A.1 Detaillierte Beschreibung der Fallstudie 1

A.1.1 Modellierte Services, Geschäftsschäden und Klassifikationen

Im Rahmen der Fallstudie wurde der Service „Sendungsverfolgung“ eines Kunden dargestellt, welcher Logistikdienstleister ist. Mit diesem Service kann der aktuelle Lieferstatus und -ort einer anzuliefernden Ware verfolgt werden. Da dem Kunden seine Services schon vor der Beauftragung der IT-Sicherheitsberater bekannt waren, kann die Risikoanalyse im Rahmen einer Sicherheitskonzeption für eine feste Anzahl an Services verwendet werden. Die Fallstudienpartner merkten dabei an, dass die Anzahl der Kunden, welche eine Beauftragung vornehmen ohne die Services benennen zu können, welche es zu betrachten gilt, stetig abnimmt (**Erkenntnis 1.1**).

Für den Service wurden drei mögliche Schäden modelliert (siehe Tabelle 1). Die Modellierung zeigte, dass eine Abgrenzung der Disruption des logistischen Stroms und des Wertstroms problematisch war, da der logistische Strom auch der, oder Teil des Wertstroms sein kann. Die Schadenscharakteristika sind somit nicht trivial abgrenzbar und müssten hinsichtlich ihrer Abgrenzbarkeit untereinander verbessert werden (**Erkenntnis 1.2**).

Die Einschätzung der Schäden auf einer Meta-Skala wurde als problematisch empfunden, da viele Kunden Schäden nicht metrisch exakt, sondern mit Risikoklassen definieren würden. Die Definition der Risikoklassen müsse daher vor der Schadensmodellierung erfolgen (**Erkenntnis 1.3**)

Geschäftsschaden	**Beschreibung**	**Schadenscharakteristika**
Verstoß gegen Complianceanforderungen (1.000.000 €)	Datenschutzanforderungen werden verletzt und personenbezogene Daten gelangen in fremde Hände	Differenzierungsverlust, Verlust von Einkommensquellen, Gewinnreduktion durch Kostenerhöhung
Einschränkung der Serviceverfügbarkeit	Service steht aufgrund von hohen Zugriffszahlen oder DoS Attacken nicht zur Verfügung	Differenzierungsverlust, Verlust von Einkommensquellen, Disruption des logistischen Stroms, Disruption des Wertstroms
Integritätsfehler in der Diensterbringung	Aufgrund mangelnder Datenqualität in Umsystemen werden nicht integere Daten verarbeitet oder erzeugt	Differenzierungsverlust, Disruption des logistischen Stroms, Disruption des Wertstroms

Tabelle 1: Geschäftsschäden des Service Sendungsverfolgung.

Für den Service wurden Risiko-, Schadens- und Wahrscheinlichkeitsklassen mit ihrem jeweiligen Intervall auf der Meta-Skala definiert (siehe Tabelle 2). Diese wurden nun zur Einschätzung des Risikoappetits herangezogen.

Klassenart	**Klasse**	**Intervall**
Risiko	Niedrig	1..25
	Mittel	26..50
	Hoch	51..75
	Sehr hoch	76..100
Schaden	Niedrig	1..33
	Mittel	34..66
	Hoch	67..100
Wahrscheinlichkeit	Gering	1..33
	Mittel	34..66
	Häufig	67..100

Tabelle 2: Risiko-, Schadens- und Wahrscheinlichkeitsklassifikationen der Fallstudie.

Bei der Einschätzung des Risikoappetits wurden zur Kombination der Existenz- und Erfolgswahrscheinlichkeit ein Wert von $\phi_{prob} = 0{,}67$ gewählt, was einem Anteil von 67% der Erfolgswahrscheinlichkeit und 33% der Existenzwahrscheinlichkeit bei der Bestimmung der Eintrittswahrscheinlichkeit entspricht. Zur Bestimmung der Risikoanteile, wurde ein Wert von $\phi_{risk} = 0{,}5$ gewählt, was einem Anteil von 50% der Eintrittswahrscheinlichkeit und 50% der Schadenshöhe entspricht. Somit ist für das Unternehmen die Bestimmung der Eintrittswahrscheinlichkeit auf Grundlage möglicher Angriffsmöglichkeiten etwas wichtiger als die grundlegende Möglichkeit einer Angriffsexistenz. Schadenshöhe und Eintrittswahrscheinlichkeit sind hingegen gleich wichtig.

Hierdurch ergibt sich die in Abbildung 1 dargestellte Matrix zur Ermittlung der Eintrittswahrscheinlichkeit, sowie die in Abbildung 2 dargestellte Matrix zur Ermittlung der Risikoklasse.

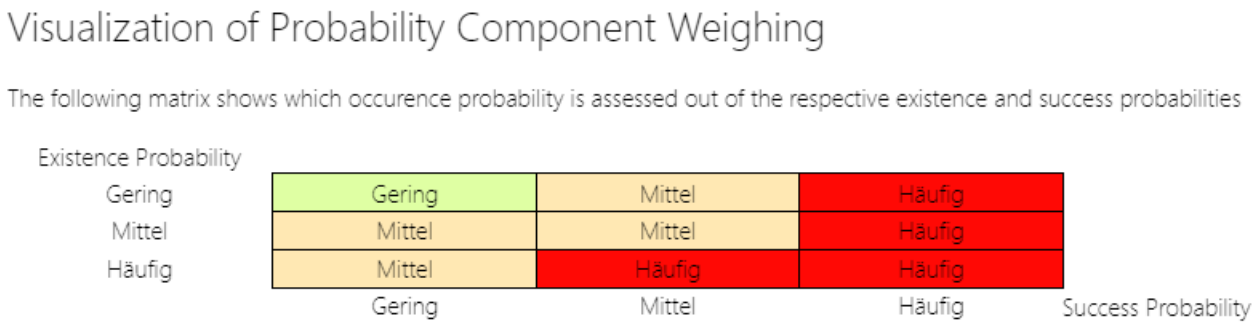

Abbildung 1: Matrix zur Bestimmung der Eintrittswahrscheinlichkeit anhand der Erfolgs- und Eintrittswahrscheinlichkeit.

Die Ermittlung der Werte für ϕ_{prob} und ϕ_{risk} erfolgte mit einem Schieberegler. Hier merkten die Fallstudienteilnehmer an, dass viele ihrer Kunden metrisch denken und daher eine ergänzende Werteingabe für den Schieberegler sinnvoll wäre, sofern ein Kunde einen direkten Wert vorzieht (**Erkenntnis 1.4**).

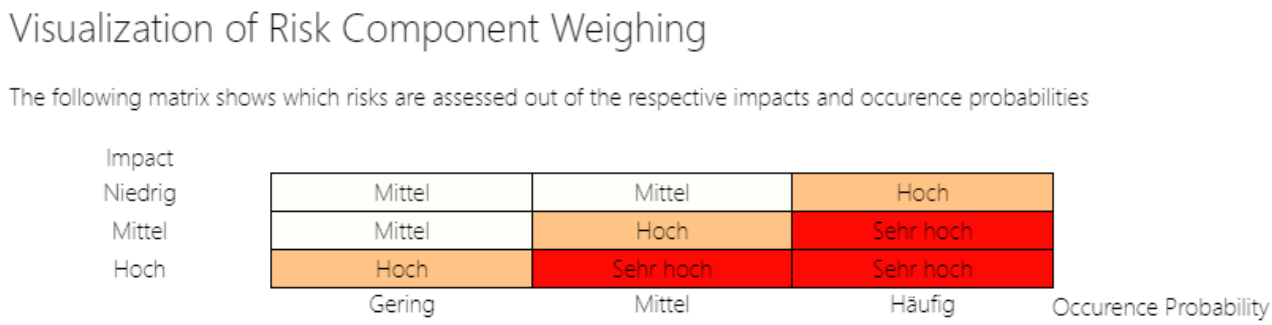

Abbildung 2: Matrix zur Bestimmung der Risikoklasse auf Grundlage des ermittelten Schadens und der Eintrittswahrscheinlichkeit.

Außerdem wurde angemerkt, dass die Matrizengenerierung und die Ermittlung der Klassifikationen hilfreich ist, da sie „...den Kunden schlagartig auf einen Reifegrad katapultiert, von dem viele Kunden nur träumen“. So können hierdurch ohne viel Aufwand Klassen bedarfsorientiert festgelegt werden, denn die Klassendefinition würde ansonsten nur schrittweise erfolgen und über die Zeit um Klassen ergänzt werden (**Erkenntnis 1.5**).

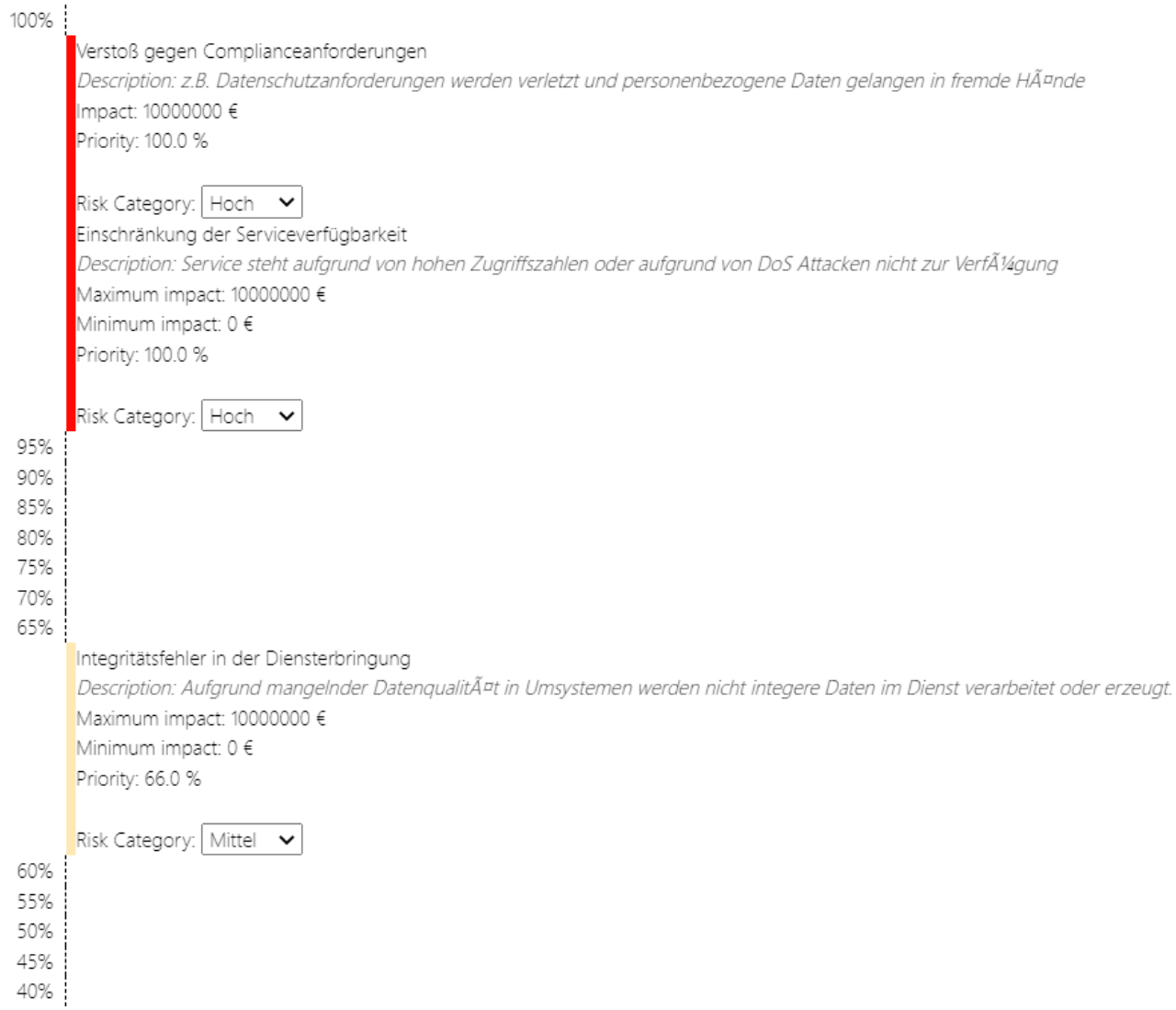

Abbildung 3: Screenshot der ermittelten Schadenspriorisierung der Fallstudie 1.

In der Fallstudie zeigte sich jedoch, dass eine niedrige Risikoklasse bei den gewählten Schadens- und Wahrscheinlichkeitsklassen nicht möglich ist. Dies lag daran, dass es zwar vier verschiedene Risikoklassen gab, wobei die Klasse „Niedrig“ bereits beim Wert 25 auf der Meta-Skala endete. Jedoch endeten die niedrigsten Schadens- und Wahrscheinlichkeitsklassen jeweils bei 33. Per Maximumprinzip leitet die Referenzimplementierung jedoch bei sich überlappenden Klassen, wie dies hier der Fall ist, die höhere vor. Somit konnte die Risikoklasse „Niedrig“ in der Fallstudie nicht erreicht werden (**Erkenntnis 1.6**). Die Fallstudienteilnehmer merkten jedoch an, dass dies unproblematisch sei, da dies durch die Darstellung als Matrix transparent sei und somit in der Adressierung der Risiken berücksichtigt werden könnte.

Die Schadenshöhen wurden durch einen paarweisen Vergleich ermittelt. Dem Schaden „Einschränkung der Serviceverfügbarkeit“ wurde ein maximaler finanzieller Schaden von 1.000.000€ zugewiesen. Der „Integritätsfehler in der Diensterbringung“ wurde ein mittlerer

Schaden zugewiesen. Dies führte zu einem maximalen finanziellen Schaden von 1.000.000€ für diesen (siehe Abbildung 3).

Die Teilnehmer merkten an, dass der paarweise Vergleich und die anschließende Darstellung auf einer Skala die Arbeit der Einschätzung der Schadenshöhe erheblich erleichtert. Die durch den paarweisen Vergleich ermittelte Kategorie kann in der Referenzimplementierung nachträglich angepasst werden, was ebenfalls positiv aufgenommen wurde. Jedoch könnte diese Darstellung insbesondere im Umgang mit sehr vielen Schäden unübersichtlich werden. Insbesondere in Projekten mit 30 Schäden, welche keine Seltenheit darstellen, oder Extremfällen mit 50 Schäden wäre die gewählte Visualisierungsform nicht in der Lage einen übersichtlichen Vergleich zu bieten (**Erkenntnis 1.7**).

A.1.2 Einschätzung der Existenzwahrscheinlichkeit

Zur Einschätzung der Existenzwahrscheinlichkeit wurde zunächst eine Gewichtung der angriffsermöglichenden und -motivierenden Faktoren vorgenommen. Hierzu wurde von der Referenzimplementierung ein Fragebogen generiert, welcher einen paarweisen Vergleich der Faktoren gemäß dem AHP Vorgehen ermöglicht. Der sich dabei ergebende Eigenvektor der paarweisen Vergleichsmatrix führt dabei zu der Gewichtung der angriffsmotivierenden (Abbildung 4) und -ermöglichenden Faktoren (Abbildung 5).

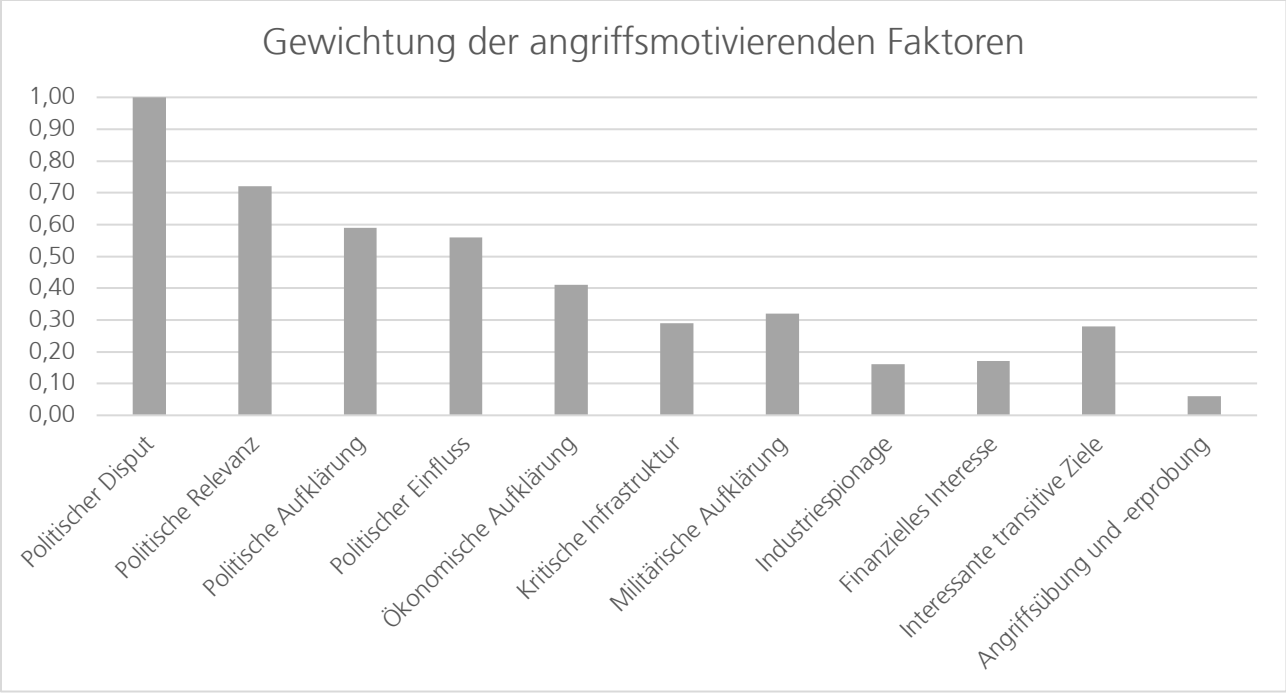

Abbildung 4: Gewichtung der angriffsmotivierenden Faktoren.

Dabei spielt der politische Disput zwischen dem Land des Logistikdienstleisters und Ländern möglicher Angreifer die größte Rolle, gefolgt von politischer Relevanz des Dienstleisters, Angriffe zum Zwecke des politischen Einflusses und der politischen Aufklärung. Angriffe zum Zweck der ökonomischen Aufklarung, kritischer Infrastruktur, militärischer Aufklärung, Industriespionage, finanziellem Interesse, dem Angriff auf interessante transitive Ziele und schließlich die Angriffsübung und -erprobung spielen eine nachgelagerte Rolle.

Bei der Angriffsermöglichung spielen Cloud Services die größte Rolle, gefolgt von Verwundbarkeiten, Exploits, abgeflossenen Credential und abgeflossenen Opferinformationen. Dem folgt Schatten-IT und die Verwundbarkeit gegenüber Spearphishing beziehungsweise Social Engineering. Der physische Supply Chain Zugriff, der physische Organisationszugriff, die Existenz öffentlich zugreifbarer Systeme, 0-Day exploits, sowie kompromittierte laterale Organisationen spielen eine untergeordnete Rolle.

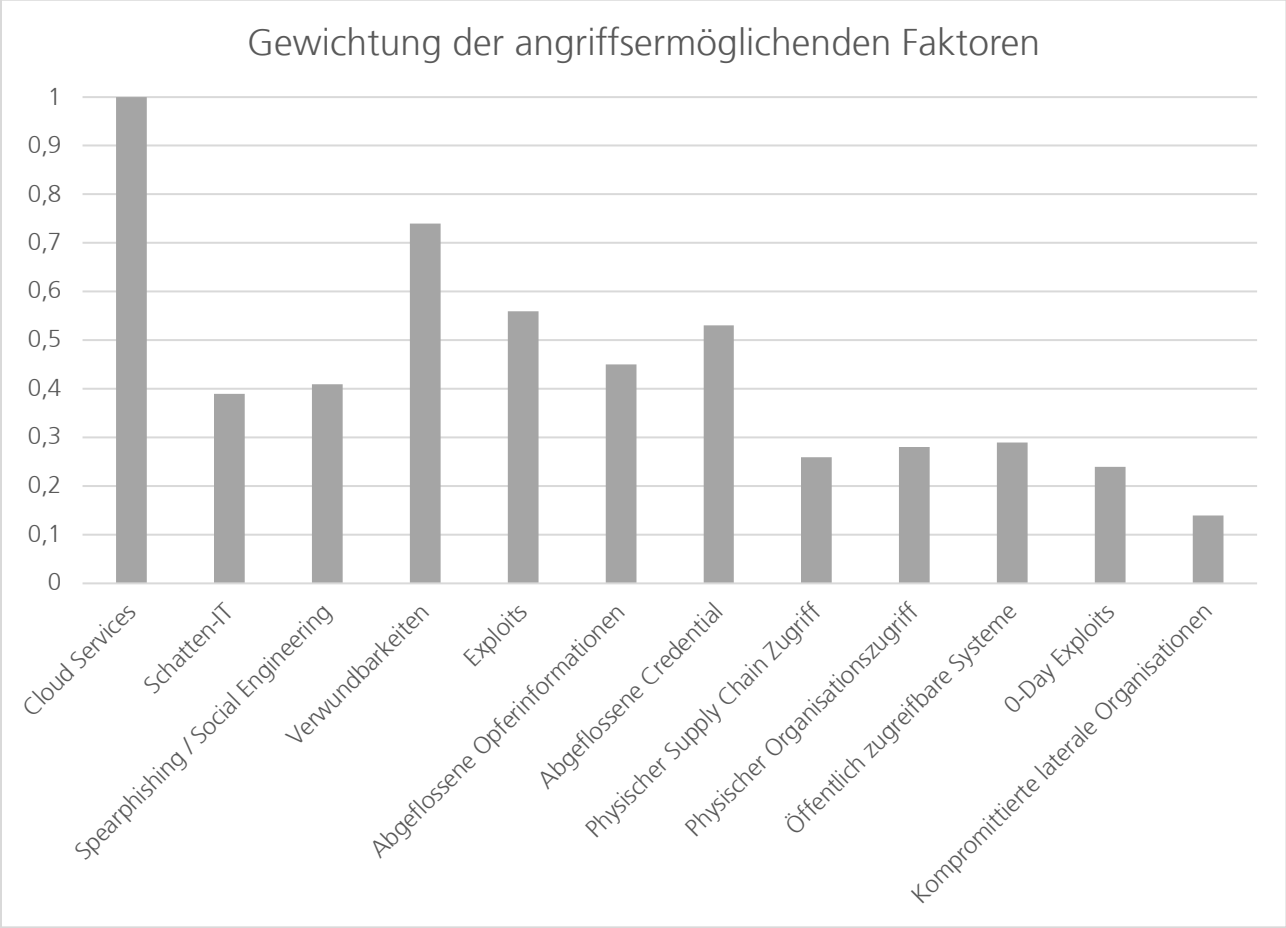

Abbildung 5: Gewichtung der angriffsermöglichenden Faktoren.

Die Gewichtung der Faktoren stellte in der Fallstudie mit einer Stunde Bearbeitungszeit die langwierigste Aufgabe dar. So merkten die Fallstudienpartner an, dass diese Einschätzung einmalig für Organisationen sinnvoll ist, jedoch nicht für Services, sonst würde der Aufwand

schnell erheblich werden. Auch seien die Fragen sehr anstrengend zu beantworten, da fachkundige Expertise notwendig ist. So könnte mehr als ein Meeting zur Beantwortung der Fragen notwendig werden.

Der Bedarf an Fachmännern und der damit einhergehende Aufwand sei jedoch rechtfertigbar, da das Vorgehen methodisch richtig, jedoch umfangreicher sei als das was bisher gemacht würde. So besteht die Gefahr, dass Beantwortende bei der Beantwortung der Fragen abgehängt würden. Diese Einschätzung müsse daher auf jeden Fall begleitet werden.

Erkenntnis 1.8: Die Gewichtung der wahrscheinlichkeitsbedingenden Faktoren muss durch fachkundige Experten des Unternehmens und unter Begleitung eines Beraters durchgeführt

Das Ausfüllen des Fragebogens zur Ermittlung der Existenzwahrscheinlichkeit hingegen, fiel den Teilnehmenden leicht. So konnte ohne großen Aufwand die in Anhang A.1 dargestellten zutreffenden angriffsmotivierenden und -ermöglichenden Faktoren festgestellt werden.

A.1.3 Analyse der IT-Sicherheitsrisiken

Tabelle 3 zeigt die von den Fallstudienpartnern gewählten analyserelevanten Komponenten. Bei der Bestimmung der Komponenten wurde angemerkt, dass keine Unterscheidung der Cloud Computing Komponenten dahingehend vorhanden ist, ob diese intern oder extern sind. Weiterhin wurde angemerkt, dass keine Auswahlmöglichkeit für Platform-as-a-Service (PaaS) Komponenten existiert. Schließlich seien auch nicht alle Cloud Plattformen in der Auflistung vorhanden, sondern lediglich Office365, AWS und der Google Workspace. Diese Auswahlmöglichkeiten wären jedoch relevant, da der Cloud Einsatzung bei Kunden in der Regel hybrid sei.

Erkenntnis 1.9: Die Auflistung der Cloud Komponenten, insbesondere die Consumer Cloud Lösungen sollte vollständig sein, da viele Kunden einen hybriden Cloud Einsatz nutzen.

So gäbe es Kunden, die ihre Infrastruktur in IaaS migrieren und hierbei Azure DevOps zur Entwicklung verwenden. Das Deployment der Anwendungen würde jedoch im Kundennetzwerk (On-Premise) erfolgen. Ein hybrider Einsatz der Cloud Lösungen sollte bei der Auswahl der Cloud Komponenten daher ergänzt werden.

Erkenntnis 1.10: Der hybride Cloud Einsatz sollte bei der Auswahl der analyserelevanten Komponenten auswählbar sein.

In der Auswahl der weiteren Komponenten war häufig unklar ob es sich um direkt auf den Service bezogene Komponenten oder auch um indirekte handeln sollte. So würden

beispielsweise Benachrichtigungsdienste zur Benachrichtigung von Administratoren in Sicherheitskonzepten in der Regel ausgeblendet. Nach dieser Logik müssten daher beispielsweise keine SMS oder E-Mail Kommunikation in der Analyse berücksichtigt werden.

Erkenntnis 1.11: Die Bestimmung analyserelevanter Komponenten sollte eine Angabe über einen direkten, oder transitiven (indirekten) Bezug der Komponente zum Service beinhalten.

Dies zeigt, dass die Differenzierungsproblematik, welche im Ansatz durch die Wahl von Services als Analysesubjekt adressiert wurde (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**), in der Auswahl der analyserelevanten Komponenten wieder auftritt. Jedoch ist diese nun auf den Service bezogen und daher in geringerer Komplexität lösbar, als dies eine Differenzierung der Güter eines Unternehmens oder Unternehmensteils wäre.

Erkenntnis 1.12: Die Differenzierungsproblematik tritt zwar in der Bestimmung der analyserelevanten Komponenten wieder auf, jedoch in einer beherrschbaren Komplexität.

Schließlich wurden doppeldeutige Komponentennamen angemerkt. So wäre bei Messaging Services unklar, ob dies auch MQTT Systeme miteinschließe und Third Party könne auch als Third Party Library gedeutet werden.

Erkenntnis 1.13: Die dargestellten Komponentennamen sind teilweise doppeldeutig und sollten konkretisiert werden.

Komponentenart	**Vorhandende Komponenten**
Cloud Computing	IaaS, SaaS
Kollaboration	Menschen, E-Mail Kommunikation, SMS, Messaging Services, E-Mail Clients, Passwort manager, Office, Web Browser, Confluence, 2-Faktor Authentifizierung, Softwareentwicklungstools
Virtualisierung	Container
Betriebssysteme	Windows, Linux
Infrastruktur	IT Netzwerk, Active Directory, SAML basierende Authentifizierung, Shared Storage Locations, Netzwerk Shares, Fileshares, Software Deployment Tool, Repositories, Information Repositories, Internal Webpage, Webpage, Webanwendung, Datenbank, SSH, RDP, Layer 3 Routing

Tabelle 3 Analyserelevante Komponenten der Fallstudie 1

Bei der Bestimmung des Zutreffens beziehungsweise Nicht-Zutreffens der Maßnahmen und der Implementierungsausnahmen (siehe Anhang A.3), wurde angemerkt, dass die Implementierungsausnahmen erst eingeblendet werden sollten, wenn die Checkbox, die indiziert, dass Ausnahmen bestehen nicht ausgewählt wurde (siehe Abbildung 6).

Erkenntnis 1.14: Der Maßnahmereport sollte einen schrittweisen Prozess erzwingen, indem die Implementierungsausnahmen erst eingeblendet werden, wenn vom Benutzenden angezeigt wird, dass Ausnahmen existieren.

Darüber hinaus sei eine Kommentierungsfunktion notwendig, da hierdurch die Auditrelevanz des Maßnahmenreports ermöglicht werden könnte. So könnte an dieser Stelle beispielsweise vermerkt werden ob die Maßnahme bereits implementiert sei, wann diese implementiert wurde, oder ob diese in Planung sei.

Erkenntnis 1.15: Der Maßnahmereport sollte die Möglichkeit zur Kommentierung der Entscheidung über Zutreffen, Nicht-Zutreffen und Implementierungsausnahmen beinhalten um eine Auditierbarkeit der Services zu ermöglichen.

Schließlich wurde in der Auswahl der Implementierungsausnahmen eine Verständnisproblematik durch die Formulierung der Ausnahmenauswahl festgestellt. So klinge die aktuelle Bezeichnung der Checkbox für eine Implementierungsausnahme („Control does not apply to this threat“) danach, dass eine Bedrohung nicht relevant sei. Besser sei ein Satz wie „Control does not adress this threat“.

Der Checklisten-Ansatz des Maßnahmenreports wurde sehr positiv aufgenommen, da er eine vollständige Betrachtung der Maßnahmen ermögliche. Hier sei, laut Fallstudienpartner ohne eine Checkliste die Gefahr sehr groß etwas zu vergessen. Dies sei in der Referenzimplementierung nicht der Fall.

Erkenntnis 1.16: Der Checklistenansatz des Maßnahmenreports verhindert, dass Maßnahmen vergessen oder übersehen werden und bietet eine vollständige Betrachtung der Maßnahmen.

Allerdings wurde angemerkt, dass die Detaillierung des Maßnahmenreports je nach Person schwer zu beantwortende Fragen beinhalten würde. So muss bei der Erstellung des Maßnahmenreports Wissen zum Vorhandensein beziehungsweise Nicht-Vorhandensein, technischer, organisatorischer und technisch-organisatorischer Maßnahmen vorliegen. Zusätzlich müssen Beantwortende über, von einer Maßnahmenimplementierung adressierte beziehungsweise nicht adressierte Bedrohungen informiert sein. Daher wurde angemerkt, dass es sinnvoll wäre, die Erstellung des Maßnahmenreports unabhängig zu ermöglichen, so dass unterschiedliche Teile des Reports von unterschiedlichen Personen ausgefüllt werden könnten.

Erkenntnis 1.17: Die Erstellung des Maßnahmenreports sollte personenunabhängig möglich sein, so dass unterschiedliche Teile des Reports von unterschiedlichen Personen beantwortet werden

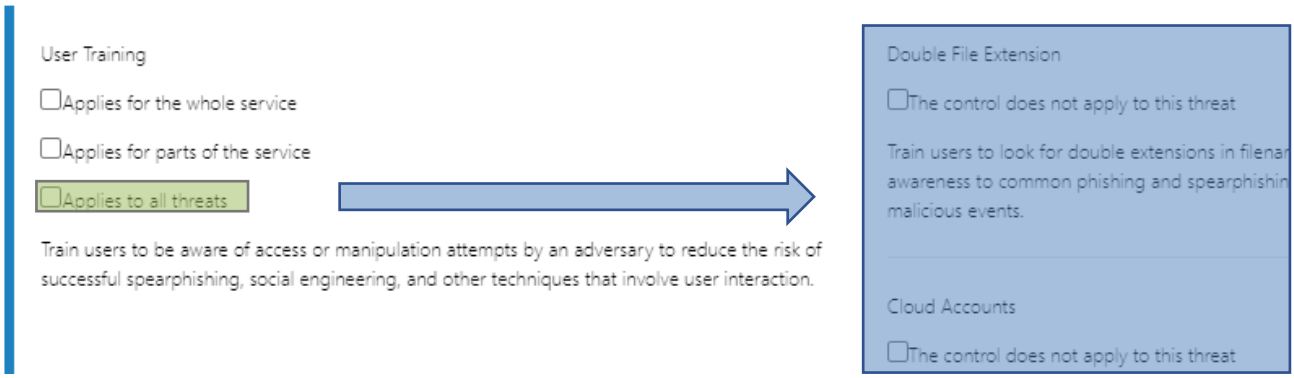

Abbildung 6: Sicht des Control Reports mit der Frage nach der Existenz von Ausnahmen der Maßnahmenimplementierung (grün) und der auszuwählenden Ausnahmen (blau).

Zur Erstellung des Maßnahmenreports wurden 50 Minuten Zeitaufwand benötigt. Hierbei wurde angemerkt, dass bei Zeitaufwänden von annähernd einer Stunde, mehr Erklärung und eine schrittweise Präsentation notwendig sei.

Erkenntnis 1.18: Die Erstellung des Maßnahmenreports sollte schrittweise angeleitet werden.

Darüber hinaus könne der Maßnahmenreport nur unter Anleitung ausgefüllt werden. So seien Kompetenzen der IT-Sicherheit, insbesondere der Abdeckung der Maßnahmen für bestimmte Bedrohungen genauso notwendig, wie das Wissen über Vorhandensein und Nicht-Vorhandensein der Maßnahmen.

Erkenntnis 1.19: Zur Erstellung des Maßnahmenreports sind Personen mit Wissen über die Implementierung der Maßnahmen, sowie Personen mit Wissen zur Bedrohungsadressierung der Maßnahmen notwendig.

Abschließend stellten die Fallstudienpartner fest, dass das Vorgehen zur Risikoanalyse bis zu diesem Schritt strukturiert und vergleichbar mit dem Ansatz STRIDE ist. Jedoch ist STRIDE mit einem höheren Aufwand verbunden, während die Ergebnisse des Verfahrens genauso gut seien.

Erkenntnis 1.20: Die Qualität der Verfahrensergebnisse ist mit STRIDE vergleichbar, jedoch sind die Kosten des Verfahrens geringer als bei einer Analyse mit STRIDE.

Auf Grundlage der zutreffenden beziehungsweise nicht-zutreffenden Maßnahmen konnte ein Bedrohungsbild ermittelt werden, welches zeigte, dass nicht vollständig adressierte Bedrohungen erst in den Kill Chain Phasen Defense Evasion, Persistence und Command & Control vorhanden sind. Dies bedeutet, dass Angriffe eine ursprünglich geringe Erfolgswahrscheinlichkeit haben. Sofern jedoch eingehende Bedrohungen der Kill Chain Phase Initial Access erfolgreich wären, könnten Erkennungs- und Abwehrmechanismen umgangen,

sowie ein langfristiger Zugriff und Fernsteuerungskanäle mit mittlerer Erfolgswahrscheinlichkeit etabliert werden (siehe Tabelle 4).

Kill-Chain Phase	**Max(P‘)**	**Nicht vollständig adressierte Bedrohungen**
Defense Evasion	Mittel	Traffic Signaling (Mittel)
Persistence	Mittel	Web Shell (Mittel), Traffic Signaling (Mittel)
Command & Control	Mittel	Multi-hop Proxy (Mittel), External Proxy (Mittel), Internal Proxy (Mittel), One-Way Communication (Mittel), Bidirectional Communication (Mittel), Dead Drop Resolver (Mittel), Traffic Signaling (Mittel), Multi-Stage Channels (Mittel), Web Service (Mittel), Fallback Channels (Mittel)

Tabelle 4: Nicht vollständig adressierte Bedrohungen und deren Erfolgswahrscheinlichkeit der Fallstudie 1.

Der Anteil der Bedrohungen, die durch andere ermittelte Bedrohungen bedingt sind (pivotisierte Bedrohungen) betrug zusätzlich 52,59%. Gemeinsam mit der Beobachtung, dass nicht vollständig adressierte Bedrohungen erst in späteren Kill-Chain Phasen auffindbar sind, spricht dies für eine zusätzliche Betrachtung des pivotisierten Bedrohungsbilds (siehe Tabelle 5).

Kill-Chain Phase	**Max(P‘)**	**Nicht vollständig adressierte Bedrohungen**
Defense Evasion	Mittel	Traffic Signaling (Mittel)
Persistence	Mittel	Traffic Signaling (Mittel)
Command & Control	Mittel	Traffic Signaling (Mittel)

Tabelle 5: Maximale Erfolgswahrscheinlichkeit der pivotisierten Bedrohungen der Fallstudie 1.

Die ermittelten, nicht vollständig adressierten Bedrohungen der Tabelle 5 waren jedoch nicht Teil der pivotisierten Bedrohungen. Somit ergibt sich für pivotisierte Bedrohungen eine Erfolgswahrscheinlichkeit von Niedrig, während diese im nicht pivotisierten Fall Mittel beträgt. Gemeinsam mit der ermittelten Existenzwahrscheinlichkeit ergeben sich somit die Risikomatrizen für die maximale (Abbildung 7) und pivotisierte Eintrittswahrscheinlichkeit (Abbildung 8).

	Eintrittswahrscheinlichkeit		
Schaden	**Gering**	**Mittel**	**Häufig**
Niedrig	Mittel	Mittel	Hoch
Mittel	Mittel	**Hoch**	Sehr hoch
Hoch	Hoch	**Sehr hoch**	Sehr hoch

Abbildung 7: Risikomatrix der Analyse mit maximaler Eintrittswahrscheinlichkeit der Fallstudie 1.

	Eintrittswahrscheinlichkeit		
Schaden	**Gering**	**Mittel**	**Häufig**
Niedrig	Mittel	Mittel	Hoch
Mittel	**Mittel**	Hoch	Sehr hoch
Hoch	**Hoch**	Sehr hoch	Sehr hoch

Abbildung 8: Risikomatrix der Analyse mit pivotisierter Eintrittswahrscheinlichkeit der Fallstudie 1.

Im Risikoreport wurde die Möglichkeit zur Pivotisierung positiv angemerkt. Dies würde Kunden ermöglichen eine zusätzliche Abmilderung von Risiken durch die Komplexität der risikomaterialisierenden Angriffe zu berücksichtigen, was je nach Risikoappetit der Kunden sinnvoll sei. Jedoch sei die Darstellung der pivotisierten Bedrohungen herausfordernd, da sehr viele Bedrohungen durch eine bedingt sein können. So sollte eine Möglichkeit gefunden werden, um die nicht relevanten Pfeile besser auszublenden.

Erkenntnis 1.21: Nicht relevante Verweise auf bedingte Bedrohungen (Pfeile) sollten bei der Betrachtung pivotisierter Bedrohungen besser ausgeblendet werden.

Auch der Vorschlag der Gegenmaßnahmen wurde sehr positiv aufgenommen. So bietet die Darstellung der Gegenmaßnahmen eine Übersicht darüber, welche alternativen Adressierungsmöglichkeiten für eine Bedrohung unter Berücksichtigung möglicher Veränderungen der angriffsermöglichenden Faktoren und der sich hieraus ergebenden Erfolgswahrscheinlichkeit der Bedrohung bekannt sind (siehe Abbildung 9). Diese Darstellung würde in der Ableitung der Gegenmaßnahmen erhebliche Hilfestellung leisten.

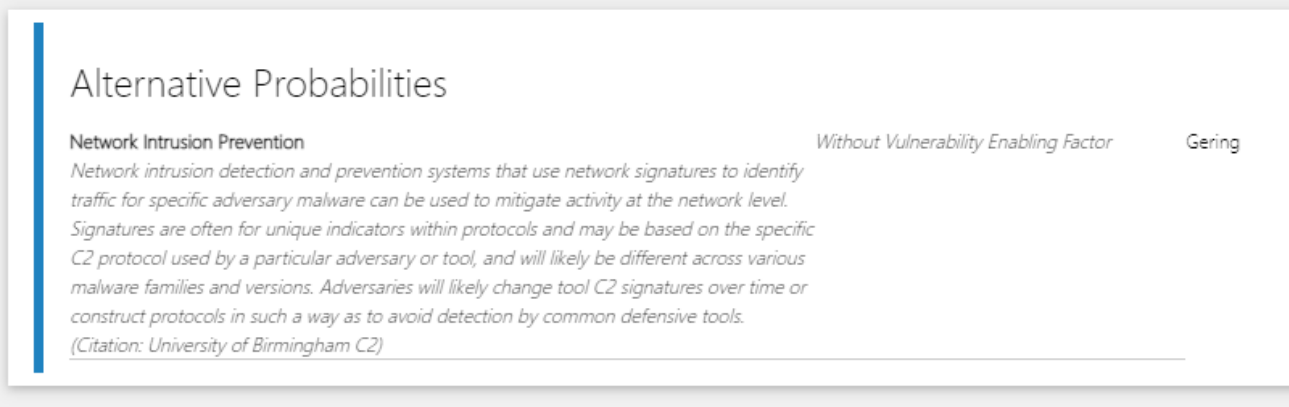

Abbildung 9: Beispiel einer vorgeschlagenen Gegenmaßnahme der Fallstudie 1. Die Gegenmaßnahme (linke Spalte), wird gemeinsam mit zutreffenden angriffsermöglichenden Faktoren (mittige Spalte) und der sich ergebenden Erfolgswahrscheinlichkeit (rechte Spalte) dargestellt.

Die zusätzliche Ermittlung der relevanten Angreifer sei hingegen nicht sehr hilfreich, da der Detaillierungsgrad zu hoch sei. Es könne zwar unterstützend zur Maßnahmenplanung genutzt werden, sei jedoch keine unbedingt notwendige Information. Die ermittelte relevante Malware sei hingegen hilfreicher, da Kunden hiermit überprüfen könnten ob auf eine bestimmte Malware gescannt werden müsse. Dies sei insbesondere für die Chief Information Officer (CIO) und Chief Information Security Officer (CISO) Rollen relevant.

Erkenntnis 1.21: Die Auflistung relevanter Angreifer ist für Unternehmen nicht so relevant, wie die Auflistung relevanter Malware, die insbesondere für CISO und CIO von Interesse ist.

A.2 Angriffsmotivierende und -ermöglichende Faktoren in Fallstudie 1

Angriffsmotivierender Faktor	**Erfüllt?**		**Angriffsermöglichender Faktor**	**Erfüllt?**
Politischer Disput			Cloud Services	√
Politische Relevanz			Schatten-IT	√
Politische Aufklärung			Spearphishing / Social Engineering	√
Politischer Einfluss	√		Verwundbarkeiten	√
Ökonomische Aufklärung	√		Exploits	√
Kritische Infrastruktur	√		Abgeflossene Opferinformationen	√
Militärische Aufklärung			Abgeflossene Credential	√
Industriespionage	√		Physischer Supply Chain Zugriff	√
Finanzielles Interesse	√		Physischer Organisationszugriff	
Interessante transitive Ziele			Öffentlich zugreifbare Systeme	√
Angriffsübung und -erprobung	√		0-Day Exploits	√
			Kompromittierte laterale Organisationen	√

Tabelle 6: Ermitteltes Zutreffen der angriffsermöglichenden und -motivierenden Faktoren.

A.3 Zutreffende Maßnahmen der Fallstudie 1

Maßnahme		**Ausnahmen**
Data Loss Prevention	✓	Keine
Software Configuration	O	Blockieren von Angriffsindikatoren, Installieren von Root Zertifikaten, Umgehen von Vertrauenskontrollen
Data Backup	✓	Keine
User Account Control	O	Übernehmen des Ausführungsablaufs
Update Software	O	Pre-OS Boot, Firmware Corruption, Supply Chain Kompromittierung
Exploit Protection	✓	Keine
Antivirus/Antimalware	✓	Keine
Application Isolation and Sandboxing	✓	Keine
Application Developer Guidance	O	Übernehmen des Ausführungsablaufs
Audit	O	Übernehmen des Ausführungsablaufs
Boot Integrity	O	Firmware Corruption
Code Signing	×	
Restrict Library Loading	×	
Credential Access Protection	✓	Keine
Disable or Remove Feature or Program	O	Downgrade Attacke, ARP Cache Poisoning, SSH Authorized Keys, Adversary-in-the-Middle, Traffic Signaling, Trusted Developer Utilities Proxy Execution, Command and Scripting Interpreter
Encrypt Sensitive Information	O	Manipulation gespeichert Daten, Datenmanipulation, Email Forwarding Regeln, Stehlen oder Fälschen von Kerberos Tickets, Kerberoasting, Löschen der Linux oder Mac System Logs, Entfernen von Angriffsindikatoren auf dem Host
Behavior Prevention on Endpoint	✓	Keine
Environment Variable Permissions	✓	Keine
Execution Prevention	✓	Keine
Filter Network Traffic	O	ARP Cache Poisoning, Adversary-in-the-Middle
Account Use Policies	✓	Keine
Limit Access to Resource over Network	O	ARP Cache Poisoning, Adversary-in-the-Middle
Limit Hardware Installation	✓	Keine
Limit Software Installation	✓	Keine
Multi-factor Authentication	✓	Keine
Network Intrusion Prevention	✓	Keine
Network Segmentation	✓	Keine
Remote Data Storage	O	Software Deployment Tools

Maßnahme		**Ausnahmen**
Operating System Configuration	✓	Keine
Password Policies	✓	Keine
Privileged Account Management	✓	Keine
Privileged Process Integrity	✓	Keine
Restrict Registry Permissions	✓	Keine
Restrict File and Directory Permissions	✓	Keine
Restrict Web-Based Content	✓	Keine
SSL/TLS Inspection	✓	Keine
Threat Intelligence Program	✗	
User Account Management	✓	Keine
User Training	✓	Keine
Vulnerability Scanning	✓	Keine
Active Directory Configuration	O	SID-History Injection, Software Deployment Tools
✓ Trifft zu O Trifft mit Ausnahmen zu ✗ Trifft nicht zu		

Tabelle 7: Zutreffen der Maßnahmen und deren Implementierungsausnahmen in Fallstudie 1.

A.4 Ausgangsbefragung der Fallstudie 1

Ist das Verfahren wiederholbar?

Ja, das ist es.

Sehen Sie Einschränkungen in der Wiederholbarkeit?

Methodisch ist das Verfahren auf jeden Fall wiederholbar und hat einen entsprechenden Reifegrad. Jedoch ist es in der Implementierung des Verfahrens ein Aufwand die ganzen Detailfragen durchzugehen.

Was hilfreich wäre ist, wenn die Beantwortung der Fragen bei einer Neuevaluierung gespeichert würden. Wenn dem so ist, würde ich auch unterstellen, dass das technisch gut wiederholbar ist.

Nice-to-have wäre, wenn man überprüfen könnte, wie sich die Risiken in verschiedenen Bedrohungsmodellen über die Zeit verändern.

Ist der Anbahnungs- und Durchführungsaufwand ihrer Meinung nach beherrschbar?

Der Aufwand zur Anbahnung ist grundsätzlich beherrschbar. Ich sehe die Hürde aber noch im Zusammenspiel. Ich brauche auf der einen Seite jemanden, der für den Service auskunftsfähig ist und auf der anderen Seite jemanden der fachlich weiß, wie Threat Modellierung funktioniert. Beide müssen im gleichen Zeitfenster zusammentreffen.

Das muss man aber immer machen, wenn ich eine Risikoanalyse machen möchte. Hier halte ich das aber für sehr strukturiert, weil man an die Hand gennommen wird und nicht bewerten muss, welche Threats die gängigen sind.

Also insofern ja, halte ich für realistisch, dass das hier ein effizienter Weg ist.

Der Durchführungsaufwand des Verfahrens ist schon noch hoch, aber im Verlgeich zu anderen Methoden deutlich reduziert. Bei anderen Methoden muss ich mich mit dem Systemaufbau auseinandersetzen, etc. Hier kann ich das auf techhnische Plattformen einschränken und erhalte eine Vorselektion. Ich muss also nicht die ganze Welt mappen und dann erhalte ich die entsprechenden Threats. Also hoch, aber im Vergleich zu anderen deutlich reduziert.

Wir haben hier jetzt 2x2 Stunden benötigt, um das durchzuexerzieren. Bei einem Kunden ist das wahrscheinlich dann mit Faktor 2 zu berechnen, also ein kompletter Arbeitstag pro Teilnehmer.

Wie verhält sich der Anbahnungs- und Durchführungsaufwand relativ zu vergangenen Analysen?

Ein Personentag pro Teilnehmer ist immer noch ein vertretbarer Aufwand. Wenn wir das gleiche mit STRIDE gemacht hätten, wären es vermutlich 3-5 Tage für die reine Analyse, plus

der Aufwand zur Überführung in den formalen Rahmen beim Kunden. Also ist das Verfahren mit Faktor 2-3 besser als STRIDE.

Kann das Verfahren messbare und kommunizierbare Risikoanalysen bereitstellen?

Ja. Sowohl, als auch.

Messbar ist es definitiv, weil das ganze ja einer Systematik folgt. Vergleichbar ist es auch. Die Frage der Kommunizierbarkeit hängt auch an der Frage, an wen man es kommuniziert. Man hat ja zwei Kommunikationsebenen, wenn man eine Risikoanalyse machen möchte.

Einmal möchte ich den Risikoeigner informieren, was er denn im Portfolio hat. Da kann man hier den Haken dran machen.

Die zweite Ebene ist, dass ich die Mitigation oder das Management operativ steuern möchte, also bestimme welche Maßnahmen definiert und implementiert werden. Hier braucht es ein Steuerungstool. Da wäre es eher ein Fragezeichen, da die Implementierung nur eine Ebene betrachtet, nämlich den Stand jetzt und eben nicht betrachtet, was der Stand der Zukunft ist.

Kommunikation zur Darstellung von Investitionsdringlichkeiten ist damit aber möglich. Ich kann zum Risikoeigner gehen und sagen. „Du hast hier noch viele Restrisiken mit einer hohen Wahrscheinlichkeit, lass uns mal die Tätigkeiten unternehmen, damit du das mitigieren kannst“. Es betrachtet aber noch nicht die Erfolgsgeschichte des CISO oder des IT-Leiters. In der zweiten Linie ist es dann immer noch die Aufgabe des CISO oder des Risk Managers hieraus eine Entscheidungsgrundlage zu bauen. Insofern ist die Implementierung für das Management der Risiken ein notwendiges, aber kein hinreichendes Instrument.

Wie verhält sich die Mess- und Kommunizierbarkeit relativ zu vergangenen Analysen?

Vorteil gegenüber vergangenen Analysen ist, dass es bestehende Best Practices nutzt und auf einem aktuellen Datenbestand aufbaut, wo man eben nicht Gefahr läuft, dass man was vergessen hat. Sondern man nutzt ja eigentlich das was schon am Markt existiert und etabliert ist und verknüpft das geschickt. Das spart dadurch tendentiell Zeit.

Somit führt das Verfahren natürlich auch zu Ergebnissen, die tendentiell besser einzuschätzen sind.

Bei STRIDE hängt es sehr stark von der Person ab, die die Analyse durchführt. Der eine baut da ein richtig großes Bild, der andere baut ein richtig kleines Bild. Das Verfahren hier ist hingegen ein personenunabhängiger, systematischer Ansatz.

Reduziert das Verfahren die Varianz der analysierten Risiken?

Die Varianz sollte eigentlich deutlich kleiner sein als mit bestehenden Methoden. Es sollten bei wiederholter Durchführung Ergebnisse herauskommen, die sehr ähnlich sind.

Am Anfang ist erklärungsbedürftig was Eintrittswahrscheinlichkeit von Erfolgswahrscheinlichkeit unterscheidet. Wenn ich das aber mal verstanden habe, sollte die Erfolgswahrscheinlichkeit unter den Tatbeständen, die ich untersuche, eine niedrige Varianz aufweisen. Bei der gleichen Applikation sollte auch die gleiche Erfolgswahrscheinlichkeit herauskommen. Je mehr Bewusstsein über eine Bedrohung da ist, desto höher kann auch der Erfolg eingeschätzt werden.

Wie verhält sich dies relativ zu vergangenen Analysen?

Die Varianz sollte kleiner sein, weil die Personenabhängigkeit nicht so stark ist.

Würden Sie das Verfahren weiter nutzen?

Würden wir weiter nutzen. Wir möchten es tatsächlich auch gerne in der Praxis ausprobieren. Eben aus den genannten Gründen. Weil die Personenabhängigkeit reduziert wird. Ich brauche also nicht einen Experten, der schon 20 Jahre Berufserfahrung hat, sondern das kann auch jemand machen der technisch fit ist, aber noch nicht ganz viel Praxiserfahrung in der Risikoanalyse gemacht hat.

Und es ist eben reproduzierbar. Unter gleichen Annahmen kommen die gleichen Ergebnisse heraus und ich kann das auch nutzen um die gleichen Analysen durchzuführen.

A.5 Detaillierte Beschreibung der Fallstudie 2

A.5.1 Modellierter Service, Geschäftsschäden und Klassifikationen

Der Service, welcher zur Erprobung genutzt wird ist die „Produktauslieferung“, bei welcher ein Produkt an einen Business-to-Consumer (B2C) Kunden übergeben wird. Für diesen wurden die in Tabelle 8 dargestellten Schäden modelliert. Hierbei gab es seitens der Fallstudienpartner keine Anmerkungen. Insbesondere die Schadenscharakteristika konnten ohne Rückfragen zugewiesen werden.

Geschäftsschaden	**Beschreibung**	**Schadenscharakteristika**
Ausfall der Webseite	Webseite steht nicht zur Verfügung. Kundenbestellungen können nicht durchgeführt werden.	Verlust von Einkommensquellen, Disruption des Wertfluss
Customer Data Loss	Kundendaten werden geleaked	Differenzierungserlust, Verlust von Einkommensquellen, Gewinnreduktion durch Kostenerhöhung
Broken Integrity of customer data	Verfälschung der Dateneingabe von Kundendaten	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Stroms

Tabelle 8: Modellierte Schäden und zugewiesene Schadenscharakteristika der Fallstudie 2.

Die modellierten Schäden machen jedoch deutlich, dass der Begriff des Geschäftsschadens unklar ist. So wird im Schaden „Ausfall der Webseite“ zwar die direkte Konsequenz des Schadens für die Wertschöpfung des Unternehmens deutlich, jedoch ist der Schaden wie ein auf die IT- oder die IT-Sicherheit bezogener Schaden bezeichnet. Bei den anderen beiden Schäden ist jedoch aus der Beschreibung und aus der Benennung des Schadens keine direkte Konsequenz für das Unternehmen erkennbar. Lediglich die Schadenscharakteristika bieten eine abstrakte Beschreibung des möglichen Schadens für das Unternehmen.

Dies deutet daraufhin, dass der Ausgangspunkt der Analyse, welcher im Verfahren in den zu modellierenden Geschäftsschäden liegt, für die Anwendung durch IT-Sicherheitsexperten herausfordernd sein kann. Ein möglicher Grund hierfür könnte darin liegen, dass die Verfahren des Stand der Technik mit auf die IT oder IT-Sicherheit bezogenen Schäden arbeiten.

Erkenntnis 2.1: Die Modellierung von Geschäftsschäden kann für IT-Sicherheitsexperten herausfordernd sein, während die Zuweisung der Schadenscharakteristika kein Problem darstellte.

Für diesen Service wurden die in Tabelle 9 dargestellten Klassifikationen definiert. Der Fallstudienpartner merkte an, dass die Definition von Risiken in der Regel eine Ebene tiefer, also bezogen auf die IT oder die IT-Sicherheit stattfindet. Es sei herausfordernd die korrekte

Tiefe der Risikodefinition zu wählen, da die Ebene des Risk Statements in der Implementierung nicht angegeben sei. Die Flughöhe des Risikos habe dabei erheblichen Einfluss auf den Risikoappetit. So sei dieser Appetit in der Regel höher, wenn zufällige Ereignisse betrachtet würden und niedriger, wenn es sich bei einem Vorfall um eine technisch herbeigeführte Ursache handelt.

Klassenart	**Klasse**	**Intervall**
Risiko	Very Low	0..15
	Low	16..32
	Medium	33..48
	High	49..68
	Critical	69..88
	No Go	89..100
Schaden	Very Low	0..15
	Low	16..42
	Medium	43..62
	High	63..100
Wahrscheinlichkeit	Very Low	0..15
	Low	16..42
	Medium	43..62
	High	63..100

Tabelle 9: Definition der Klassifikationen für Risiken, Schäden und Wahrscheinlichkeiten.

Dabei können die Klassifikationen für Risiken, Schäden und Wahrscheinlichkeiten je nach Unternehmensebene unterschiedlich sein. Der Ausgangspunkt des Verfahrens kann hiermit jedoch nicht umgehen, da das Klassifikationen zwar für Geschäftsrisiken und Geschäftsschäden vorgenommen werden sollen, auf der anderen Seite jedoch einen reinen, auf intentionale Herbeiführung durch Angreifende bezogenen IT-Sicherheitsbegriff verwendet. Die Definition eines Risikostatements ist hierdurch erheblich erschwert.

Erkenntnis 2.2: Klassifikationen für Risiken, Wahrscheinlichkeiten und Schäden können in Unternehmen über verschiedene Unternehmensebenen hinweg heterogen sein. Dies kollidiert jedoch mit dem geschäftsbezogenenen Ausgangspunkt des Verfahrens und dem Fokus auf Angriffe der IT-Sicherheit.

Ohne die Definition eines Risikostatements sei jedoch eine genaue Betrachtung des Risikoappetits erschwert. Daher muss dieses unbedingt am Anfang definiert werden.
Die Implementierung der Risikoklassendefinition wurde hingegen sehr positiv aufgenommen, da sie eine Definition der Klassifikationen mit Basisinformationen ermögliche. So würden die

Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht mit Schutzbedarfen arbeiten, welche jedoch in der Definition viele zu berücksichtigende Aspekte benötigen. Die Reduktion der Klassendefinition auf Menge der Klassen, Benennung und deren Verteilung auf der Meta-Skala hingegen würde unnötige Informationen vermeiden und eine fokussierte Definition der Klassifizierungen ermöglichen.

Erkenntnis 2.3: Die Implementierung der Klassifizierungsdefinition für Risiken, Wahrscheinlichkeiten und Schäden erlaubt eine einfache und fokussierte Definition, da unnötige Informationen vermieden werden.

Darüber hinaus bemerkten die Fallstudienpartner, dass die Definition der Schadensklassen noch einen weiteren Schritt benötigt. So muss in Unternehmen der Finanzbranche ein Wert hinter den Schadenskategorien stehen, welcher für Rücklagen genutzt werden kann, da dies beispielsweise nach Basel 3 notwendig ist. Für ein kleines Unternehmen würde die vorhandene Definition der Risikoklassen gut funktionieren, da diese nicht erforderten, dass alle Schadenshöhen quantifizierbar sind. Aber in Großkonzernen wird ein monetärer Zusammenhang mit den Schadensklassen benötigt.

Erkenntnis 2.4: Die Definition der Schadensklassifikationen muss eine Quantifizierung der Schadensklassen zur Ermöglichung der Rücklagenbestimmung enthalten.

Die Einstellungen des Risikoappetits zeigten für die Kombination von Existenz- und Erfolgswahrscheinlichkeit zur Eintrittswahrscheinlichkeit (siehe Abbildung 10) eine stärkere Priorisierung der Existenzwahrscheinlichkeit.

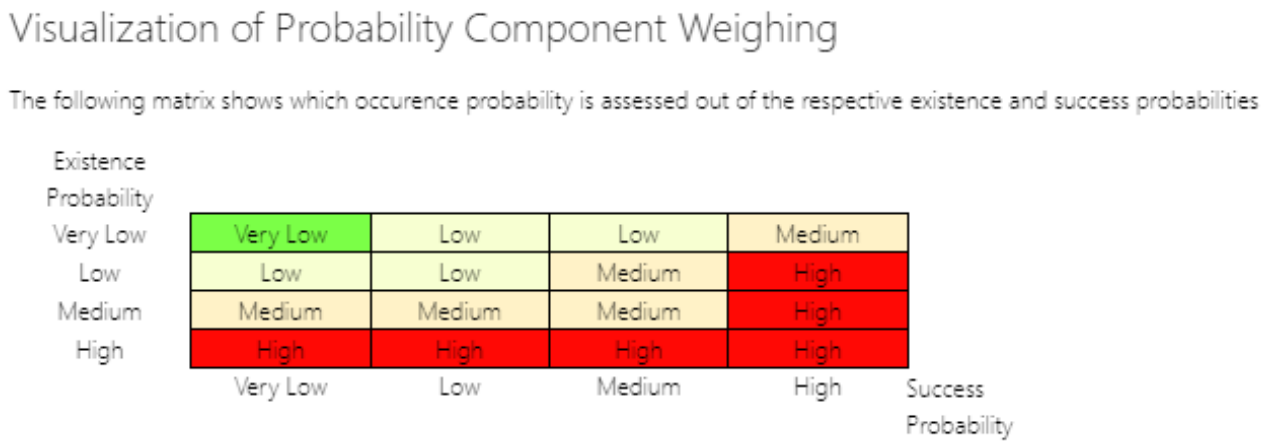

Abbildung 10: Matrix zur Zusammenführung der Erfolgs- und Existenzwahrscheinlichkeit zur Eintrittswahrscheinlichkeit in Fallstudie 2.

So erfolgt mit $\phi_{prob} = 0{,}37$ eine Bestimmung der Eintrittswahrscheinlichkeit mit einem Anteil der Erfolgswahrscheinlichkeit von 37% und einem Anteil der Existenzwahrscheinlichkeit von

63%. Für das Unternehmen ist somit die potentielle Existenz eines Angriffs wichtiger als die prinzipielle Angreifbarkeit.

Bei der Bestimmung der Risikohöhe aus Schaden und Eintrittswahrscheinlichkeit hingegen wurde mit $\phi_{risk} = 0{,}5$ ein ausgeglichenes Verhältnis von 50% der Schadenshöhe und 50% der Eintrittswahrscheinlichkeit bei der Bestimmung des Risikos gewählt (siehe Abbildung 11).

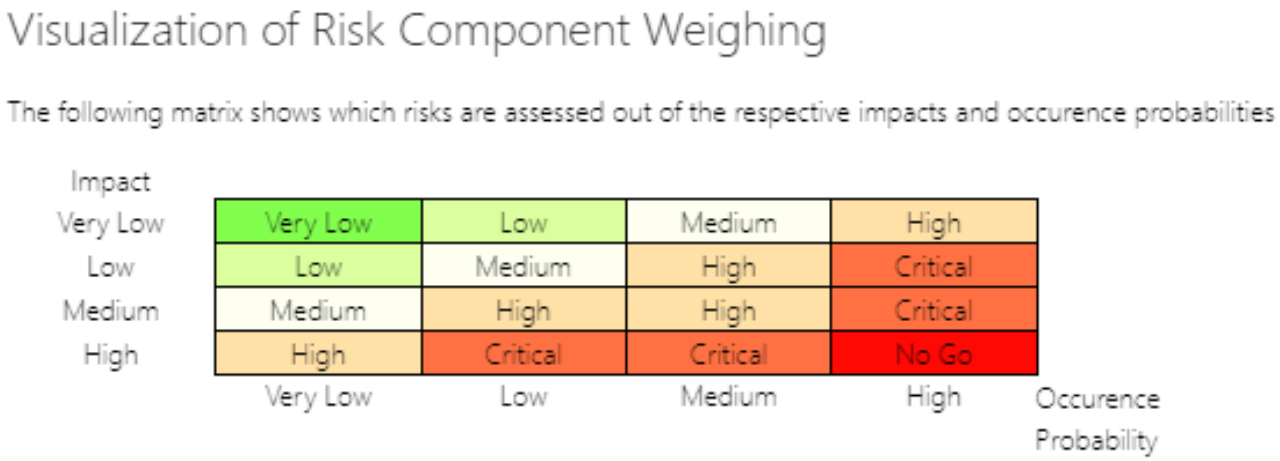

Abbildung 11: Matrix zur Bestimmung der Risikohöhe anhand von Schaden und Eintrittswahrscheinlichkeit der Fallstudie 2.

Die Abschätzung des Risikoappetits über diese Matrizen wurde von den Fallstudienpartnern positiv aufgenommen. Klassisches IT Risikomanagement sei nur auf Risiken über deren Existenz sich das Unternehmen im klaren ist und dessen Materialisierungsmöglichkeiten auch hinlänglich bekannt sind (sogenannte known knowns). Jedoch ermöglicht eine stärkere Gewichtung der Existenzwahrscheinlichkeit auch eine Berücksichtigung von nicht bekannten Risiken (unknown knowns und unknown unknowns), sowie nicht bekannten Materialisierungsmöglichkeiten (known unknowns).

Außerdem entspräche die Matrix zur Bestimmung der Risikohöhe einer Frequency Assessment Table im klassischen Risikomanagement. So kann hiermit bestimmt werden ob der Risikoappetit des Unternehmens eine höhere Gewichtung der möglichen Schäden, oder der möglichen Eintrittswahrscheinlichkeiten vorsieht.

Schließlich erfolgte eine Priorisierung der Geschäftsschäden mit Hilfe des paarweisen Vergleichs im AHP Verfahren. Da keiner der Schäden quantifiziert ist, wurden auch keine Minimal- und Maximalschäden ermittelt, wie dies in Fallstudie 1 der Fall ist. Der paarweise Vergleich führte zu den in Tabelle 10 dargestellten Schadenshöhen.

Schaden	**Schadenskategorie**	**Wert auf Meta-Skala**
Ausfall der Webseite	High	68,71
Broken integrity of customer data	Medium	62
Customer data loss	Low	42

Tabelle 10: Ermittelte Priorisierung der Schäden in Fallstudie 2.

A.5.2 Einschätzung der Existenzwahrscheinlichkeit

Die Gewichtung der angriffsmotivierenden und -ermöglichenden Faktoren zeigte, dass eine weiterführende Beschreibung der Faktoren im Nutzerinterface notwendig ist. Die Faktoren konnten durch Nachfrage jedoch aufgeklärt werden.

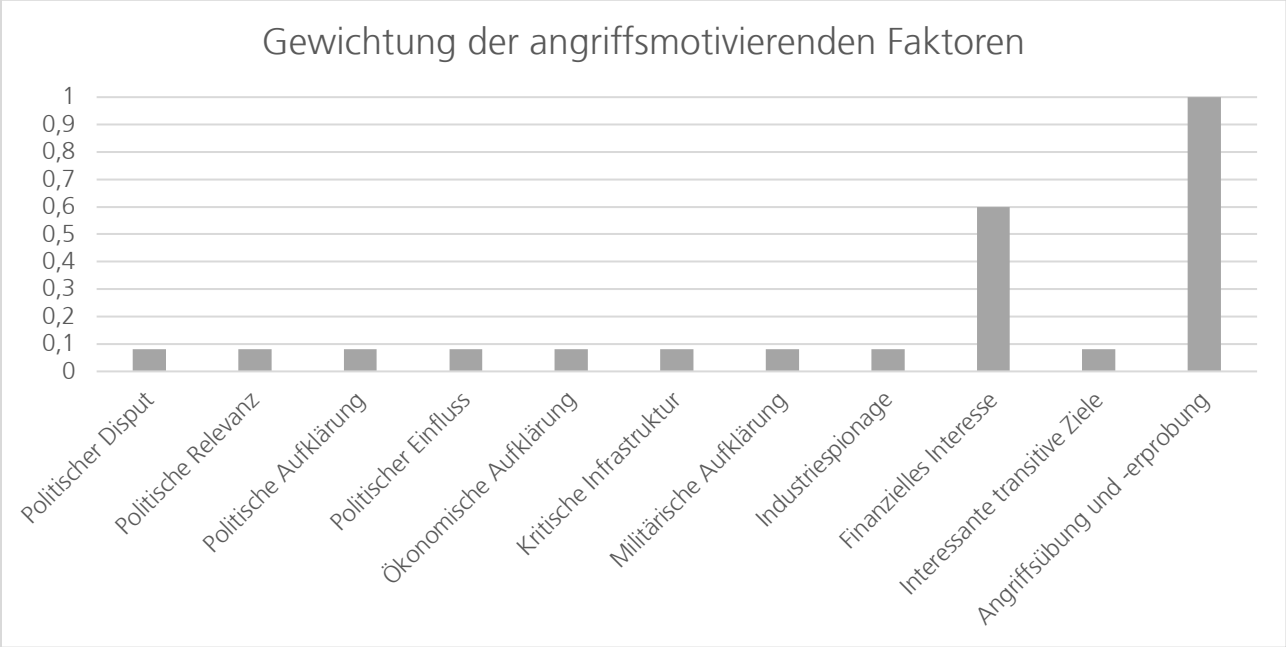

Abbildung 12: Gewichtung der angriffsmotivierenden Faktoren in Fallstudie 2.

Die angriffsermöglichenden Faktoren wurden dabei alle gleich gewichtet. Jedoch ergab sich für die angriffsmotivierenden Faktoren das in Abbildung 12 dargestellte Bild. Dies zeigt, dass für das Unternehmen primär die Erprobung und Übung von Angriffen, sowie das Erlangen finanzieller Vorteile durch Angreifende eine Motivation für einen Angriff darstellen.

Mit Hilfe der Faktorengewichtung wurde nun das Zutreffen beziehungsweise Nicht-Zutreffen der angriffsmotivierenden und -ermöglichenden Faktoren bestimmt (siehe Anhang A.5). Die angriffsmotivierenden Faktoren mit der höchsten Gewichtung treffen dabei alle zu. Außerdem treffen angriffsermöglichende Faktoren zu, welche alle gleich gewichtet sind. Somit ergibt sich in der Fallstudie 1 eine imminente Wahrscheinlichkeit für einen bevorstehenden Angriff ($P_{Existenz} = 1$).

A.5.3 Analyse der IT-Sicherheitsrisiken

Zur Analyse der IT-Sicherheitsrisiken wurden die in Tabelle 11 dargestellten analyserelevanten Komponenten durch den Fallstudienteilnehmer bestimmt. Dabei traten keine Schwierigkeiten, Rückfragen oder Verständnisprobleme auf.

Anschließend erzeugte die Referenzimplementierung einen Fragebogen zur Bestimmung der zutreffenden beziehungsweise nicht-zutreffenden Maßnahmen und möglicher Ausnahmen (Anhang A.7). Hier zeigte sich, dass manche Maßnahmen nicht vollständig implementiert waren. So existierten auch hier Implementierungsausnahmen, darüber hinaus gab es jedoch Maßnahmen wie das Code Signing, welches zwar in seiner Umsetzung sämtliche der Bedrohungen abdeckte, jedoch nicht für den gesamten Service implementiert war.

Komponentenart	**Vorhandende Komponenten**
Cloud Computing	SaaS
Kollaboration	Menschen, E-Mail Kommunikation, E-Mail Clients, Web Browser
Virtualisierung	Container
Betriebssysteme	Linux
Infrastruktur	IT Netzwerk, Active Directory, Shared Storage Locations, Netzwerk Shares, Fileshares, Repositories, Information Repositories, Internal Webpage, Webpage, Webanwendung, Datenbank, SSH

Tabelle 11: Analyserelevante Komponenten der Fallstudie 2.

Hinsichtlich der Maßnahmenkategorisierung wurde angemerkt, dass die Kategorisierung des NIST Cybersecurity Frameworks (CSF) die Auffindbarkeit der Maßnahmen im Fragebogen erleichtern würde. Die Kategorisierung der Maßnahmen nach der wirtschaftlichen Perspektive, wie sie in der Referenzimplementierung umgesetzt ist, hätte jedoch den Vorteil, dass die Maßnahmen besser beim Vorstand verargumentiert werden könnten. Die Triage-Denkweise des CSF, nach welcher Maßnahmen nicht alleinestehen, sondern als Verbund aus detektiver, verhindernder und wiederherstellender Maßnahme dargestellt werden, würde jedoch gerade die Argumentation von Maßnahmenbündeln unterstützen.

Erkenntnis 2.5: Die Klassifikation des NIST Cyber Security Frameworks kann insbesondere bei Maßnahmenbündeln zur Argumentation des Investitionsaufwands genutzt werden.

Der sich ergebende Risikoreport zeigte ein mittleres bis kritisches Risiko (siehe Abbildung 13). Dies ist durch die geringe bis mittlere Erfolgswahrscheinlichkeit und die sehr hohe, stärker gewichtete Existenzwahrscheinlichkeit zurückzuführen. Mit einer Abdeckung der pivotisierten Bedrohungen von 52,71% ist das pivotisierte Bedrohungsbild bei der Risikoanalyse zwar ebenfalls zu berücksichtigen, jedoch ergibt dieses keine Veränderung der Risikohöhe.
Dabei ergibt sich die Erfolgswahrscheinlichkeit Low bis Medium aus den nicht vollständig adressierten Bedrohungen der Kill-Chain Phasen (siehe Anhang A.8). Insbesondere der Cloud Service Einsatz, sowie die fehlende Adressierung der Web Shell Bedrohungen und die

Anfälligkeit gegenüber Spearphishing stellen dabei eingehende Angriffsvektoren dar. Diese können über entsprechende Scripting Bedrohungen Schadsoftware ausführen und Privilegien eskalieren. Ein langfristiger Zugriff kann schließlich über entwendete oder unbefugt eingerichtete Cloud Accounts, sowie wiederum der Einrichtung von Web Shells erreicht werden.

Die Verringerung der öffentlichen Zugriffsmöglichkeiten, sowie die vollständige Einführung von Multi-Faktor Authentifizierung, Netzwerksegmentierung und Data Loss Prevention Systemen im Service können die Eintrittswahrscheinlichkeit der meisten ermittelten Bedrohungen von Low auf Very Low verringern.

Allerdings zeigt die Sichtung der alternativen Adressierungsoptionen auch, dass Bedrohungen existierten, deren Eintrittswahrscheinlichkeit Low aufgrund der feinen Granularität der Wahrscheinlichkeitsklassen zustande kam.

		Eintrittswahrscheinlichkeit			
		Very Low	**Low**	**Medium**	**High**
Schaden	**Very Low**	Very Low	Low	Medium	High
	Low	Low	**Medium**	High	Critical
	Medium	Medium	**High**	High	Critical
	High	High	**Critical**	Critical	No Go

Abbildung 13: Risikomatrix der Fallstudie 2.

Erkenntnis 2.6: Fein granulare Wahrscheinlichkeitsklassifikationen können dazu führen, dass vollständig adressierte Bedrohungen nicht der niedrigsten Wahrscheinlichkeitsklasse zugewiesen werden.

Der Fallstudienpartner merkte an, dass die Möglichkeit einzusehen welche Bedrohungen zu welchem Risiko führen hilfreich in der Bewertung des Reports wären. Dies ist zwar durch den Ansatz möglich, jedoch nicht in der Referenzimplementierung implementiert.

Erkenntnis 2.7: Eine Darstellung welche Bedrohungen zu welchem Risiko führen unterstützt in der Bewertung des Risikoreports.

Darüber hinaus wäre eine Darstellung der CSF Triage innerhalb der Bedrohungen vorteilhaft um die Maßnahmen besser bewerten zu können. So könne hervorgehoben werden welche

Bedrohungen lediglich durch detektive Maßnahmen überwacht und für welche auch vermeidende, oder reaktive Maßnahmen vorgesehen sind (Erkenntnis 2.5).

Die Darstellung der relevanten Angreifenden und der Malware wurde positiv kommentiert. Diese würde einen Faktor mit der Risikoanalyse verbinden, über welchen man sich sonst keine Sorgen machen würde, da sich aktuelle Analysen kaum damit auseinandersetzen wer eigentlich angreifen könnte. Dies helfe aber bei der Priorisierung von Investitionsbedarfen. Man könne diese Liste an Experten im Unternehmen weiterreichen, welche den Service und die implementierten Maßnahmen auf Grundlage der möglichen Angreifenden- und Malwareaktivitäten weiter verfolgen könnten. Am Ende sei das Ziel die Risiken zu mitigieren indem die Schwachstellen reduziert werden. Die Malware und Angreifendenliste helfe hierbei.

Erkenntnis 2.8: Eine Darstellung der relevanten Angreifenden und relevanter Malware unterstützt bei der Priorisierung von Investitionsbedarfen.

A.6 Angriffsmotivierende und -ermöglichende Faktoren der Fallstudie 2

Angriffsmotivierender Faktor	**Erfüllt?**		**Angriffsermöglichender Faktor**	**Erfüllt?**
Politischer Disput			Cloud Services	√
Politische Relevanz			Schatten-IT	√
Politische Aufklärung			Spearphishing / Social Engineering	√
Politischer Einfluss			Verwundbarkeiten	
Ökonomische Aufklärung			Exploits	
Kritische Infrastruktur			Abgeflossene Opferinformationen	
Militärische Aufklärung			Abgeflossene Credential	
Industriespionage	√		Physischer Supply Chain Zugriff	
Finanzielles Interesse	√		Physischer Organisationszugriff	√
Interessante transitive Ziele			Öffentlich zugreifbare Systeme	√
Angriffsübung und -erprobung	√		0-Day Exploits	√
			Kompromittierte laterale Organisationen	

Tabelle 12: Zutreffen beziehungsweise Nicht-Zutreffen der angriffsermöglichenden und -motivierenden Faktoren in Fallstudie 2.

A.7 Zutreffen der ermittelten Gegenmaßnahmen in Fallstudie 2

Maßnahme		**Ausnahmen**
Data Loss Prevention	✓/O	Exfiltration über alternative Protokolle
Software Konfiguration	O	Spearphishing via Links, Spearphishing via Anhänge, Phishing nach Informationen, Phishing
Daten Backup	✓	
User Account Control	×	
Softwareupdates	✓	Pre-OS Boot, Firmaware Corruption, Drive-by Compromise
Exploit Protection	×	
Antivirus/Antimalware	✓	
Application Isolation and Sandboxing	×	
Application Developer Guidance	✓	
Audit	O	Malicious Image, Löschen von Cloud Instanzen, E-Mail Forwarding Regeln, Erstellen oder Modifizieren von Systemprozessen
Boot Integrity	✓	
Code Signing	✓/O	
Einschränken des Ladens von Softwarebibliotheken	✓	
Credential Access Protection	✓	
Deaktivieren oder Entfernen von Feature oder Programm	✓/O	Downgrade Attack, VBA Stomping, Visual Basic, Web Shell, Server Software Component
Verschlüsseln sensibler Informationen	✓/O	
Behavior Prevention on Endpoint	×	
Environment Variable Permissions	✓	
Execution Prevention	✓	
Filter Network Traffic	✓	
Account Use Policies	✓	
Limit Access to Resource over Network	✓/O	
Limit Hardware Installation	✓	
Limit Software Installation	✓	
Multi-factor Authentication	✓/O	
Network Intrusion Prevention	✓	
Network Segmentation	✓/O	
Remote Data Storage	✓	
Operating System Configuration	✓	
Password Policies	✓	
Privileged Account Management	✓	

Maßnahme		**Ausnahmen**
Privileged Process Integrity	✓	
Restrict Registry Permissions	✓	
Restrict File and Directory Permissions	✓	
Restrict Web-Based Content	✓	
SSL/TLS Inspection	✓	
Threat Intelligence Program	✗	
User Account Management	✓/O	
User Training	O	GUI Input Capture, Browser Extensions, Browser Session Hijacking
Vulnerability Scanning	✓	
Active Directory Configuration	✓/O	
✓ Trifft vollständig zu O Trifft mit Ausnahmen zu ✓/O Trifft nicht vollständig (mit Ausnahmen) zu ✗ Trifft nicht zu		

Tabelle 13: Zutreffen beziehungsweise Nicht-Zutreffen der ermittelten Maßnahmen der Fallstudie 2.

A.8 Nicht vollständig adressierte, ermittelte Bedrohungen der Fallstudie 2

Kill-Chain Phase	Max(P')	Nicht vollständig adressierte Bedrohungen
Initial Access	Low	Cloud Accounts (Low), Compromise Hardware Supply Chain (Low), Compromise Software Supply Chain (Low), Exploit Public Facing Application (Low), Valid Accounts (Low)
Execution	Low	Malicious Image (Low), Systemd Timers (Low), JavaScript (low), Malicious File (Low), Malicious Link (Low), Python (Low), Visual Basic (Low), Unix Shell (Low), User Execution (Low), Native API (Low), Command and Scripting Interpreter (Low), Scheduled Task/Job (Low)
Privilege Escalation	Low	Container Orchestration Job (Low), Systemd Timers (Low), Cloud Accounts (Low), Hijack Execution Flow (Low), Unix Shell Configuration Modification (Low), Create or Modify System Process (Low), Valid Accounts (Low), Scheduled Task/Job (Low)
Defense Evasion	Low	Pluggable Authentication Modules (Low), Cloud Accounts (Low), Hijack Execution Flow (Low), Valid Accounts (Low)
Persistence	Medium	Container Orchestration Job (Low), Systemd Timers (Low), Pluggable Authentication Modules (Low), Cloud Accounts (Low), Hijack Execution Flow (Low), Cloud Account (Medium), Unix Shell Configuration Modification (Low), Additional Cloud Credentials (Low), Create or Modify System Process (Low), Web Shell (Medium), Server Software Component (Low), Browser Extensions (Low), Valid Accounts (Low), Scheduled Task/Job (Low)
Command & Control	Low	DNS (Low), Mail Protocols (Low), File Transfer Protocols (Low), Web Protocols (Low), Protocol Tunneling (Low), Protocol Impersonation (Low), Steganography (Low), Junk Data (Low), Multi-hop Proxy (Low), External Proxy (Low), Internal Proxy (Low), One-Way Communication (Low), Dead Drop Resolver (Low), Non-Standard Port (Low), Domain Generation Algorithms (Low), Dynamic Resolution (Low), Remote Access Software (Low), Data Encoding (Low), Ingress Tool Transfer (Low), Multi-Stage Channels (Low), Web Service (Low), Non-Application Layer Protocol (Low), Proxy (Low), Application Layer Protocol (Low), Fallback Channels (Low), Data Obfuscation (Low)
Credential Access	Low	Pluggable Authentication Moduls (Low)
Exfiltration	Low	Exfiltration over Asymmetric Encrypted Non-C2 Protocol (Low), Exfiltration over Symmetric Encrypted Non-C2 Protocol (Low), Exfiltration over Web Service (Low), Exfiltration over alternative Protocol (Low), Exfiltration over C2 Channel (Low)

Kill-Chain Phase	**Max(P‘)**	**Nicht vollständig adressierte Bedrohungen**
Impact	Low	Runtime Data Manipulation (Low), Stored Data Manipulation (Low), Data Manipulation (Low), Application or System Exploitation (Low), External Defacement (Low), Internal Defacement (Low), Inhibit System Recovery (Low), Service Stop (Low), Data Encrypted for Impact (Low)

Tabelle 14: Nicht vollständig adressierte ermittelte Bedrohungen der Fallstudie 2.

A.9 Ausgangsbefragung der Fallstudie 2

Ist das Verfahren wiederholbar?

Ja auf jeden Fall. Der einzige Punkt ist die Einschätzung der Einordnung der Risiken. Das kann von Person zu Person variieren. Dass ich gesagt habe, dass ein Risiko von der Auswirkung her höher ist als ein anderes. Das kann zwischen Personen variieren.

Ist der Anbahnungs- und Durchführungsaufwand beherrschbar?

Der Aufwand zur Anbahnung ist absolut beherrschbar und auch im Vergleich geringer, als übliche Methoden.

Der Aufwand zur Durchführung ist auch beherrschbar. Ich finde vom Aufwand her gegenüber dem klassischen Risikoassessment, man muss sagen Threat Assessment, ein wenig mehr Aufwand, weil man das ganze MITRE Framework durch geht. Aber ich finde auch präziser, weil man das sonst mit Bauchgefühl macht.

Dadurch wird es aber nicht unpragmatisch. Ich finde es bringt sogar noch den Charme mit, dass man dadurch eine gute Gap-Analyse hat gegenüber dem MITRE Framework.

Wie verhält sich der Anbahnungs- und Durchführungsaufwand relativ zu vergangenen Analysen?

Geht durchaus schneller, als das was ich kenne. Eventuell sogar schneller als das Risiko Framework der NIST. Auf jeden Fall schneller, als die häufige Kombination aus Annual Loss Estimation, Expected Loss, etc. was im CISSP gelehrt wird.

Kann das Verfahren messbare und kommunizierbare Risikoanalysen bereitstellen?

Ja.

Wie verhält sich die Mess- und Kommunizierbarkeit relativ zu vergangenen Analysen?

Ich würde tatsächlich sagen, es ist ein bisschen besser messbar als andere Verfahren, außer eben das Verfahren, dass im CISSP gelehrt wird.

Die Kommunizierbarkeit ist aber eher ähnlich wie bei anderen Verfahren.

Reduziert das Verfahren die Varianz der analysierten Risiken?

Da bin ich mir nicht so sicher. Ich weiß nicht ob wir vielleicht dafür das falsche Beispiel gewählt haben. Ich bin mir nicht sicher, ob man dadurch die Aussage treffen kann, denn ich glaube dass es sehr generalistische Risiken sind, die dabei rauskommen. Und da könnte die Mittelebene fehlen.

Ich hab zwar unten sehr detailliert und tief die Threats und oben heraus generell die Risiken. Aber vielleicht waren wir eine Flughöhe zu hoch. Und deshalb ist die Relevanz der Risiken nicht so gut darstellbar, als wenn es eine Mittelebene aus Vertraulichkeit, Integrität und Verfügbarkeit gibt. Hierdurch könnte die Einschätzung der Risiken variieren.

Eine Mittelebene wie, “Risk of Confidentiality due to…”, würde hier wiederum helfen das ganze zusammenzubinden. Dies würde die Varianz in Bezug auf die Wahrscheinlichkeit reudzieren.

Wie verhält sich dies relativ zu vergangenen Analysen?

Es reduziert die Varianz. Es ist auf jeden Fall weniger Varianz weil es ein bisschen mehr Systematik reinbringt.

Würden Sie das Verfahren weiter nutzen? Wenn ja, warum? Falls nicht, warum nicht?

Teile daraus ja. Teile daraus weil ich gerade die Ermittlung über die generelle „Bin ich ein Ziel für bestimmte Angriffstypen“ super finde. Dann die Abwägung der Risiken [Anmerkung: angriffsmotivierenden und -ermöglichenden Faktoren] finde ich großartig.

Die Risikobewertung würde ich aber nicht nehmen, denn das muss in das bestehende Enterprise Risk Management reinpassen. Das besteht aktuell auf der Befolgung einer Policy oder generellen Eintrittsfaktoren, wo man einfach eine Eintrittswahrscheinlichkeit rechnet und dann einen Betrag X zur Seite legt. Es wäre für mich also schwer das Verfahren in Gänze zu nutzen.

Der Anfang des Verfahrens [Anmerkung: Service Modellierung, Schadensmodellierung, Schadenspriorisierung, Bestimmung der Existenzwahrscheinlichkeit] passt tatsächlich komplett, weil das auch zur finanziellen Betrachtung passt.

Aber auf der grünen Wiese würde ich es einsetzen. Wenn ich jetzt mal weg von meinen bestehenden Prozessen denke, dann würde ich es vollständig nutzen. Von Anfang an würde es komplett funktionieren.

A.10 Detaillierte Beschreibung der Fallstudie 3

A.10.1 Betrachtete Anbindungsszenarien

Das erste Szenario sah die Einbindung der Auslandsliegenschaften in das nationale IT-Netzwerk über sichere Tunnelprotokolle vor. Hierzu sollte jede Auslandsliegenschaften ein eigenes Netz, mit eigenem Network Attached Storage (NAS) und eigener Administrationskraft erhalten. Alle Standorte werden mit einer VPN Verbindung an das nationale IT-Netzwerk angebunden.

Hierdurch wird jedoch auch die Struktur der Authentifizierungsdaten (in diesem Fall Active Directory) dupliziert und in die Auslandsnetze eingebunden. Dadurch ergibt sich eine Vertrauensstellung der Auslandsnetzwerke in das Inlandsnetzwerk. Die Authentifizierung in den Auslandsnetzwerken ist somit über die übergeordneten Active Directory möglich, es ist jedoch keine Authentifizierung über die Auslands-Active Directory aus anderen Auslandsnetzwerken möglich. Dies führt zu der in Abbildung 14 dargestellten Active Directory Struktur.

Im zweiten Szenario erfolgt keine Zusammenlegung der Netzwerk, dafür wird die Anbindung der Auslandsliegenschaften über die Bereitstellung einer Cloud Lösung und Web Applikationen ermöglicht. Hierzu soll die Authentifizierung mit einer 2-Faktor Authentifizierung abgesichert werden.

Schließlich wird im dritten Szenario eine Lösung für das entfernte Arbeiten, beispielsweise Citrix, eingeführt. Über diese werden Netzwerklaufwerke bereitgestellt. Auch hier erfolgt jede Authentifizierung mit einer 2-Faktor Authentifizierung.

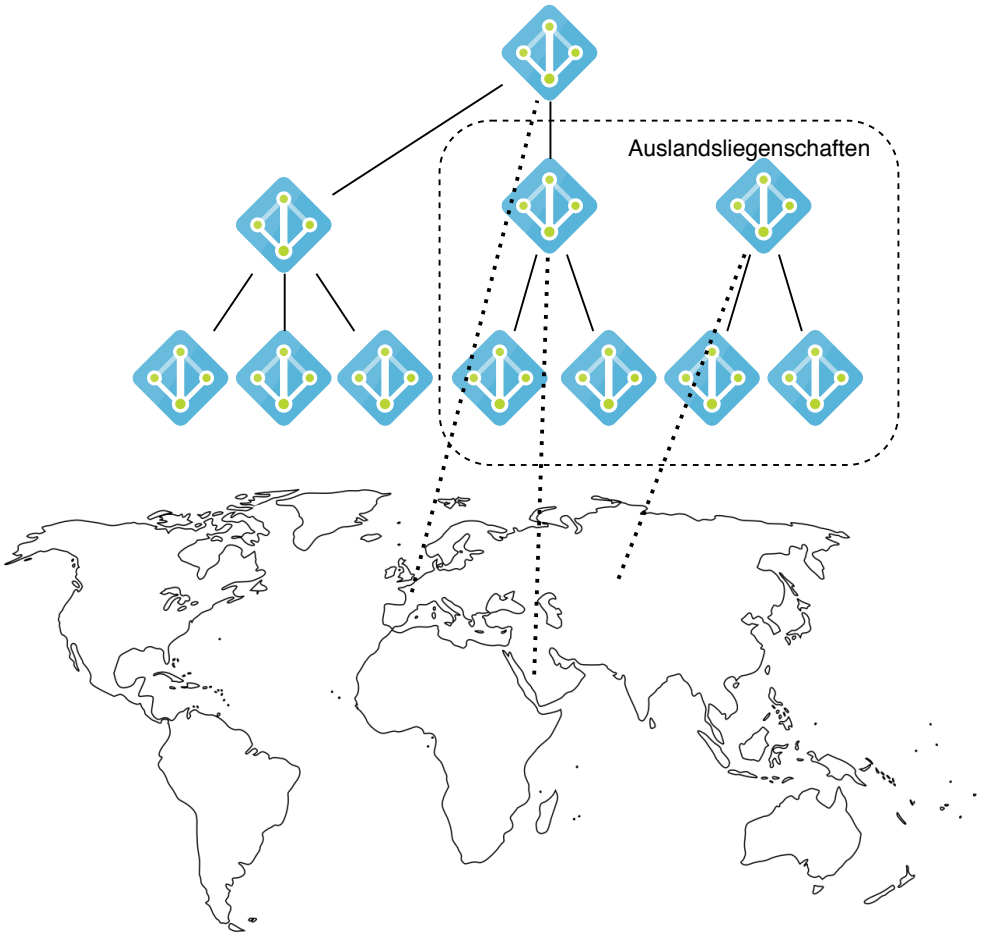

Abbildung 14: Active Directory Wald des Szenario 1. Die Auslandsliegenschaften werden hierbei in das nationale IT-Netzwerk integriert, was zu den dargestellten Vertrauensstellungen des zentralen Active Directory, gegenüber denen des Auslands führt. Namen und Orte wurden gelöscht beziehungsweise verändert um den Schutz des Kunden zu gewährleisten.

A.10.2 Modellierte Services, Geschäftsschäden und Klassifikationen

Die Modellierung der Services konnte auf Grundlage einer Serviceliste erfolgen, welche den Fallstudienpartnern bereits vorlag. Hierdurch konnten die zu berücksichtigenden Services effizient modelliert werden. Jedoch zeigte sich in der Modellierung, dass viele Services keinem IT-Service im Sinne des IT-Service Management entsprechen, also hinsichtlich ihrer Werterfüllung und in Bezug auf die Erfüllung einer Kundenerwartung (Axelos 2019; Hunnebeck 2013, p. 13) dokumentiert sind. Stattdessen handelt es sich hierbei um eine Konsolidierung der darunterliegenden IT-Systeme zum Zweck einer Aufgabenerfüllung. In der Modellierung der Services war dies zunächst unproblematisch. Jedoch führte dies bei der Modellierung der Schäden zu Schwierigkeiten hinsichtlich der Zuweisung Schadenscharakteristika, da hierzu ein Wert- und Kundenbezug in der Beschreibung des Services notwendig ist. Diese Zuweisung konnte nur implizit und somit unscharf erfolgen, da

in der Konsequenz viele Schadensszenarien auf das IT-System und nicht auf die Schäden des Geschäfts ausgerichtet waren.

Erkenntnis 3.1: Werden Services nicht mit einem direkten Geschäftsbezug im Sinne des IT-Service Management modelliert, so erschwert dies die Zuordnung der Schadenscharakteristika.

Anhang A.10 zeigt die modellierten Services, deren Beschreibung und, aus Platzgründen die mit diesen assoziierten Schäden, deren durch paarweisen Vergleich der Schäden für jeden Service ermittelten Höhen und die mit den Schäden assoziierten Schadenscharakteristika.
Zusätzlich zum systembezogenen Servicebegriff zeigte sich in der Zuordnung der Schadenscharakteristika, dass manche Charakteristika für die Arbeit eines NGO nicht sinnvoll sind. So besteht ein sensibler Geschäftsschaden für das NGO in der unbefugten Offenlegung von Dissidentendaten. Dies würde mit einer Gefahr für Leib und Leben der Dissidenten einhergehen. Jedoch geht dies außerhalb eines Reputationsverlusts, einem Wegbrechen möglicher Einkommensquellen, sowie einer durch den Verlust des Dissidenten in der Arbeit des NGO bedingten Disruption des Wertstroms einher.
Für das NGO ist dies jedoch ein beträchtlicher Schaden. Da der Abfluss dieser Daten mit dem, einem Verlust der Marktnische zugrundeliegenden möglichen Abfluss geistigen Eigentums am nächsten kommt, wurde nachträglich der Nischenverlust zu den Datenschutzschäden und der Offenlegung von Daten der Auslandsliegenschaften angeführt.

Dies offenbart jedoch, dass die Schadenscharakteristika ausschließlich für Geschäftsschäden anwendbar sind, die einen direkten monetären Einfluss auf das eigene Geschäftsmodell haben. Schäden, die das Selbstverständnis oder die Mission des Unternehmens betreffen, welche jedoch nicht auf einer auf das Unternehmen bezogenen monetären Grundlage beruhen, können durch die Schadenscharakteristika nicht erfasst werden.

Erkenntnis 3.2: Schäden, die nicht auf eine, auf das Unternehmen bezogene, monetäre Grundlage zurückzuführen sind, sondern sich auf Schäden der Allgemeinheit, oder Dritter beziehen, oder keine Konsequenz haben, die in einen monetären Schaden für das Unternehmen mündet, können durch die Schadenscharakteristika nicht abgebildet werden.

Die Schäden und die paarweise Gewichtung der Schäden wurden dabei anhand der Serviceliste durch die Analysierenden modelliert und vorgenommen. Diese wurden anschließend durch den Auftraggeber überprüft und angepasst, was zu der in Tabelle 18 dargestellten Auflistung führte.
Die Modellierung der Schäden erfolgte dabei aufgrund eines eingehenden Workshops mit der

IT-Abteilung der NGO. In dieser wurde auch die Mission und somit die Bedeutung des Schutzes von Dissidentendaten für die Analysierenden deutlich.
An diesem Workshop nahmen insgesamt 13 Mitarbeitende der IT-Abteilung teil. Da die Referenzimplementierung lediglich den paarweisen Vergleich einer Partei berücksichtigt, hätte ein dem AHP entsprechendes Vorgehen bei Vergleichen durch mehrere Personen mit sämtlichen Teilnehmern nicht stattfinden können.

Erkenntnis 3.3: Die Implementierung des AHP muss mehrere paarweise Vergleiche und Konfliktauflösungen ermöglichen.

Die Klassifikationen für Risiken, Schäden und Wahrscheinlichkeiten lagen im Unternehmen bereits am BSI-Standard 200-3 orientiert vor. Diese wurden gleichverteilt auf die Meta-Skala übertragen (siehe Tabelle 15).

Klassenart	**Klasse**	**Intervall**
Risiko	Gering	1..25
	Mittel	26..50
	Hoch	51..75
	Sehr hoch	76..100
Schaden	Vernachlässigbar	1..25
	Begrenzt	26..50
	Beträchtlich	51..75
	Existenzbedrohend	76..100
Wahrscheinlichkeit	Selten	1..25
	Mittel	26..50
	Häufig	51..75
	Sehr häufig	76..100

Tabelle 15: Gleichverteilung der Klassifikation des BSI-Standard 200-3 auf die Meta-Skala.

Zur Einschätzung des Risikoappetits wurden zur Kombination der Existenz- und Erfolgswahrscheinlichkeit ein Wert von $\phi_{prob} = 0{,}56$ gewählt, was einem Anteil von 57% der Erfolgswahrscheinlichkeit und 44% der Existenzwahrscheinlichkeit bei der Bestimmung der Eintrittswahrscheinlichkeit entspricht. Dies repräsentiert eine geringfügige Neigung der Organisation dahin, bekannte Risiken als vollständig beziehungsweise unvollständig adressiert zu betrachten, während eine mutmaßliche unbekannte Risikomaterialisierung zwar als möglich, jedoch etwas weniger priorisiert als die bekannten Materialisierungsarten betrachtet wird.
Zur Bestimmung der Risikoanteile wurde ein Wert von $\phi_{risk} = 0{,}79$ gewählt, was einem Anteil von 79% der Eintrittswahrscheinlichkeit und 21% der Schadenshöhe entspricht. Der eingehende Workshop machte dabei deutlich, dass Risiken weniger aufgrund ihres möglichen

Schadens, sondern aufgrund ihrer Eintrittswahrscheinlichkeit priorisiert werden. Dies spiegelt sich im gewählten ϕ_{risk}-Wert wieder.

Hierdurch ergibt sich die in Abbildung 15 dargestellte Matrix zur Bestimmung der Eintrittswahrscheinlichkeit auf Grundlage von Erfolgs- und Existenzwahrscheinlichkeit, sowie die in Abbildung 16 dargestellte Matrix zur Bestimmung der Risikohöhe auf Grundlage von Eintrittswahrscheinlichkeit und Schadenshöhe.

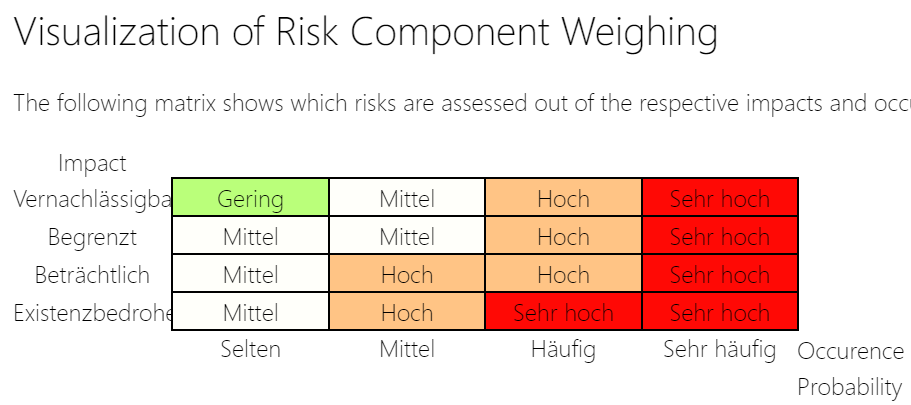

Abbildung 15: Risikomatrix der dritten Fallstudie.

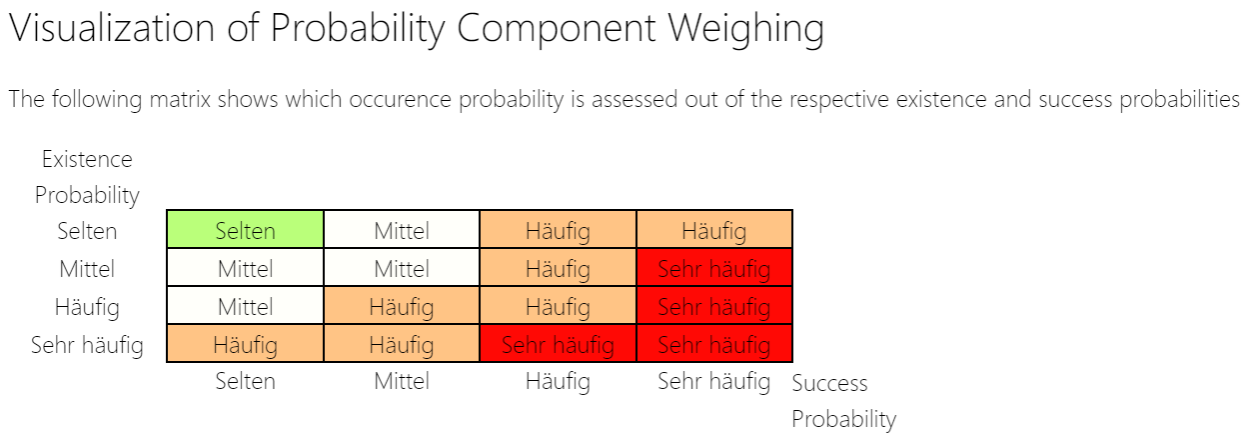

Abbildung 16: Matrix zur Kombination der Existenz- und Erfolgswahrscheinlichkeit zur Eintrittswahrscheinlichkeit in Fallstudie 3.

A.10.3 Einschätzung der Existenzwahrscheinlichkeit

Vor Bestimmung der Existenzwahrscheinlichkeit wurde eine Gewichtung der angriffsmotivierenden und -ermöglichenden Faktoren über einen paarweisen Vergleich im Rahmen des implementierten AHP Verfahrens vorgenommen. Hierbei zeigte sich, dass sämtliche angriffsermöglichenden Faktoren gleichgewichtet wurden. Allerdings fanden sich erhebliche Unterschiede in der Bedeutung der angriffsmotivierenden Faktoren für das Unternehmen (siehe Abbildung 17).

Aufgrund der politischen Arbeit der NGO sah sich diese primär im Rahmen eines politischen Disputs mit anderen Ländern, aufgrund ihrer politisch relevanten Arbeit, der von ihr im Rahmen der Arbeit verarbeiteten Information beispielsweise bei Zusammenarbeit mit Dissidenten oder dem politischen Einfluss ihrer Arbeit.

Ein Angriff zur ökonomischen Aufklärung, aufgrund einer Rolle als kritische Infrastruktur, zur militärischen Aufklärung, zu Spionagezwecken, um einen finanziellen Mehrwert zu erreichen, oder zur Übung und Erprobung von Angriffen wurde untergeordnet betrachtet. Lediglich der Kontakt der NGO mit anderen interessanten Zielen und somit deren Nutzung im Rahmen von Angriffen auf diese Ziele wurde als relevanter, jedoch den politischen Aspekt untergeordnete Motivation möglicher Angriffe betrachtet.

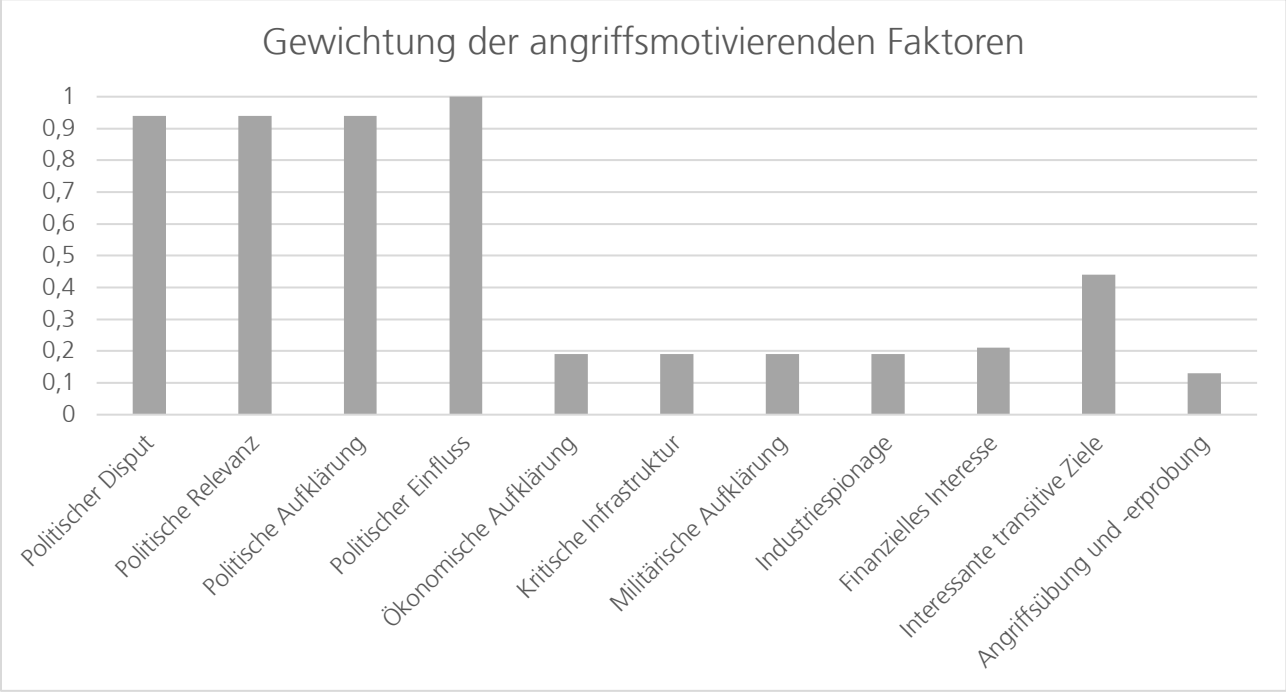

Abbildung 17: Gewichtung der angriffsmotivierenden Faktoren in Fallstudie 3.

Die Gewichtung der angriffsmotivierenden Faktoren ging mit 30 Minuten Zeitaufwand doppelt so schnell, wie im Fall von Fallstudie 1. Dies lag jedoch daran, dass bis auf fünf Faktoren sämtliche weiteren ausgeschlossen hinsichtlich ihrer Relevanz ausgeschlossen werden konnten, was einen genauen Vergleich ausschließlich für diese fünf Faktoren notwendig machte. Da vier dieser Faktoren jedoch gleichgewichtet wurden, war diese Arbeit trivial. Zusätzlich signalisierten die Mitarbeiter der IT-Abteilung eine gute Kenntnis der Mission der NGO, so dass die umfangreichen Fragen bereits durch den Projektleiter aus der IT-Abteilung beantwortet werden konnten.

Erkenntnis 3.4: Die Beantwortung der Fragen zur Gewichtung der angriffsmotivierenden und -ermöglichenden Faktoren kann durch Mitarbeiter einer Abteilung, beispielsweise der IT-Abteilung durchgeführt werden, wenn diese ausreichend Kenntnis über die Tätigkeiten und die Mission des Unternehmens haben.

Der Fragebogen zur Erfüllung der angriffsmotivierenden und angriffsermöglichenden Faktoren wurde für jedes Szenario erneut ausgefüllt. Dieser zeigte, dass die NGO auch finanzielle Anreize für Angriffe bieten könnte. Jedoch unterschieden sich die angriffsmotivierenden Faktoren nicht in den jeweiligen Szenarien. Die angriffsermöglichenden Faktoren unterschieden sich jedoch aufgrund der direkten Einbindung der Netzwerke der Auslandsliegenschaften. So bestand zum Zeitpunkt der Analyse noch keine reife IT-Organisation in den Liegenschaften, wodurch vor allem Probleme des Spearphishing und durch Social Engineering gesehen wurden. Jedoch auch das unkontrollierte Installieren von Software und die damit einhergehende mögliche Existenz unbehandelter Verwundbarkeiten, sowie möglicher Exploits zeichnet das erste Szenario aus.
Im zweiten Szenario findet sich der Einsatz von Cloud Services als angriffsermöglichender Faktor wieder. Das dritte Szenario bietet schließlich die geringste Anzahl an angriffsermöglichenden Faktoren und somit die niedrigste Existenzwahrscheinlichkeit.
Aufgrund des Zutreffens, beziehungsweise Nicht-Zutreffens und der Gewichtung der angriffsermöglichenden und -motivierenden Faktoren ergaben sich für alle Szenarien eine Existenzwahrscheinlichkeit von $P_{existenz} = 1$.

A.10.4 Analyse der IT-Sicherheitsrisiken

Bei der Analyse der IT-Sicherheitsrisiken fiel auf, dass die Gegenmaßnahmen im Netzwerk der NGO für alle Services gleich waren. Um daher den Aufwand zur Analyse weiter zu reduzieren, wurden die Komponenten der IT-Services aggregiert betrachtet. Dies führt zur Übersicht in Tabelle 16.

Komponentenart	**Vorhandende Komponenten**
Cloud Computing	SaaS*
Kollaboration	Menschen, E-Mail Kommunikation, E-Mail Clients, Passwort Manager, Office Anwendungen, Web Browser, Drittparteien, Sharepoint, 2-Faktor Authentifizierung, Softwareentwicklungstools
Virtualisierung	Virtualisierungsplattformen
Betriebssysteme	Windows, Linux
Infrastruktur	Active Directory, SAML Authentifizierung, Shared Storage Locations / Network Shares / File Shares, Softwareentwicklungstools, Informations- und

Komponentenart	Vorhandende Komponenten
	Datenrepositories, SMB Protokolle, WebDAV Protokolle, Interne Webseite, Externe Webseite, Webanwendungen, Datenbanken, SSH Protokolle, Layer 3 Routing

*Tabelle 16: Relevante Komponenten der IT Services der Fallstudie 3. Mit * markierte Komponenten treffen nur für Szenario 2 zu.*

Bei den Gegenmaßnahmen wurde deutlich, dass der IT-Sicherheitsbetrieb innerhalb der NGO vollständig innerhalb der IT Abteilung angesiedelt war. So existierten kaum Sicherheitsspezifische Drittsysteme, wie beispielsweise Data Loss Prevention Systeme, Vulnerability Scanner, oder Boot Integrity Scanner. Auch prozessuale Maßnahmen wie Audits, oder Threat Intelligence waren nicht vorhanden. Dafür sind aber bereits viele abmildernde und vermeidende Maßnahmen, wie die korrekte Konfiguration der Komponenten vorhanden. Schließlich werden Nutzende im sicheren Umgang mit IT geschult, diese Schulungen berücksichtigen jedoch nicht sämtliche mögliche Bedrohungen. Anhang A.13 zeigt die Maßnahmen, deren Zutreffen, sowie mögliche Ausnahmen auf welche die implementierten Maßnahmen nicht zutreffen an.
Dies führte zu den Risikoreports, deren ermittelte Bedrohungen in Anhang A.14 dargestellt ist.

Die pivotisierten Bedrohungen konnten nur 32,6% der ermittelten Bedrohungen abdecken. Daher wurden diese aufgrund ihrer geringen Aussagekraft in diesem Fall nicht berücksichtigt.

Alle Szenarien mündeten in die gleichen möglichen Bedrohungen. Deren Materialisierung unterschied sich doch hinsichtlich deren Interpretation durch die Analysierenden. Dies zeigt, dass Unterschiede zwischen Szenarien mit der gewählten Methodik nicht notwendigerweise automatisiert erfolgen können, sondern einer nachgelagerten Interpretation der Analysierenden, hinsichtlich möglicher Ausprägungen der Bedrohungen in einem Szenario unterliegen können.

So bestehen Bedrohungen mit einer mittleren Erfolgswahrscheinlichkeit in der Kompromittierung der Lieferketten, Spearphishing, dem Ausnutzen von Multi-Hop Proxies, also über verschiedene Hosts im IT-Netzwerk hinweg, der Verwendung von Protokolltunnel, beispielsweise VPN zur Etablierung von Möglichkeiten zur Fernsteuerung von Malware und dem Ausschleusen von Daten, dem Einrichten von Web Shells im IT-Netzwerk, dem Ausnutzen von Inklusionsfeatures, sowie dem Vortäuschen von vertrauenswürdigem Netzwerktraffic.

In Szenario 1 könnte dies als primäre Angriffsquelle durch die Auslandsliegenschaften gedeutet werden. Die Kompromittierung der dort vorliegenden Softwarelieferketten, könnte durch das Einschleusen von Schatten-IT, oder das Einschleusen von Angreifenden in den Auslandsliegenschaften erfolgen.

In Szenario 2 ist die direkte Einbindung der Auslandsliegenschaften nicht vorhanden. Vielmehr greifen diese auf gemeinsame Cloud Dienste und Apps zu. Hierdurch liegt der mögliche Kompromittierungsweg in der Auslieferung der Cloud Dienste und der Apps, sowie über mögliche DoS Angriffe auf die Cloud Dienste welche jedoch durch die gegebenen Gegenmaßnahme hinreichend adressiert sind.

In Szenario 3 hingegen liegt der mögliche Kompromittierungsweg in der Kompromittierung der Lieferkette des Fernwartungsservices. Hierdurch wird der mögliche Kompromittierungsweg erheblich eingeschränkt.

Sämtliche Szenarien bergen jedoch eine grundsätzliche Gefahr durch Spearphishing und Abfangen von Multi-Faktor Zugangsdaten.
Die Erfolgswahrscheinlichkeiten der Bedrohungen ergeben, unter Berücksichtigung der Existenzwahrscheinlichkeit der Szenarien, die jeweils imminent ($P_{existenz} = 1$) ist und der Risikoappetiteinstellungen, die in Abbildung 18 dargestellte Risikomatrix. Die zutreffenden Risiken bewegen sich dabei, abhängig von ihrem Schaden auf einem mittleren bis hohen Niveau.

		Eintrittswahrscheinlichkeit			
		Selten	**Mittel**	**Häufig**	**Sehr häufig**
Schaden	**Vernachlässigbar**	Gering	**Mittel**	Hoch	Sehr hoch
	Begrenzt	Mittel	**Mittel**	Hoch	Sehr hoch
	Beträchtlich	Mittel	**Hoch**	Hoch	Sehr hoch
	Existenzbedrohend	Mittel	**Hoch**	Sehr hoch	Sehr hoch

Abbildung 18: Risikomatrix der Fallstudie 3. Zutreffende Risiken sind dick umrahmt.

Für dieses Szenario konnten nun anhand der Bedrohungen mögliche alternative Adressierungsoptionen identifiziert werden. Ein Ausschnitt einer solchen Adressierungsoption für die Bedrohung „Compromise Software Supply Chain“ ist in Anhang A.15 dargestellt.

Weiterhin zeigte sich, dass für die Bedrohungen Multi-Hop Proxy und Protocol Tunneling der Command & Control Kill Chain Phase keine alternativen Adressierungsoptionen ermittelt werden konnten. Daher wurde zusätzlich die Anwendung eines Security Monitoring Tools und der Aufbau eines entsprechenden Prozess mit eigenen Rollen vorgeschlagen.

Darüber hinaus konnte eine Vielzahl politisch motivierter staatlicher Angreifergruppen im Risikoreport ermittelt werden, die eine Motivation für einen Angriff hätten und deren Techniken mit den angriffsermöglichenden Faktoren und den ermittelten Bedrohungen übereinstimmen. Somit könnten die Auslandsliegenschaften von möglichen eingeschleusten Mitarbeitern bedroht werden. Um diese Bedrohung abzumildern, wurde in Szenario 1 zusätzlich eine Stärkung des Registrierungsprozess nach ISO 29115 Level of Assurance (LoA) 3 vorgeschlagen, wobei eine stärkere Überprüfung des Hintergrunds einer Person bei der Beantragung von Nutzerdaten, sowie eine Stärkung von Übergabe und Versand der Zugriffsdaten erfolgt.

Sowohl das Security Monitoring, als auch die Stärkung des Identitätsmanagement stellen Maßnahmen dar, die nicht direkt auf die dargestellten Bedrohungen wirken, jedoch eine Grundlage zur Kompromittierung der Software Supply Chain und für die Etablierung eines Kanals zur Fernsteuerung ermöglichen. Diese waren jedoch nicht in den verwendeten Daten auffindbar und mussten durch die Analysierenden nachträglich zur Auswertung hinzugefügt werden.

Erkenntnis 3.5: Die automatisiert ermittelten Maßnahmen müssen durch IT-Sicherheitsexperten zusätzlich erörtert und ergänzt werden, da eine vollständig automatisierte Zuweisung der Maßnahmen aufgrund der Wirkungskomplexität möglicher Maßnahmen nicht zuverlässig ist.

A.10.5 Defizite und Vorteile des Verfahrens gegenüber der Erstanalyse

Die Analyse offenbarte Defizite gegenüber der ebenfalls verwendeten STRIDE Methodik. So wurde mit dieser eine Analyse der möglichen Angriffswege anhand eines Netzwerkdiagramms vorgenommen. Dieses offenbarte Schwachstellen durch eingesetzte Systeme innerhalb des IT-Netzwerks. So nutzte das eingesetzte LineCrypt System zur Verbindung lokaler IT Netzwerke (LAN) den International Data Encryption Algorithm (IDEA) zur Transportsicherung. Dieser gilt jedoch, mit reduzierter Rundenanzahl (6 Runden) als gebrochen. Aufgrund der sich ergebenden Unsicherheiten hinsichtlich des Zusammenhangs notwendiger

Verschlüsselungsrunden und der möglichen Zuordnung von Klartext und/oder Schlüssel zu einem Chiffre in IDEA wurde deshalb von der Verwendung von IDEA abgeraten. Da dies eine Konfigurationsschwachstelle darstellt, welche im Verfahren nur generalisiert berücksichtigt, konnte dies nicht automatisiert ermittelt werden.

Erkenntnis 3.6: Bedrohungen, die aufgrund bestehender Konfigurationsschwächen vorhanden sind, können durch das Verfahren aufgrund der fehlenden detaillierten Analyse des IT-Netzwerks nicht berücksichtigt werden.

Darüber hinaus zeigten die Szenarien Unterschiede hinsichtlich des notwendigen Einsatzes von Kryptographie und somit dem Export und Import von Kryptographie. So kann insbesondere die Verwendung von VPN Tunneln zur Anbindung der IT-Netzwerke (Szenario 1), oder zur Verfügbarmachung der Fernwartungsdienste (Szenario 3) nationalen Importrestruktionen unterliegen. So können eingesetzte Soft Token, je nach verwendeten Verschlüsselungsstandard unter die Dual-Use Definition des Wassenaar-Abkommens (2020) fallen, wodurch diese Exportrestriktionen in Embargoländer der Abkommensteilnehmenden Länder unterliegen. Weiterhin kann die Verwendung von VPN Tunnel in Ländern wie China zu Konflikten führen, sofern diese unter der neuen Gesetzgebung nicht registriert sind, wie sich aus einer möglichen Interpretation des 11. Artikels des chinesischen Data Security Law oft he People's Republic of China aus dem Jahr 2021 schließen lässt, oder die Zugänglichmachung der verwendeten kryptographischen Schlüssel für Strafverfolgungsbehörden notwendig machen, was aus dem 18. Artikel des Thailändischen Computer Crime Acts aus dem Jahr 2017 folgt.

Diese stellen jedoch keine Angriffsmöglichkeit dar und gehen daher über den Begriff der IT-Sicherheit als Sicherheit vor intentioneller Schädigung hinaus. Sie können jedoch für eine Analyse von IT-Sicherheitsrisiken interessant werden, sofern es sich, wie in dieser Fallstudie um einen Vergleich möglicher Architekturoptionen handelt. Jedoch ist hervorzuheben, dass durch die STRIDE Methodik eine solche Analyse ebenfalls nicht möglich ist.

Erkenntnis 3.7: Nicht auf Angreifende bezogene Aspekte, wie die gestalterisch bedingte Verletzung eines möglichen rechtlichen Rahmens können durch das Verfahren nicht berücksichtigt werden.

Bis auf die fehlende Erkennung der möglichen Schwachstelle durch Einsatz des LineCrypt Systems, kam sowohl die Erstanalyse als auch die Wiederholung der Analyse mit dem Verfahren jeweils zum gleichen Ergebnis. Unterschiede konnten sich jedoch hinsichtlich des

Durchführungsaufwands feststellen lassen. Tabelle 17 stellt die Aufwände des Verfahrens mit denen der Erstanalyse unter Verwendung von STRIDE gegenüber. Beide Verfahren nutzten einen eingehenden Workshop bei denen der Aufwand für die Analysierenden bei 3,1 Personentage inklusive Vor- und Nachbereitung des Workshops betrug. Dieser diente zur Ermittlung der relevanten Informationen hinsichtlich existierender Services, möglicher Gegenmaßnahmen, möglicher Schäden, aber auch zum Kennenlernen des NGO. Anschließend erfolgte im Verfahren eine Modellierung der Services und Schäden, was aufgerundet mit 0,7 Personentagen (PT) Aufwand gemessen wurde. Die Bestimmung der Existenzwahrscheinlichkeit erfolgte wie beschrieben in gegenüber Fallstudie 1 und 2 relativ kurzer Zeit mit aufgerundet 0,01 PT Aufwand. Die Bestimmung der Bedrohungen erfolgte automatisiert durch die Referenzimplementierung, weshalb hier keine zusätzlichen Aufwände anfielen.

Schritt	**Verfahren der Dissertation**	**Erstanalyse mit STRIDE**
Eingangsworkshop (Vor- und Nachbereitung)	3,1 PT	3,1 PT
Modellierung der Services	$11 * 0{,}5h = 5{,}5h \approx 0{,}7\ PT$	2 PT
Bestimmung der Existenzwahrscheinlichkeit	$0{,}75h \approx 0{,}01\ PT$	Nicht zutreffend
Bestimmung der Bedrohungen	Nicht zutreffend	4,1 PT
Erstellung und Interpretation der Risikoreports	$11h \approx 1{,}375\ PT$	3,1 PT
Summe	$2{,}385\ PT + 3{,}1\ PT \approx 5{,}5\ PT$	$3{,}1\ PT + 6{,}1\ PT = 12{,}2\ PT$

Tabelle 17: Aufwand des Verfahrens (links) gegenüber der Erstanalyse mit STRIDE (rechts).

Jedoch mussten anschließend die Risikoreports nicht nur erzeugt, sondern auch interpretiert werden, da Unterschiede hinsichtlich möglichen Gegenmaßnahmen und möglichen Bedrohungsumsetzungen erst durch die Analysierenden sichtbar gemacht werden konnten. Hierzu wurde für jeden Service aufgerundet 1 Stunde (h) Arbeit benötigt, was einem Aufwand von 1,375 PT entspricht.

Die Erstanalyse mit STRIDE hingegen benötigte 2 Personentage zur Ermittlung und Modellierung der Informationsflüsse der IT Systeme und nachgelagert 4,1 Personentage zur Ermittlung der Bedrohungen.

Somit ergibt sich für das Verfahren ein aufgerundeter Aufwand von 5,5 Personentagen und mit der Erstanalyse ein Aufwand von 12,2 Personentage. Das Verfahren der Dissertation bietet in Fallstudie 3 somit eine Kostenersparnis von 45%.

Darüber hinaus wurde in STRIDE keine etablierte Grundlage für die anzuwendenden Bedrohungen genutzt. Wäre das MITRE ATT&CK Framework beispielsweise verwendet worden, hätte jede Bedrohung separat auf deren Anwendung hin überprüft werden müssen, da keine Aufteilung des Wahrscheinlichkeitsbegriffs und somit keine Festlegung der Anwendbarkeit einer Bedrohung abseits des Analysesubjekts möglich ist. Wäre in STRIDE daher die gleiche Bedrohungsgrundlage genutzt worden, wären weit höhere Aufwände zur Bestimmung der Bedrohungen aufgetreten.

Erkenntnis 3.8: Das Verfahren bietet Kostenersparnisse von ca. 45% gegenüber einer Analyse mit der STRIDE Methodik

Schließlich führten beide Analysen zum gleichen Ergebnis. Die Darstellung der Materialisierung von Geschäftsschäden, wie dies durch das Verfahren der Dissertation möglich war, führte dabei dazu, dass Folgeinvestitionen hinsichtlich der Einrichtung des Security Monitoring angestoßen wurden. Daher ist davon auszugehen, dass der Geschäftsmodellbezug der Analyse auch die Kommunikation gegenüber der Entscheider unterstützte.

Erkenntnis 3.9: Das Verfahren unterstützt die handlungsinduzierende Kommunikation der Risikoanalysen mit Entscheidern

A.11 Modellierte Services und Schäden der Fallstudie 3

Service	Beschreibung	Schäden	Schadenscharakteristika
Dokumenten-management	Systeme zur Verwaltung von Dokumenten	Datenschutzverletzung und Reputationsverlust (Beträchtlich)	Nischenverlust*, Verlust von Einkommensquellen, Gewinnreduktion durch Kostenerhöhung
		Datenschutzverletzung und politische Ausgesetztheit (Beträchtlich)	Nischenverlust*, Differenzierungsverlust Verlust von Einkommensquellen, Gewinnreduktion durch Kostenerhöhung
		Datenschutzverletzung von Dissidentendaten (Existenzbedrohend)	Nischenverlust* Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertfluss
		Abfluss privilegierter Accountdaten (Beträchtlich)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Fluss, Disruption des Wertfluss
		Abfluss von Dokumenten und Daten (Beträchtlich)	Nischenverlust*, Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung
		Veränderung des Dokumenten-managements (Beträchtlich)	Differenzierungsverlust, Disruption des logistischen Fluss, Disruption des Wertfluss
		Testdaten sind nicht verfügbar (Begrenzt)	Differenzierungsverlust, Disruption des Wertfluss
		Testsystem ist nicht verfügbar (Begrenzt)	Disruption des Wertfluss
		Dokumenten-management ist nicht verfügbar (Beträchtlich)	Disruption des Wertfluss
Adressdaten-organisation	Speicherung, Klassifizierung und Archivierung von Adressdaten	Belästigung des Datensubjekts (Beträchtlich)	Nischenverlust*, Differenzierungsverlust, Verlust von Einkommensquellen, Gewinnreduktion durch Kostenerhöhung
		Einladungen zu Veranstaltungen werden nicht zugestellt (Beträchtlich)	Verlust von Einkommensquellen, Disruption des logistischen Stroms, Disruption des Wertstroms

Service	Beschreibung	Schäden	Schadenscharakteristika
		Adressdaten nicht verfügbar (Begrenzt)	Disruption des logistischen Stroms, DIsruption des Wertstroms
Raumbuch-ungssystem	Systeme zum buchen von Räumen	Buchungssystem nicht verfügbar (Beträchtlich)	Differenzierungsverlust, Disruption des logistischen Stroms, Disruption des Wertstroms
		Buchungen werden unbefugt verändert (Vernachlässigbar)	Disruption des Wertstroms
Stipendien-verwaltung	Systeme zur Verwaltung von Stipendiaten und Bewerbungen	Datenschutzverletzung von Stipendiatendaten (Beträchtlich)	Nischenverlust*, Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung
		Finanzierungsprobleme der Stipendiaten durch Nicht-Verfügbarkeit (Begrenzt)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms
Stipendiums-zahlung	Systeme zur Abwicklung und Archivierung der Zahlungen an Stipendiaten	Datenschutzverletzung (Vernachlässigbar)	Gewinnreduktion durch Kostenerhöhung
		Veränderung von Zahlungsvorgängen (Begrenzt)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung
		Unbefugter Zahlungsvorgang (Begrenzt)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung
		Verhindern von Zahlungsvorgängen (Beträchtlich)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Verlust von Einnahmequellen Disruption des Wertstroms
Lohnverwal-tung	Verwaltung der Löhne und Gehälter	Verzögerung der Abrechnungsprozesse (Begrenzt)	Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms
		Veränderung von Zahlungsvorgängen (Begrenzt)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms
		Datenschutzverletzung (Vernachlässigbar)	Nischenverlust*, Gewinnreduktion durch Kostenerhöhung
Finanzbuch-haltung	Systeme zur Verwaltung von Finanzdaten und zur	Verzögerung der Abrechnungsprozesse (Begrenzt)	Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms

Service	Beschreibung	Schäden	Schadenscharakteristika
	Abwicklung von Zahlungen	Veränderung von Zahlungsvorgängen (Begrenzt)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms
		Unbefugter Zahlungsvorgang (Begrenzt)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung
		Datenschutzverletzung (Vernachlässigbar)	Nischenverlust*, Gewinnreduktion durch Kostenerhöhung
Webauftritt	Webauftritt, Projektpräsentation und Mitgliederbereich	Gefährdung der Vertraulichkeit der Außenliegenschaften durch Abfluss wiederverwendeter Credential (Existenzbedrohend)	Nischenverlust*, Differenzierungsverlust, Verlust von Einkommensquellen, Gewinnreduktion durch Kostenerhöhung
		Reputationsverlust als Folge eines (teilweisen) Defacement oder durch Auslieferung von Malware (Begrenzt)	Differenzierungsverlust, Verlust von Einkommensquellen
		Ausspähen von Mitarbeitern und Assoziierten (Beträchtlich)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms
		Malwarekompromittierung von Besuchern (Beträchtlich)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung
		Gezielte Desinformation über Webseite (Begrenzt)	Differenzierungsverlust
		Reputationsverlust durch Nicht-Erreichbarkeit (Beträchtlich)	Differenzierungsverlust, Verlust von Einnahmequellen, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Stroms, Disruption des Wertstroms
Sharepoint	Sharepoint System zur Dokumentenablage und Workflow-organisation	Reputationsverlust durch Nicht-Erreichbarkeit (Beträchtlich)	Differenzierungsverlust, Verlust von Einnahmequellen, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Stroms, Disruption des Wertstroms

Service	Beschreibung	Schäden	Schadenscharakteristika
		Veränderung sensibler Dokumente der nationalen Büros (Begrenzt)	Differenzierungsverlust, Disruption des Wertstroms
		Veränderung sensibler Dokumente der Auslandsliegenschaften (Begrenzt)	Differenzierungsverlust, Disruption des Wertstroms
		Veränderung von Zugriffsdaten (Beträchtlich)	Differenzierungsverlust, Verlust von Einnahmequellen, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Stroms, Disruption des Wertstroms
		Abfluss sensibler Dokumente zu nationalem Personal oder kollaborierenden Personen (Beträchtlich)	Nischenverlust*, Differenzierungsverlust, Disruption des Wertstroms, Gewinnreduktion durch Kostenerhöhung
		Abfluss sensibler Dokumente zu ausländischen Personal oder kollaborierenden Personen (Existenzbedrohend)	Nischenverlust*, Gewinnreduktion durch Kostenerhöhung, Differenzierungsverlust, Disruption des Wertstroms
Exchange System	System zum Versenden von E-Mails und Verwaltung von Kalendern	Reputationsverlust durch Nicht-Erreichbarkeit (Beträchtlich)	Differenzierungsverlust, Verlust von Einnahmequellen, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Stroms, Disruption des Wertstroms
		Abfluss von E-Mails (Existenzbedrohend)	Nischenverlust*, Gewinnreduktion durch Kostenerhöhung, Differenzierungsverlust, Disruption des Wertstroms
		Veränderung von E-Mails (Beträchtlich)	Disruption des logistischen Stroms, Disruption des Wertstroms, Differenzierungsverlust
		Langfristiger Zugriff durch Accountdaten-veränderung (Beträchtlich)	Differenzierungsverlust, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms, Disruption des logistischen Stroms

Service	Beschreibung	Schäden	Schadenscharakteristika
Skype	Conferencing Lösung	Reputationsverlust durch Nicht-Erreichbarkeit (Beträchtlich)	Differenzierungsverlust, Verlust von Einnahmequellen, Gewinnreduktion durch Kostenerhöhung, Disruption des logistischen Stroms, Disruption des Wertstroms
		Abhören nationaler Gespräche und Chats (Beträchtlich)	Nischenverlust*, Gewinnreduktion durch Kostenerhöhung, Differenzierungsverlust, Disruption des Wertstroms
		Abhören von Gesprächen und Chats der Auslandsliegenschaften (Existenzbedrohend)	Nischenverlust*, Gewinnreduktion durch Kostenerhöhung, Differenzierungsverlust, Disruption des Wertstroms
		Kompromittierung von nationalen Gesprächen (Begrenzt)	Differenzierungsverlust, Disruption des Wertstroms
		Kompromittierung von Gesprächen der Auslandsliegenschaften (Begrenzt)	Differenzierungsverlust, Disruption des Wertstroms

*Tabelle 18: Übersicht der modellierten Services und deren möglichen Schaden. Mit * gekennzeichnete Schadenscharakteristika mussten durch die Analysierenden nachträglich ergänzt werden.*

A.12 Angriffsermöglichende und -motivierende Faktoren der Fallstudie 3

Angriffsmotivierender Faktor	**Szenario**		
Faktor	**1**	**2**	**3**
Politischer Disput	√	√	√
Politische Relevanz	√	√	√
Politische Aufklärung	√	√	√
Politischer Einfluss	√	√	√
Ökonomische Aufklärung			
Kritische Infrastruktur			
Militärische Aufklärung			
Industriespionage			
Finanzielles Interesse	√	√	√
Interessante transitive Ziele	√	√	√
Angriffsübung und -erprobung			
√ Faktor trifft zu (leer) Faktor trifft nicht zu			

Angriffsermöglichender Faktor	**Szenario**		
Faktor	**1**	**2**	**3**
Cloud Services		√	
Schatten-IT	√		
Spearphishing / Social Engineering	√	√	√
Verwundbarkeiten	√		
Exploits	√		
Abgeflossene Opferinformationen	√	√	√
Abgeflossene Credential			
Physischer Supply Chain Zugriff	√	√	√
Physischer Organisationszugriff			
Öffentlich zugreifbare Systeme	√	√	√
0-Day Exploits	√	√	√
Kompromittierte laterale Organisationen	√		

Tabelle 19: Ermitteltes Zutreffen der angriffsermöglichenden und -motivierenden Faktoren der dritten Fallstudie.

A.13 Zutreffende und nicht zutreffende Maßnahmen der Fallstudie 3

Maßnahme		**Ausnahmen**
Data Loss Prevention	✗	
Vulnerability Scanning	✗	
Softwareupdates	✓	
Threat Intelligence	✗	
User Training	O	Vertauschen von Dateiendungen, Ausnutzen von 2-Faktoren Authentifizierung, Abfangen des 2. Faktors bei der Authentifizierung, Nutzerseitige Erkennung von Man-in-the-Middle Attacken, Unsichere Verwaltung von Zugriffsdaten, Abwägung der Adäquatheit von Dateiablagen auf Sharepoint Systemen und Informations Repositories, Servicegetriebenes Spearphishing, Überdeckung / Wiederverwendung von Zugriffsdaten, Schadhafte Ereignisse und schädliche Dialog Boxen in Microsoft Office, Vorbeugen des Stehlens von Web Session Cookies, Erkennung von Template Injection Attacken
Audit	✗	
Application Developer Guidance	✗	
Password Policies	✓	
Privileged Process Integrity	✓	
Restrict Registry Permissions	✓	
Restrict File and Directory Permissions	✓	
Restrict Web-Based Content	✗	
Software Configuration	✓	
User Account Control	✓	
Code Signing	✗	
Restrict Library Loading	✗	
Credential Access Protection	✓	
Disable or Remove Feature Program	✓	
Environment Variable Permissions	✓	
Account Use Policies	✓	
Limit Access to Resource over Network	✓	
Limit Hardware Installation	✗	
Limit Software Installation	✗	
Network Segmentation	✗	
Operating System Configuration	✓	
Data Backup	✓	
Antivirus / Antimalware	✓	

Maßnahme		**Ausnahmen**
Privileged Account Management	✓	
SSL/TLS Inspection	✓	
User Account Management	✓	
Exploit Protection	✕	
Application Isolation and Sandboxing	✕	
Active Directory Configuration	✓	
Boot Integrity	✕	
Encrypt Sensitive Information	✓	
Behavior Prevention on Endpoint	✕	
Execution Prevention	✕	
Filter Network Traffic	✓	
Multi-factor Authentication	✓	
Network Intrusion Prevention	✕	
Remote Data Storage	✓	
✓ Trifft zu	O Trifft mit Ausnahmen zu	✕ Trifft nicht zu

Tabelle 20: Maßnahmen, deren Zutreffen und mögliche Ausnahmen von der Maßnahmenwirkung der Fallstudie 3.

A.14 Ermittelte Bedrohungen der Fallstudie 3

Kill-Chain Phase	**Max(P‘)**	**Nicht vollständig adressierte Bedrohungen**
Initial Access	Mittel	Compromise Software Supply Chain (Mittel), Spearphishing via Service (Mittel), Local Accounts (Mittel), Cloud Accounts (Mittel)
Execution	Gering	Keine
Defense Evasion	Häufig	Traffic Signaling (Häufig)
Persistence	Häufig	Traffic Signaling (Häufig), Web Shell (Mittel), Accessibility Features (Mittel)
Credential Access	Selten	Keine
Privilege Escalation	Mittel	Accessibility Features (Mittel)
Command and Control	Häufig	Traffic Signaling (Häufig), Multi-hop Proxy (Mittel), Protocol Tunneling (Mittel)
Lateral Movement	Selten	Keine
Exfiltration	Selten	Keine
Impact	Selten	Keine

Tabelle 21: Kill-Chain Phasen der ermittelten Bedrohungen, deren maximale Erfolgswahrscheinlichkeit P‘, sowie Bedrohungen der jeweiligen Phase, bei denen P‘ höher als „Selten“ ist, der Fallstudie 3.

A.15 Automatisiert ermittelte Gegenmaßnahmen der Fallstudie 3

Maßnahme	**Angriffsermöglichender Faktor**	**P‘**	**Bewertung**
Update Software	Kein Faktor	Selten	Nicht anwendbar. Die Adressierung besteht ausschließlich in der Veränderung des angriffsermöglichenden Faktors
Vulnerability Scanning	Kein Faktor	Selten	Vulnerability Scanner könnten mögliche Schwachstellen und Schatten-IT detektieren.
Wake-on-LAN deaktivieren	Existenz öffentlich zugreifbarer Systeme	Mittel	Wake-on-LAN kann nicht durchgehend deaktiviert werden, kann aber für die Auslandsliegenschaften sinnvoll sein.
Wake-on-LAN deaktivieren und Netzwerktraffic filtern	Existenz öffentlich zugreifbarer Systeme	Selten	Eine Kombination der generellen Deaktivierung mit einem Filtern des Netzwerktraffic kann sinnvoll sein, benötigt jedoch eine entsprechende Informiertheit über mögliche Bedrohungen.
Verwenden von Remote Desktop Gateways für den Zugriff auf Ressourcen	Kein Faktor	Selten	Nicht anwendbar. Die Verwendung von Remote Desktop Gateways steht der Integration der Aussenliegenschaften in das zentrale Netzwerk entgegen.
Execution Prevention	Kein Faktor	Selten	Anwendbar. Gezieltes Blockieren nicht vertrauenswürdiger Anwendungen in den Aussenliegenschaften über Tools wie Windows Defender Application Control, AppLocker, oder Software Restriction Policies.
Entfernen von Web Shell ermöglichenden Funktionen	Existenz öffentlich zugreifbarer Systeme	Selten	Anwendbar. Web Anwendungen sollten dahingehend überprüft werden, ob diese Code Execution ermöglichende Funktionen, wie PHPs `eval()` Funktion beinhalten. Diese sollten deaktiviert werden.
Limitieren der möglichen Web-Inhalte und Erweiterung des Nutzertrainings um Spearphishing und Multi-Faktor Abfangen	Kein Faktor	Selten	Nicht anwendbar. Eine Restriktion der erreichbaren Web-Inhalte wäre nicht sinnvoll, da dies die Arbeit der NGO erheblich einschränken würde.

Tabelle 22: Automatisierte Maßnahmenermittlung der Fallstudie 3. P‘ zeigt die, nach Maßnahmenanwendung zu erwartende Eintrittswahrscheinlichkeit an.

A.16 Detaillierte Beschreibung der Fallstudie 4

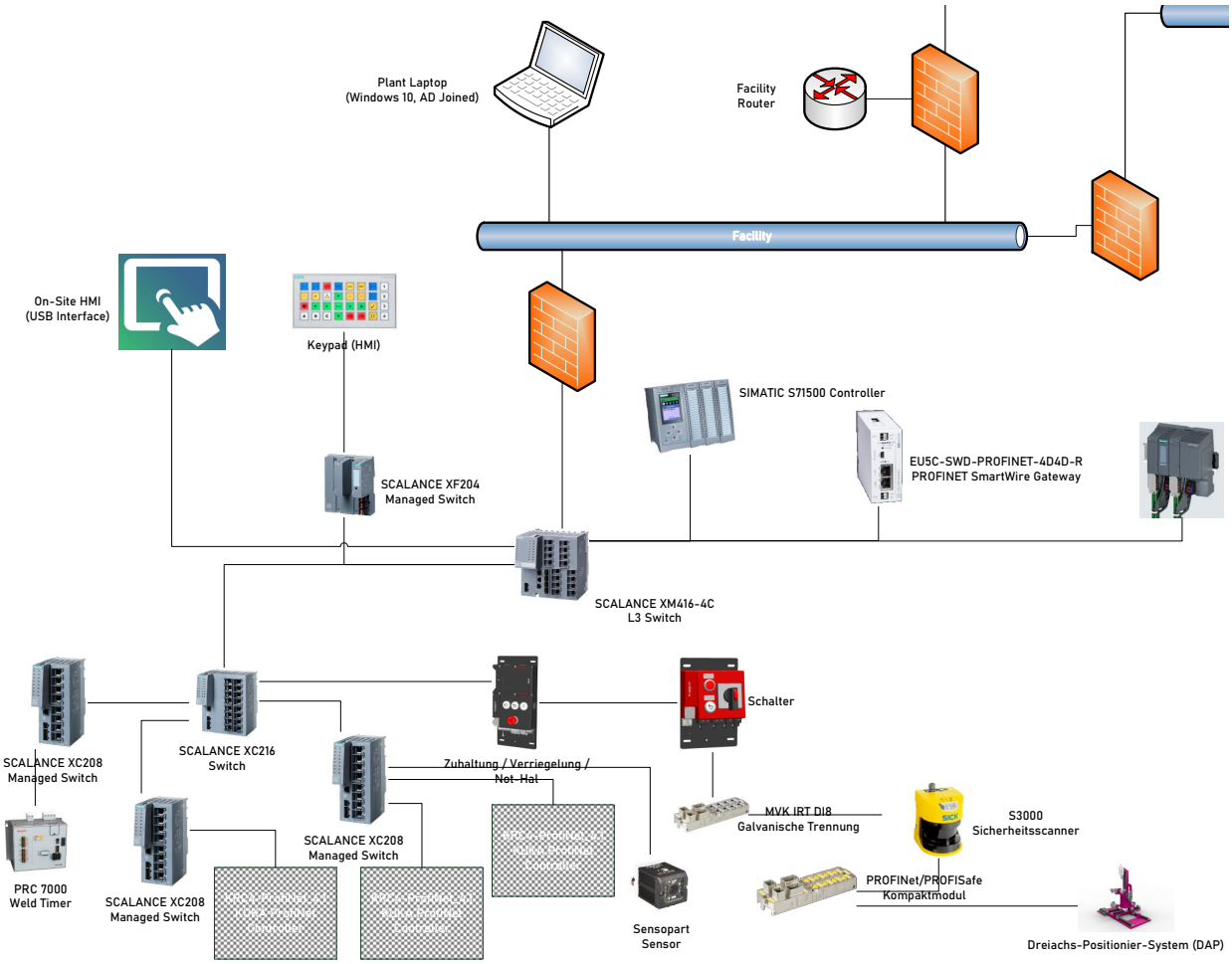

Abbildung 19: Ausschnitt der Modellierung der Produktionszelle.

Im Rahmen der Fallstudie erfolgte zunächst eine Besichtigung der Produktionszelle und ein Vor-Ort Workshop mit den Verantwortlichen für die Produktionszelle. Im Rahmen des Workshops wurden Informationen zur Bestimmung der Existenzwahrscheinlichkeit erfasst, Schäden modelliert und Informationen zum Aufbau der Produktionszelle bereitgestellt.

Letztere wurden über das existierende Siemens Simatic System und eine gepflegte Portliste bereitgestellt. Indem die Analysierenden diese Informationen mit den Informationen des Workshops zu Erreichbarkeit unternehmensweiter Netze und Systeme der demilitarisierten Zone (DMZ) kombinierten, konnte der in Abbildung 19 dargestellte Aufbau der Produktionszelle modelliert werden. Dieser wurden dem Fallstudienpartner zur Überprüfung zur Verfügung gestellt und von diesem freigegeben.

A.16.1 Modellierung und relevante Geschäftsschäden der Produktionszelle

Die Produktionszelle Abbildung 19 wurde als ein Service modelliert. Im Rahmen der Analyse sollten dabei lediglich drei verschiedene mögliche Schadensszenarien betrachtet werden. Diese sind in Tabelle 23 gemeinsam mit ihren Schadenscharakteristika dargestellt. Keiner der dargestellten Schäden konnten von den Fallstudienteilnehmern quantifiziert werden. Die Schäden stellen keine Geschäftsschäden, sondern Schäden mit imminenten Geschäftsbezug dar. So konnten außerhalb einer Unternehmensweiten Analyse bei Fokus auf ein begrenztes, nicht als Service definiertes Analysesubjekt, wie dies bei der betrachteten Produktionszelle der Fall ist, keine Geschäftsschäden modelliert werden. Die nicht technische Formulierung der Schäden erlaubte es jedoch, die Konsequenzen für das Unternehmen abzuwägen und Schadenscharakteristika zu benennen.

Erkenntnis 4.1: Werden Schäden nicht bezogen auf IT Komponenten des Services sondern auf prozessuale, oder kundenorientierte Teile eines Service formuliert, können Schadenscharakteristika ebenfalls zugewiesen werden.

Schaden	**Beschreibung**	**Schadenscharakteristika**
Ausfall der Fernwartung	Die Fernwartung ist aufgrund eines Angriffs nicht verfügbar.	Disruption des Wertstroms
Produktionsausfall	Die Produktion ist aufgrund eines Angriffs nicht verfügbar.	Differenzierungsverlust, Verlust von Einnahmequellen, Gewinnreduktion durch Kostenerhöhung, Disruption des Wertstroms
Sabotage der Produktion	Der Produktionsablauf wird aufgrund eines Angriffs gestört.	Differenzierungsverlust, Verlust von Einnahmequellen, Disruption des Wertstroms

Tabelle 23: Mit der Produktionszelle einhergehende mögliche Schadensszenarien.

Weiterhin wurden drei- beziehungsweise viergliedrige Klassifikationen für Risiken, Schäden und Wahrscheinlichkeiten modelliert, die in Tabelle 24 gemeinsam mit ihrem Intervall auf der Meta-Skala dargestellt sind.

Klassenart	**Klasse**	**Intervall**
Risiko	Low	1..25
	Middle	26..50
	High	51..75
	Severe	76..100
Schaden	Low	1..25

	Middle	26..50
	High	51..75
Wahrscheinlichkeit	Low	1..25
	Middle	26..50
	High	51..75

Tabelle 24: Klassifikationen für Risiken, Schäden und Wahrscheinlichkeiten der Fallstudie 4.

Nun konnte mit Hilfe eines paarweisen Vergleichs die Priorisierung der Schäden ermittelt werden, wobei der Produktionsausfall mit Schadensklasse „High“ den höchsten Wert annahm, gefolgt von der Sabotage der Produktion (Middle) und dem Ausfall der Fernwartung (Low).
Anschließend erfolgte eine Einschätzung des Risikoappetits. Bei der Zusammenführung von Existenz- und Erfolgswahrscheinlichkeit zeigten die Fallstudienpartner dabei eine Gleichheit der Komponenten mit dem gewählten Wert $\phi_{prob} = 0.5$ an, was einem Anteil von 50% der ermittelten Erfolgswahrscheinlichkeit und 50% der Existenzwahrscheinlichkeit eines Angriffs entspricht. Hierdurch ergibt sich die in Abbildung 1 dargestellte Kombinationsmatrix zur Ermittlung der Eintrittswahrscheinlichkeit.
Bei der Ermittlung der Risikoklasse aus Schadenshöhe und Eintrittswahrscheinlichkeit zeigte sich jedoch mit $\phi_{risk} = 0{,}64$ ein etwas stärkere Gewichtung der Eintrittswahrscheinlichkeit gegenüber der Schadenshöhe, da dies einem Anteil von 64% der Eintrittswahrscheinlichkeit und 36% der Schadenshöhe bei der Bestimmung der Risikoklasse entspricht. Hieraus ergibt sich die in Abbildung 21 dargestellte Risikomatrix.

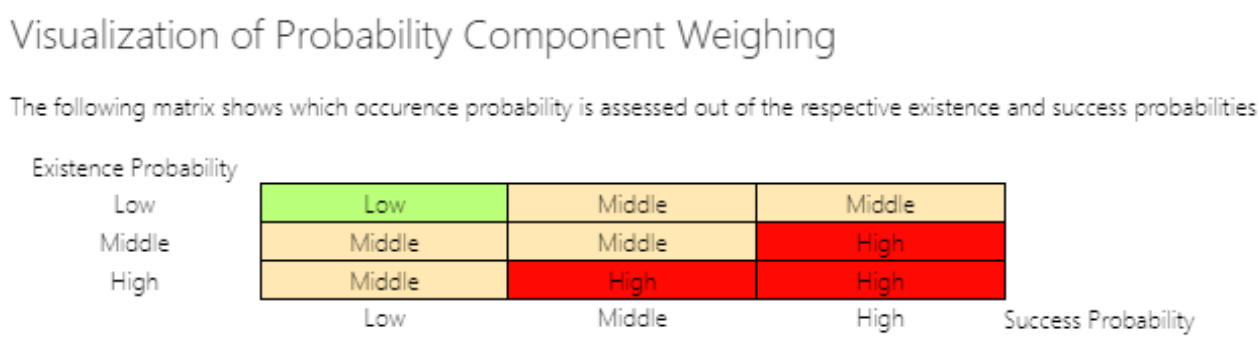

Abbildung 20 Matrix zur Kombination von Existenz- und Erfolgswahrscheinlichkeit zur Eintrittswahrscheinlichkeit

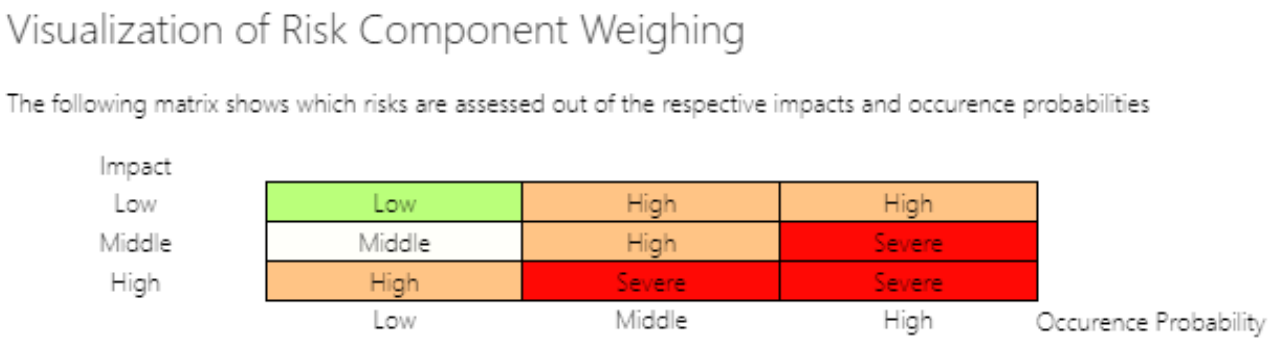

Abbildung 21: Matrix zur Ermittlung der anzuwendenden Risikoklasse aus Schadenshöhe und Eintrittswahrscheinlichkeit.

A.16.2 Einschätzung der Existenzwahrscheinlichkeit

Vor der Einschätzung der Existenzwahrscheinlichkeit wurde mit Hilfe des paarweisen Vergleichs des AHP Verfahrens eine Gewichtung der angriffsmotivierenden und -ermöglichenden Faktoren vorgenommen. Abbildung 22 zeigt die sich ergebende Gewichtung der angriffsmotivierenden Faktoren.

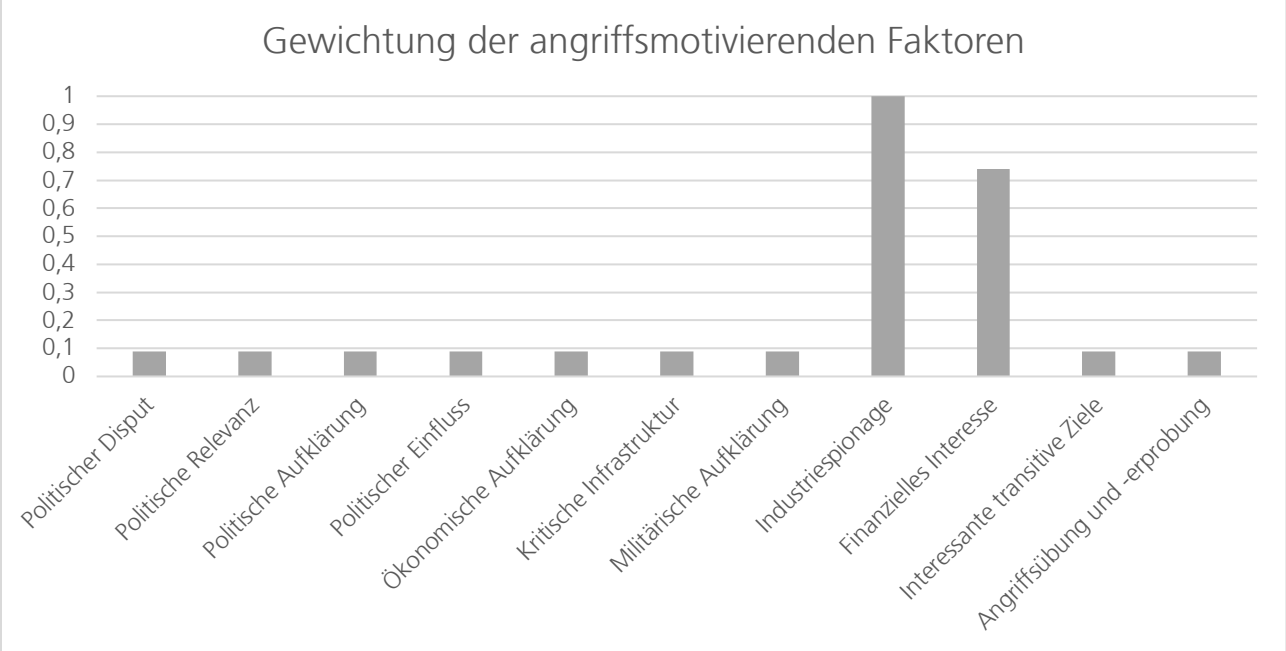

Abbildung 22: Gewichtung der angriffsmotivierenden Faktoren der Fallstudie 4.

So stellen für den Fallstudienpartner die Industriespionage und das Erlangen finanzieller Vorteile die hauptsächlichen Motivationen dar. Zwar könnte die Automobilindustrie auch im Rahmen politischer Dispute in den Fokus staatlicher Angreifergruppen rücken.

Jedoch wären die Schäden zwar wirtschaftlich schädigend, jedoch nicht imminent, wie dies beispielsweise für Banken der Fall wäre. Daher wurde dieser Faktor als nicht wichtiger, als die restlichen Faktoren gesehen und ist somit sehr niedrig gewichtet (0,09).

Die Gewichtung der angriffsermöglichenden Faktoren ist in Abbildung 23 dargestellt. Die größte Gewichtung erhalten existierende Verwundbarkeiten als angriffsermöglichender Faktor, gefolgt von der Möglichkeit des physischen Organisationszugriffs und der Kompromittierung lateraler Organisationen, insbesondere im Zusammenhang mit der Produktionszelle arbeitende Zuliefererunternehmen. Auf diese folgen der physische Zugriff auf die Lieferkette, sowie das Vorhandensein von Exploits.

Abbildung 23: Gewichtung der angriffsermöglichenden Faktoren der Fallstudie 4.

Das Zutreffen beziehungsweise Nicht-Zutreffen der angriffsermöglichenden und -motivierenden Faktoren der Fallstudie 4 ist in Anhang A.16.3 dargestellt. Da die am höchsten gewichteten angriffsermöglichenden und -motivierenden Faktoren zutreffen, ergibt sich für die Fallstudie 4 eine Existenzwahrscheinlichkeit von $P_{existenz} = 1$, also eine imminente Möglichkeit eines Angriffversuchs.

A.16.3 Analyse der IT-Sicherheitsrisiken

Zur Analyse der IT-Sicherheitsrisiken wurden die in Tabelle 25 dargestellten Komponenten angegeben. Hierbei handelt es sich um eine Mischung an Komponenten der IT und Operational Technology (OT). Letztere beschreibt spezielle Komponenten, die ausschließlich in industriellen Steueranlagen zum Einsatz kommen. Jedoch ist auch in OT Umgebungen der Einsatz typischer IT Komponenten geläufig. Darüber hinaus ist die Authentifizierung und

Autorisierung in der Produktionszelle über Active Directory gelöst, so dass auch hier eine IT Komponente in einer OT Umgebung eingesetzt wird.

8

Komponentenart	**Vorhandende Komponenten**
Betriebssysteme	Windows, Linux
Infrastruktur	Engineering Workstation, Sicherheits (Safety) Systeme / Schutzrelais, Zellencontroller / RTU / PLC / IED, Kontrollserver, Human-Machine Interface, I/O-Server, Active Directory

Tabelle 25: Identifizierte analyserelevante Komponenten der Produktionszelle.

Auf Grundlage der identifizierten Komponenten wurde automatisiert ein Fragebogen erzeugt, welcher das Zutreffen, Nicht-Zutreffen und mögliche Ausnahmen der Maßnahmenimplementierungen für die, die identifizierten Komponenten potentiell betreffenden Bedrohungen, erfragt. Aufgrund der Größe der Produktionszelle waren Maßnahmen jedoch entweder vollständig oder gar nicht implementiert, so dass keine Ausnahmen vermerkt sind. Anhang A.18 zeigt die zutreffenden beziehungsweise nicht zutreffenden Maßnahmen.
Dies führte zur Identifikation von IT und OT Bedrohungen, sowie einer Kombination der Kill Chain Phasen der jeweiligen Bedrohungen. Obwohl diese aus unterschiedlichen Sammlungen stammen, konnten diese in der Analyse kombiniert werden. Dies spricht dafür, dass die Implementierung auch in der Lage ist Mischformen von Systemen, die Bedrohungen aus unterschiedlichen Anwendungsbereichen, wie industriellen Steueranlagen, mobilen Systemen oder weiteren beinhalten, analysieren kann.

Erkenntnis 4.2: Das Verfahren ist in der Lage Analysesubjekte zu analysieren, deren zutreffenden Bedrohungen aus unterschiedlichen Anwendungsbereichen kommen.

Hieraus ergab sich eine Übersicht der möglichen Bedrohungen. In der Fallstudie bestand dabei ein Anteil der pivotisierten Bedrohungen von lediglich 38,4% so, dass die pivotisierte Wahrscheinlichkeitsbetrachtung nicht berücksichtigt wurde. Für die Kill Chain Phasen Initial Access (OT), ersistence (IT), Privilege Escalation (IT), Command & Control (IT), Command & Control (OT), Exfiltration (IT) und Collection (OT) ergibt sich jeweils eine maximale Erfoglswahrscheinlichkeit von „Middle“.

Angriffsmöglichkeiten können dabei primär durch Kompromittierung wechselnder Zellenhardware, der Fernwartungsdienste, aus dem Internet zugreifbare Systeme und über die Zulieferer erfolgen. Anschließend können die IT Komponenten aufgrund fehleneder Prozessauthentifizierung und fehlendem Exploit Schutz zur Einrichtung langfristiger Prozessänderungen, oder von Web Shells genutzt werden. Die Command & Control, Exfiltration und Collection Möglichkeiten machen sich die fehlende Netzwerkauthentifizierung und Überwachung zu Nutze (siehe Anhang A.19).

Dieses Bedrohungsbild führt zu einer möglichen Materialisierung hoher bis schwerer Risiken innerhalb der Produktionszelle (siehe Abbildung 24)

		Eintrittswahrscheinlichkeit		
		Low	**Middle**	**High**
Schaden	**Low**	Low	**High**	High
	Middle	Middle	**High**	Severe
	High	High	**Severe**	Severe

Abbildung 24: Risikomatrix der Fallstudie 4.

Als Maßnahmen konnte der Einsatz von Antivirus / Antimalware Lösungen für die OT Systeme, die Einbringung von Jump Hosts für den entfernten Zugriff auf die Produktionszelle Durch die potentielle Kompromittierung der Zulieferer sollten diese, sofern möglich, aus der Produktionszelle ausgeschlossen oder im Umgang mit dieser stärker überwacht werden, beispielsweise durch die Einführung von privilegierten Identitätsmanagementsystemen.
Schließlich wurde empfohlen eine Network Intrusion Prevention Lösung für den Shop Floor zu sondieren.
Die vorgeschlagenen Gegenmaßnahmen, sowie die Risikoanalyse wurden durch die Fallstudienpartner geprüft und für sinnvoll erachtet.

A.17 Angriffsmotivierende und -ermöglichende Faktoren der Fallstudie 4

Angriffsmotivierender Faktor	**Erfüllt?**		**Angriffsermöglichender Faktor**	**Erfüllt?**
Politischer Disput	√		Cloud Services	√
Politische Relevanz			Schatten-IT	
Politische Aufklärung			Spearphishing / Social Engineering	√
Politischer Einfluss			Verwundbarkeiten	√
Ökonomische Aufklärung			Exploits	√
Kritische Infrastruktur			Abgeflossene Opferinformationen	√
Militärische Aufklärung			Abgeflossene Credential	
Industriespionage	√		Physischer Supply Chain Zugriff	√
Finanzielles Interesse	√		Physischer Organisationszugriff	
Interessante transitive Ziele	√		Öffentlich zugreifbare Systeme	√
Angriffsübung und -erprobung	√		0-Day Exploits	√
			Kompromittierte laterale Organisationen	√

Tabelle 26: Zutreffen beziehungsweise Nicht-Zutreffen der angriffsermöglichenden und -motivierenden Faktoren in Fallstudie 4.

A.18 Zutreffende und nicht zutreffende Maßnahmen der Fallstudie 4

Maßnahme und Zutreffen der Maßnahme		**Ausnahmen**
Audit	✓	Keine
Supply Chain Management	✓	Keine
Minimize Wireless Signal Propagation	✗	
Encrypt Network Traffic	✗	
Human User Authentication	✓	Keine
Authorization Enforcement	✗	
Data Loss Prevention	✗	
Mechanical Protection Layers	✓	Keine
Access Management	✓	Keine
Communciation Authenticity	✗	
Software Configuration	✓	Keine
Data Backup	✓	Keine
Update Software	✓	Keine
Exploit Protection	✗	
Antivirus/Antimalware	✗	
Application Isolation and Sandboxing	✗	
Boot Integrity	✓	Keine
Code Signing	✓	Keine
Restrict Library Loading	✗	
Disable or Remove Feature or Program	✗	
Encrypt Sensitive Information	✗	
Execution Prevention	✗	
Filter Network Traffic	✓	Keine
Account Use Policies	✓	Keine
Limit Access to Resource Over Network	✓	Keine
Limit Hardware Installation	✗	
Network Allowlists	✓	Keine
Multi-factor Authentication	✓	Keine
Network Intrusion Prevention	✗	
Network Segmentation	✓	Keine
Software Process and Device Authentication	✗	
Static Network Configuration	✓	Keine
Out-of-Band Communications Channel	✗	
Operating System Configuration	✗	
Redundancy of Service	✓	Keine
Watchdog Timers	✓	Keine
Operational Information Confidentiality	✓	Keine

Maßnahme und Zutreffen der Maßnahme		**Ausnahmen**
Safety Instrumented Systems	✓	Keine
Password Policies	✓	Keine
Privileged Account Management	✓	Keine
Restrict Registry Permissions	✓	Keine
SSL/TLS Inspection	✓	Keine
Threat Intelligence Program	✓	Keine
User Account Management	✓	Keine
User Training	✓	Keine
Vulnerability Scanning	✓	Keine
Active Directory Configuration	✓	Keine
Application Developer Guidance	✗	
Disable or Remove Feature or Program	✓	Keine
User Account Management	✓	Keine
✓ Trifft zu O Trifft mit Ausnahmen zu ✗ Trifft nicht zu		

Tabelle 27: Zutreffen beziehungsweise Nicht-Zutreffen der ermittelten Gegenmaßnahmen.

A.19 Nicht vollständig adressierte Bedrohungen der Fallstudie 4

Kill-Chain Phase	**Max(P')**	**Nicht vollständig adressierte Bedrohungen**
Initial Access (OT)	Middle	Transient Cyber Asset (Middle), External Remote Services (Middle), Internet Accessible Device (Middle), Supply Chain Compromise (Middle)
Persistence (IT)	Middle	Create or Modify System Process (Middle), Web Shell (Middle)
Privilege Escalation (IT)	Middle	Create or Modify System Process (Middle)
Command & Control (IT)	Middle	Web Protocols (Middle), Protocol Tunneling (Middle), Protocol Impersonation (Middle), Steganography (Middle), Multi-hop Proxy (Middle), External Proxy (Middle), Internal Proxy (Middle), One-Way Communication (Middle), Bidirectional Communication (Middle), Dead Drop Resolver (Middle), Domain Generation Algorithms (Middle), Dynamic Resolution (Middle), Remote Access Software (Middle), Data Encoding (Middle), Multi-Stage Channels (Middle), Web Service (Middle), Proxy (Middle), Fallback Channels (Middle), Data Obfuscation (Middle)
Command & Control (OT)	Middle	Connection Proxy (Middle), Standard Application Layer Protocol (Middle)
Exfiltration (IT)	Middle	Exfiltration over Asymmetric Encrypted Non-C2 Protocol (Middle), Exfiltration over Symmetric Encrypted Non-C2 Protocol (Middle), Exfiltration over Alternative Protocol (Middle), Exfiltration over C2 Channel (Middle)
Collection (OT)	Middle	Man in the Middle (Middle)

Tabelle 28: Nicht vollständig adressierte Bedrohungen der Fallstudie.