicher sind.	Post-Quanten-Kryptographie wird beobachtet, noch nicht marktreif	4P5M - Post-Quanten-Kryptographie wird beobachtet - nicht marktreif - nur marktreife Technik im Einsatz - Evaluierung bei ISO/IEC 27001 Audit
4P	5M	118	Wir werden immer nur jene Technik verwenden, die es am Markt verfügbar gibt.	nur marktreife Technik im Einsatz	

4P	5M	119	Es kann sein, dass die quantensicheren Verschlüsselungen eigentlich unsicherer sind als das, was wir jetzt verwenden. Es könnte auch eine Backdoor eingebaut werden, wir befinden uns immerhin in der Post Snowden Ära.	Risiken durch Backdoor in Post-Quanten-Kryptographie möglich, Post-Snowden	- Risiken durch Backdoors in neuen Verfahren schwer evaluierbar
4P	5M	120	Wir beobachten genau.	~~Post-Quanten-Kryptographie wird beobachtet~~	
4P	5M	121	Wenn Verfahren auftauchen, sollten wir testen, ob nicht Backdoors eingebaut sind. Bei elliptischen Kurven hat es das bereits gegeben, dass Amerikaner Initalwerte gefunden haben, die Backdoors ermöglicht haben. Dafür sind wir Österreicher allerdings zu schwach.	~~Risiken durch Backdoor in Post-Quanten-Kryptographie möglich, Post-Snowden~~	
4P	5M	122	Wir evaluieren jährlich im Zuge unserer ISO/IEC 27001 Audits, ob die Verschlüsselungsmaßnahmen noch dem Stand der Technik entsprechen.	Evaluierung und Beobachtung regelmäßig durch ISO/IEC 27001 Audits	
4P	6I	123	Wir benötigen so 2-3 Jahre.	Implementierungsdauer ca. 2-3 Jahre	4P6I - Dauer 2-3 Jahre
4P	7S	124	Der Angriff ist nichts Neues. Ich kann eine alte Verschlüsselung wie SHA256 mit einem jetzigen oder zukünftigen Rechner auch knacken.	Kein neuer Angriff, bei vielen älteren Verfahren ähnlich	4P7S - nichts Neues - Datenwert sinkt, kurze Halbwertszeit - Use Case für Geheimdienste
4P	7S	125	Ich sehe kein sehr großes Risiko, ganz ehrlich, die Halbwertszeit der Daten ist relativ kurz.	Daten verlieren an Wert durch kurze Halbwertszeit	
4P	7S	126	Bei Geheimdiensten hätte solch ein Angriff mehr Relevanz.	Angriff eignet sich für Geheimdienste	
5W	1B	127	Ich sehe ein zunehmendes Problem und auch, dass die Angriffe immer mehr werden.	Bedrohungen steigen stark	5W1B Bedrohungen steigen stark: - neue Angriffsvektoren

5W	1B	128	Die Angriffsvektoren werden mit zunehmender Digitalisiserung immer mehr.	Angriffsvektoren werden mehr	- stärkere Technologien wie Cloud - Anleitungen leicht zu finden - Home Office als Türöffner
5W	1B	129	Die Technik wird viel performanter und es ist über Internetplattforem fast schon ein bisschen leicht, mit Anleitungen für Angriffe zu finden.	Technik wird stärker und Informationen zu Angriffen sind leicht verfügbar	
5W	1B	130	Ich glaube, dass die Bedrohung in den nächsten Jahren noch sehr intensiv zunehmen wird	~~Bedrohungen steigen stark~~	
5W	1B	131	Neue Zugänge und Positionierung im Home Office öffnen neue Angrifssvektoren.	Home Office als Grund dafür	
5W	2I	132	Ich sehe, dass eine beträchtliche Anzahl größerer Budgets gegen Cyberrisiken locker gemacht oder geplant werden.	Budgets für IT-Security steigen	
5W	2I	133	Wir verwenden für jedes Kundenprojekt eigene Geräte, um eine Teilung der Informationen zu verhindern.	eigenes Gerät für jedes Projekt zur Trennung vomn Informationen	5W2I - sehr hoher Stellenwert - selbst Auditor - eigenes Gerät je Projekt - nur State of the Art Infrastruktur - Budgets für IT-Security steigend
5W	2I	134	Wir sind auch Auditoren im ISO/IEC 27001 Umfeld, also legen sehr Wert auf Informationssicherheit.	Als Auditor hoher Stellenwert	
5W	2I	135	Wir verwenden nur State of the Art Infrastruktur.	Nur Starte of the Art Infrastruktur	
5W	3K	136	Wir verwenden alles, was am Markt ist. Beim Thema VPN verwenden wir elliptische Verfahren und in der Kommunikation asymmetrische Verfahren	Verwendung VPN, elliptische Kurven und asymmetrische Verfahren	5W3K - symmetrische Verfahren - asymmetrische Verfahren (elliptische Kurven, Signaturen)
5W	3K	137	Wir verwenden auch symmetrische Verfahren. Aber zur Klassischen Verschlüsselung bauen wir auf Public Key Verfahren, wie z.B: in der E-Mail Verschlüsselung oder bei digitalen Signaturen.	Auch symmetrische Verfahren, aber stärker asymmetrisch (Public Key bei Verschlüsselung und Signaturen)	

5W	4Q	138	Ich habe mich mit Quantencomputer schon beschäftigt, bin aber kein Wissender.	bereits beschäftigt, Kenntnisstand aber gering	5W4Q - beschäftigt, Wissensstand gering - Bedrohung in der Zukunft - Performance großes Problem bei Ver- und Entschlüsselung - frühe Besitzer erlangen Wettbewerbsvorteil
5W	4Q	139	Ich sehe Quantencomputer als mögliche Bedrohungslage in der Zukunft für mich und meine Kunden.	Als Bedrohung in der Zukunft gesehen	
5W	4Q	140	Ich sehe die Ver- und Entschlüsselung durch Performance als großes Problem.	Ver- und Entschlüsselung durch Performance als großes Problem	
5W	4Q	141	Die Welt kann sich sehr schnell in eine Richtung bewergen, weil es bei dieser Performance nicht mehr viel Gegenwehr gibt.	~~Bedrohung durch Performance~~	
5W	4Q	142	Wer die Technologie der Zukunft bald besitzt, kann sich damit durchaus einen Wettbewerbsvorteil oder Marktvorteil erschaffen.	Wettbewerbsvorteil oder Marktvorteil durch Besitz der Technologie	
5W	4Q	143	Ich denke schon, dass da eine potenzielle Gefahr auf uns zukommt, weil wir in Geschwindigkeiten und Relationen denken, die einfach unglaublich schnell sind. Damit steigt das Gefahrenpotenzial immens mit dieser Technologie.	~~Bedrohung durch Performance~~	
5W	5M	144	Es macht Sinn, sich der Gefahren bewusst zu werden und Risiken anders zu bewerten.	Gefahren bewusst machen, anders bewerten	5W5M - Awareness für Gefahren gefordert - neu bewerten müssen - Zertifizierungen geben regelmäßig Chance zur Evaluierung der Technik
5W	5M	145	Ich empfehle meinen Kunden, Zertifizierungen zu machen. Diese genießen einen Überprüfungsstandard und es müssen regelmäßig Technologien und Bedrohungen betrachtet und evaluiert werden. Damit bin ich immer am Stand der Technik.	Zertifizierungen als Überprüfungsstandard und regelmäßige Evaluierungspflicht. Damit immer State of the Art	
5W	5M	146	Außerdem sollte man genug Awareness schaffen, auch das unerwartete erwarten und gute Notfallpläne haben.	~~Es gehört Awareness geschaffen.~~	

5W	6I	147	Ich glaube, wir können sehr schnell auf den Zug aufspringen und die Vorteile der Technolgie nutzen.	Schnelle Adaptierungsmöglichkeit	5W6I - schnelle Adaptierung notwendig - Gefahr ernst nehmen - keine Idee zu Implementierungsdauer
5W	6I	148	Wir sollten die Gefahr nicht zu weit im Backlog haben.	Gefahr sollte ernst genommen werden	
5W	6I	149	Ich habe mich mit dem Thema zu wenig auseinandergesetzt, um eine ehrliche Antwort zu geben.	zu wenig Information	
5W	7S	150	Die Technologie ist heutzutage in der Argumentation nicht vorhanden. Wenn ich es als Bedrohung sehe, würde ich damit jede Verschlüsselung ad Absurdum führen.	Technologie noch nicht bekannt, daher keine akute Bedrohung	5W7S - kaum Bedrohung aktuell - Daten verlieren an Wert - IT wird als Showstopper gesehen - kaum sichere Verschlüsselung in AT Industrie - Keine Kultur für Informationssicherheit
5W	7S	151	Die Frage ist, ob diese Daten die man heute sammelt in der Zukunft nicht schon obsolet sind.	Daten sind verlieren an Wert	
5W	7S	152	Die Frage ist, ob wir nicht Kommunkation aufs Wesentliche reduzieren könnten und andere Formen des Datenaustausch verweden sollten.	Kommunikation aufs Wesentliche reduzieren	
5W	7S	153	Bei meinen Industriekunden wird IT nicht als Mittel zum Zweck, sonders als Showstopper und Kostenfaktor gesehen wird. Wenn Verschlüsselung eingesetzt wird, dann einfach und rudimentär.	IT-Security wird als Showstopper gesehen	
5W	7S	154	Man muss vielleicht gar nicht überall auf einen Quantencomputer warten und könnte den Verkehr in geschätzt 60% der Fälle auch so schon mithören, weil die gar nicht verschlüsselt sind.	In Industrie kaum sichere Verschlüsselung im Einsatz	
5W	7S	155	Wir müssen noch eine Kultur prägen, in der unsere Informationen unser höchstes Gut ist.	Awareness für Sicherheit muss noch geschaffen werden.	

Anhang C – Gegenüberstellung der Kategorien

KAT	1L	2K	3H	4P	5W
1B	1L1B Bedrohung steigt: - Telefonnummern und Mails werden gefälscht - Credentials tauchen im Darknet auf - Angriffe wirden professioneller und organisierter - Wird nicht zurückgehen	2K1B Bedrohungen steigen stark: - virtueller Raum und mehr potenzielle Opfer - Bedrohung wird bleiben, außer starke Reglementierung	3H1B Bedrohungen steigen, - neue Möglichkeiten durch Cloud-Rechenleistung - Angriffe aus internationalem Umfeld - monetär motiviert	4P1B Bedrohungen steigen laufend: - Abbild politischen Verfalls - Geheimdienste schaffen Backdoors - Kriminelle nutzen Backdoors	5W1B Bedrohungen steigen stark: - neue Angriffsvektoren - stärkere Technologien wie Cloud - Anleitungen leicht zu finden - Home Office als Türöffner
2I	1L2I Informationssicherheit strategisches Thema: - Ressourcen zugunsten Informationssicherheit - Maßnahmen günstiger als Kosten bei Ausfall - Orientierung stark an ISO/IEC 27001, auch BSI und NIST - ISO/IEC 27001 Zertifizierung aktuell nicht rentabel, überlegen aber manchmal - IATF 16494 zertifiziert	2K2I - hoher Stellenwert - Kunden vertrauen mit Daten darauf - arbeiten nach ISO/IEC 27001 - BSI-Grundschutz wird auch berücksichtigt - laufende Weiterentwicklung und Schulungen	3H2I - ISMS wird aufgebaut - ISO/IEC 27001 Zertifizierung geplant - Tisax auch berücksichtigt - externe Schutzschicht für Monitoring & rasche Threat/Incident Detection - dadurch für Angreifer unattraktiv machen	4P2I - hoher Wert auf Informationssicherheit - Kunden erwarten mehr, laufende Investments - Bedrohungen steigen im gleichen Ausmaß Zertifizierungen: - ISO/IEC 27001 - DIN EN 50600	5W2I - sehr hoher Stellenwert - selbst Auditor - eigenes Gerät je Projekt - nur State of the Art - Budgets für IT-Security steigend
3K	1L3K - symmetrisch (Cloud, SAP) - asymmetrisch (TLS, PKI, Zertifikate)	2K3K - asymmetrisch (TLS) - symmetrisch (AES, Bitlocker)	3H3K - symmetrisch (AES) - asymmetrisch für Authentifizierung - Hashing (SHA256) - Schlüssellänge wird ausgebaut	4P3K - symmetrische - asymmetrische - laufende Updates - Verschlüsselung als Produkt	5W3K - symmetrische Verfahren - asymmetrische Verfahren (elliptische Kurven, Signaturen)

4Q	1L4Q - privates Interesse - im Unternehmen noch kein Thema - wird neue Security Modelle benötigen - in Architektur eingreifen - im Darknet schon angeboten - Reife in 5-10 Jahren (große Unternehmen)	2K4Q - privates Interesse - beruflich kein Thema, keine Beratung - Chance durch Rechenleistung - Risiko bei Kryptographie - neue Möglichkeiten für Angreifer - Einsatz zuerst durch regierungsnahe Organisationen und Tech-Riesen - kommerzielle Nutzung in 5-10 Jahren	3H4Q - spannendes, aber komplexes Thema - geringer Wissensstand - intern thematisiert - Angriffe werden in Zukunft erwartet - Risiko moderat durch Post-Quanten-Kryptographie - symmetrische Verfahren nicht betroffen - Anwenung asysmmetrischer Verfahren neu überdenken - Angreifer schneller als Schutzmaßnahmen	4P4Q - privates Interesse - geringer Wissensstand - Quantencomputer als Ablenkungsmanöver - nur Teil der großen Bedrohung - einfachere, logischere Angriffe - Top Management überfordert, voreilige Maßnahmen - Verschlüsselung verändert sich - neue Angriffsvektoren - Militär-, Verteidigungs- und IT-Industrie federführend - in 8 Jahren möglich	5W4Q - beschäftigt, Wissensstand gering - Bedrohung in der Zukunft - Performance großes Problem bei Ver- und Entschlüsselung - frühe Besitzer erlangen Wettbewerbsvorteil
5M	1L5M - Schutzmaßnahmen vor organisiertem Verbrechen, in nächsten 3-4 Jahren unwahrscheinlich - Use Case eher bei Geheimdiensten / Staaten-vorbereiten, darüber nachdenken, aber keine Vorbereitungen - muss erst etwas passieren - nächste Jahr thematisieren	2K5M keine Maßnahmen, weil - zu weit entfernt - keine Nachfrage am Markt - dringendere Bedrohungen - kann sich rasch ändern	3H5M - aktuell keine Maßnahmen - laufende Beobachtung und Evaluierung - bei Fortschritten startet Maßnahmenplanung	4P5M - Post-Quanten-Kryptographie wird beobachtet - nicht marktreif - nur marktreife Technik im Einsatz - Evaluierung bei ISO/IEC 27001 Audit - Risiken durch Backdoors in neuen Verfahren schwer evaluierbar	5W5M - Awareness für Gefahren gefordert - neu bewerten müssen - Zertifizierungen geben regelmäßig Chance zur Evaluierung der Technik

6I	1L6I - aktuelle Verschlüsselungen ersetzen - wie ist unklar - hoher Aufwand, mehrjährig	2K6I - wenn verfügbar, 3-5 Jahre für Implementierung	3H6I - reaktives Verhalten - IT-Security als Bremse in Produktion - generell schnelle Umsetzung von Maßnahmen - maximal ein Quartal, eher kürzer durch War Room	4P6I - Dauer 2-3 Jahre	5W6I - schnelle Adaptierung notwendig - Gefahr ernst nehmen - keine Idee zu Implementierungsdauer
7S	1L7S geringes Risiko weil, - Know-How in Patenten öffentlich - Daten eher wertlos in 10 Jahren - Keine rechtliche Aufmerksamkeit (Datenschutz)	2K7S - worst case, weil Vertrauen der Kunden verletzt - Use Case für Wissenschaft, Regierungen & Nachrichtendienste - keine monetäre Motivation - Google oder Techriesen ziehen Schlüsse daraus; äußerst kritisch	3H7S Gefahr nicht zu unterschätzen, teilweise 30 Jahre Aufbewahrungsfristen kritisch: - interne Kommunkation (Teams) - Geschäftsführer (Kommunikation, Festplatte) - Krankenakten - Prozessdaten eher unkritisch: - Geschäftsgeheimnisse	4P7S - nichts Neues - Datenwert sinkt, kurze Halbwertszeit - Use Case für Geheimdienste	5W7S - kaum Bedrohung aktuell - Daten verlieren an Wert - IT wird als Showstopper gesehen - kaum sichere Verschlüsselung in AT-Industrie - Keine Kultur für Informationssicherheit