TECHNISCHE UNIVERSITÄT WIEN

DIPLOMARBEIT

Maßnahmen zur Kontrolle von Cyber-Kumulrisiken in der Versicherungswirtschaft

ausgeführt am

Institut für
Stochastik und Wirtschaftsmathematik
TU Wien

unter der Anleitung von

Prof. Dr. Stefan Gerhold
DI Dr. Michael Schlögl

durch

Andreas Schmid

Matrikelnummer: 01604777

Ahornweg 10
2522 Oberwaltersdorf

Oberwaltersdorf, am 19. Jänner 2022

Kurzfassung

Diese Diplomarbeit befasst sich mit Cyber-Risiken, wie etwa dem eines digitalen Angriffs auf die IT-Struktur von Unternehmen, aus dem Blickwinkel der europäischen Versicherungswirtschaft. Es wird einerseits auf die Versicherung expliziter Cyber-Risiken eingegangen, als auch der Umgang von Versicherungsunternehmen mit impliziten Cyber-Risiken beleuchtet. Die Risikolandschaft und -entwicklung beider Gruppen wird zunächst allgemein aufgearbeitet, um dann im Speziellen auf das Problem von Kumulen bei Cyber-Risiken zu kommen und Lösungen dazu zu erarbeiten.

Es werden verschiedene Methoden erforscht, wie Kumule im Cyber-Geschäft prinzipiell zustande kommen, und Maßnahmen vorgestellt, um diese managen zu können. Weiters werden im Anwendungsfall der Wiener Städtischen Versicherung Produktgestaltung, Tarifierung und Risikokontrolle beleuchtet, sowie eine bereits vorhandene Methode zur Kumulprognose weiterentwickelt. Dazu wird skizziert, wie eine Datenanlieferung im Falle einer eigenständigen Szenarioentwicklung zukünftig auszusehen hat, damit Versicherungen schon jetzt einen Grundstein für eine fundierte, unternehmensinterne Tarifierung und Risikokontrolle hinsichtlich Cyber-Produkten legen können.

Ebenfalls behandelt werden die Auswirkungen von impliziten Cyber-Risiken auf "klassische" Versicherungsprodukte. Auch hier besteht die Gefahr von Kumulen, welche am Beispiel eines Blackouts erforscht wird. Nach einer Risikoanalyse des österreichischen und kontinentaleuropäischen Stromnetzes werden mögliche Folgen von Blackouts für Versicherer anhand verschiedener Expertenmeinungen eruiert. Die Quantifizierung dieser Risken kann beispielsweise mittels einer Szenarioanalyse geschehen, deren Entwicklungsablauf ebenfalls kurz beschrieben wird. Nach der mathematischen Konzeption eines verallgemeinerten Blackout-Modells nach Idee der Vienna Insurance Group werden verschiedene Weiterentwicklungsoptionen entwickelt, bewertet und teils durchgeführt. Eine Anwendung mittels Microsoft Excel liegt dieser Arbeit bei und soll, analog zu den klassischen Cyber-Risiken, zusammen mit der gesamten Diplomarbeit europäischen Versicherern eine Orientierungshilfe in der Auseinandersetzung mit diesem neuartigen Risiko bieten.

Abstract

This thesis deals with currently emerging cyber risks, e.g. attacks on the IT structure of companies, and their effects on the insurance industry in Europe. It explores separately both the insurance of explicit (or affirmative) cyber risks as well as the handling of non-affirmative cyber risks by insurance companies. The risk landscape and development of both groups is at first examined in a general approach, then the issue of risk accumulation regarding cyber risks will be addressed and solutions to it will be worked out.

Multiple methods are explored as to how the accumulation of risks in the cyber insurance business can emerge, and several measures are presented for managing such hazards. Furthermore product design, pricing and risk controlling processes in Wiener Städtische Versicherung are examined and an already existing method for forecasting the accumulation risk potential will be further developed. In addition, this thesis outlines how an adequate data delivery framework should look like in case of an own-built scenario development solution for any European insurance company. Implementing this or similar frameworks, insurance companies can now already lay a foundation for developing sophisticated pricing and risk management processes regarding cyber risk.

Also, the impact of implicit cyber risks on "classic" insurance product is discussed. Here, there appear kinds of accumulation risks, too, which is explored using the example of a blackout scenario. After thorough risk analysis of the Austrian and continental European power grid, possible social and insurance-linked consequences of blackouts are examined based on various experts. The quantification of those risks can be done by scenario analysis, the development process of which is briefly described. After the mathematical conception of a general blackout model based on the idea of Vienna Insurance Group experts, various possible development options are explored, evaluated, and partly implemented. An application using Microsoft Excel is enclosed with this thesis and, analogous to classic cyber risks, is intended (together with the entire thesis) to offer European insurers an orientation aid in dealing with this new type of risk.

Danksagung

Die Anfertigung dieser Diplomarbeit und das Absolvieren meines Masterstudiums wären ohne die Unterstützung verschiedenster Personen in meinem universitären, beruflichen und privaten Umfeld nicht möglich gewesen:

Zu allererst danke ich hier meinen beiden Betreuern, Prof. Dr. Stefan Gerhold sowie DI Dr. Michael Schlögl für ihre professionelle Anleitung und Begleitung der Arbeit. Sowohl durch einige thematische Vorgaben ihrerseits, dem Lektorieren der Arbeit als auch dem Zulassen von "künstlerischen Freiheiten" haben sie erreicht, dass ich auf das Ergebnis dieser Thesis stolz und froh sein kann, einen Mehrwert für alle Beteiligten geliefert zu haben.

Gleichermaßen danke ich besonders meinen Kollegen bei der Wiener Städtischen Versicherung und der Vienna Insurance Group für die Vielzahl an Hilfeleistungen, die sie mir zusätzlich zu ihrer Vollzeittätigkeit geboten haben. DI Christina Kyriakopoulos, DI Florian Mair sowie Mag. Andreas Missbauer waren hier an der Entwicklung der Arbeit maßgeblich beteiligt.

Ebenfalls möchte ich mich gerne bei meinen Kommilitoninnen und Kommilitonen für die hervorragende Kameradschaft in den letzten fünf Jahren bedanken, wegen der ich voll positiver Erinnerungen auf meine Studienzeit an der TU Wien zurückblicken kann.

Herzlicher Dank gilt auch und besonders Dr. Bernhard Salzger, der meine mathematische Begabung bereits vor 13 Jahren erkannt und mich in diesen Belangen jahrelang gefördert hat. Ihm ist es zu verdanken, dass ich das Studium der (Finanz- und Versicherungs-) Mathematik überhaupt gewählt habe.

Zu guter Letzt gilt mein größter Dank meinen Eltern, Susanne und Klaus, sowie meiner Schwester Julia, die mich auch in den schwierigen Phasen meines Studiums stets "ertragen" und unterstützt, sowie mir diese Ausbildung überhaupt ermöglicht haben.

Oberwaltersdorf, am 19. Jänner 2022 *Andreas Schmid*

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Oberwaltersdorf, am 19. Jänner 2022

Andreas Schmid

Inhaltsverzeichnis

1 Cyberrisiken generell

Bevor wir einzelne Kumulszenarien, Anwendungsfälle im VIG-Konzern oder das Thema Silent Cyber überhaupt beleuchten können, gilt es, sich mit den aktuellen Definitionen und dem Stand des Versicherungsmarktes zum Oberbegriff "Cyberrisiken" vertraut zu machen. Ebenjene Themen werden in den folgenden Abschnitten erklärt und abgegrenzt:

1.1 Risikobeschreibung

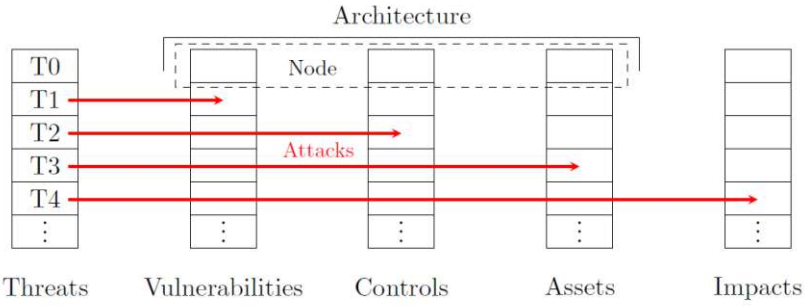
Unter Cyberrisiken versteht man Vermögens- und Reputationsschäden sowie Schäden aus Unterbrechung des Geschäftsbetriebes, welche in kausalem Zusammenhang mit dem Versagen von IT-Systemen stehen[1]. Die Gründe hierfür können vielfältig sein und überspannen Anwendungsfehler durch den Menschen, Fehler bei der internen Implementierung von Prozessen oder technisch mangelhafte externe Komponenten in der EDV-Architektur eines Unternehmens bzw. einer Privatperson, welche zu beispielsweise Hackerattacken führen können.

Vor allem mit dem Voranschreiten der Digitalisierung und dem Ausbau von festen als auch drahtlosen Vernetzungsmöglichkeiten (Stichwort 5G) sind Versicherungsnehmer verschiedensten Cyberrisiken immer mehr ausgesetzt.

1.1.1 Risikoentwicklung und -faktoren

Um Cyberversicherungen seriös anbieten zu können, gilt es, die wichtigsten Risikofaktoren und den Zusammenhang unter ihnen zu erforschen und konsistent zu modellieren. Rainer Böhme stellt in seinem Standardwerk [BLR18] ein Modell vor, welches die Risikoankunft und -entwicklung in fünf grundlegenden Klassen von Risikofaktoren anschaulich darstellt:

[1] Vgl. [CGGP20]



Quelle: [BLR18, S.14]

Abbildung 1.1: Kaskadenmodell der Risikoankunft

In den folgenden Absätzen werden die oben dargestellten Säulen

- Gefahrenquellen
- Systemschwächen
- Steuerungsmechanismen
- (Digitale) Vermögenswerte
- Auswirkungen

vorgestellt und näher beschrieben:

Gefahrenquellen

Es gibt im Groben zweierlei Gefahrenquellen bei der Realisierung eines Cyberrisikos: Zum einen handelt es sich klassischerweise um absichtliche Angriffe auf die EDV-Struktur mittels manipulierter Software, Computerviren oder dem Knacken von Passwörtern. Andererseits können Gefahren aus unabsichtlichen Fehlern in der Bedienung von Programmen, durch Unachtsamkeit als auch in der technischen Architektur selbst stammen.
Interessant ist hierbei im ersteren Fall auch das Profil der Täter: Entgegen der allgemeingültigen Annahme, fast alle Angriffe würden von außenstehenden Hackern in Kapuzenpullovern in dunklen Räumen vor großen Bildschirmen durchgeführt werden, kommen Studien der KPMG [WHSJ17] als auch des deutschen Bundesverbands für Informationswirtschaft, Telekommunikation und neue Medien [BSG15] auf ein anderes Ergebnis: Rund 60% der Gesamttätergruppe bilden nämlich aktuelle oder frühere Mitarbeiter. Laut dem Forensik-Team der KPMG ist der typische Cyber-Kriminelle damit

"...mit 60-prozentiger Wahrscheinlichkeit Innentäter,[...] männlich und zwischen Mitte 30 bis Mitte 50 Jahre alt, bereits mindestens sechs Jahre im Unternehmen beschäftigt, meist eine Führungskraft, eine respektierte, freundliche Person"[2]

Bei den anderen 40% handelt es sich beispielsweise um organisierte als auch "hobbymäßige" Kriminelle oder Geheimdienste. Solche Attacken können vielfältig sein und über mehrere Wege erfolgen:

Wir unterscheiden zunächst darunter, ob das Opfer des Cyberangriffs *zufällig* oder *gezielt* angegriffen wird, wobei das Risiko einer Attacke erster Art weitaus leichter zu quantifizieren ist als das letzterer Art.[3]

Zufällige Attacken sind zumeist standardisiert und damit skalierbar. Der Angriff erfolgt hier beispielsweise über:[4]

- Schadprogramme, übertragen und installiert durch Spam-Mails, beschädigte Dateien oder das Ausnutzen von Sicherheitslücken (ugs. *Computerviren*)
- Spezialfall: *Ransomware* bezeichnet eine immer beliebter werdene Klasse von schädlichen Programmen, die Festplatten, Ordner sowie Dateien verschlüsselt und nur gegen eine Zahlung, meist in Kryptowährungen, wieder freigibt.
- Phishing, also dem Abgreifen von Zugangsdaten. Hier ist seit Jahren vor allem das Bankwesen betroffen.
- CEO-Fraud: Ein Hacker gibt sich über Anfertigung von gefälschten Emails als Führungskraft aus und fordert beispielsweise zum Aussenden von Passwörtern oder Öffnen von Schadsoftware auf.

Wird hingegen ein Opfer gezielt ausgewählt, so ist dies meist viel zeitaufwendiger: Im Regelfall werden hier zunächst Mitarbeiter ausspioniert, um dann über beispielsweise private Interessen das Opfer auf schlecht geschützte Internetseiten zu locken. Damit können sich die Täter Zugang zum betroffenen PC und damit zum Firmennetzwerk schaffen und verdeckt spionieren oder Schaden anrichten. Bis ein solcher Angriff bemerkt wird, vergehen oft Monate. Besonders bei zum Beispiel kritischer Infrastruktur zahlen sich solche zeit- und kostenintensiven Attacken aus.

Ein weiterer gezielter Angriff auf ein Opfer besteht in sog. *DDoS-Attacken*: Hier werden Zielserver mit einer koordinierten Anfragenflut überlastet und damit wichtige Sicherheitsmechanismen im System lahmgelegt.

[2] Vgl. [WHSJ17, S.24]
[3] Vgl. [BLR18, S.14f]
[4] Vgl. [WHSJ17, S.25f]

Systemschwächen

Einen weiteren wichtigen Teil in der Kette eines Cyber-Angriffs bilden als nächstes Glied Systemschwächen. Je mehr von ihnen existieren, desto größer ist die Erfolgswahrscheinlichkeit einer Attacke einzuschätzen. In unserem Modell unterscheiden wir zwischen **symptomatischen** und **systemischen** Schwachstellen in technischen Systemen:

Erstere bezeichnen Angriffspunkte, die bei einem spezifischen Unternehmen vorkommen, etwa durch extra angepasste oder selbst entwickelte Software. Die letzteren bezeichnen Schwächen in Programmen, die mehrere Unternehmen beziehnungsweise Unternehmensgruppen verwenden, etwa SAP-Module oder Standard-Webbrowser.

Gerade systemische Schwächen sollten für Versicherer interessant sein: Bei Entstehung kann dies nämlich nicht nur die Risikoexposition eines Versicherungsnehmers erhöhen, sondern die eines beträchtlichen Teils des Versicherungsportfolios. Dadurch können Kumulrisiken entstehen, welche bei Realisierung ein unerwartetes Großevent auslösen und im Extremfall die Versicherbarkeit der Risiken infrage stellen können!

Die Entdeckung von systemischen Schwachstellen ist sowohl für Angreifer als auch Opfer interessant, weswegen Informationen über solche zu wertvollen handelbaren Gütern werden. Viele Parteien versuchen parallel, Schwächen in Systemen zu finden und dabei einen Wissensvorsprung zu bekommen, was sich einerseits am Schwarzmarkt, andererseits in Form von sogenannten "White-Hat-Hackern" in den Hard- und Softwarehäusern selbst auszahlt.[5]

Steuerungsmechanismen

Als weitere Sicherheitsstufe können Unternehmen optional Maßnahmen (egal welcher Natur) zur Risikoverringerung setzen. Ein naheliegendes Beispiel hierfür wären Bewusstsein schaffende e-Learnings für Mitarbeiter. Hier kann etwa gezeigt werden, wie man herausfindet, wohin Links tatsächlich führen, und wie ein sicheres Passwort auszusehen hat.
Im technischen Bereich unterscheidet Rainer Böhme zwischen detektiven (=aufspürenden) und präventiven Kontrollmaßnahmen.[6] Unter letztere fallen nicht nur die Installation von zusätzlichen Sicherheitsprogrammen, sondern auch das physische Trennen kritischer Infrastrukturkomponenten von einander oder das Einrichten eines "Honeypots": Dies bezeichnet ein künstlich eingerichtetes Netzwerk von Rechnern, das den Angreifer von der eigentlichen Struktur ablenken soll. Es ist meist noch extra mit detektiven Kontrollmechanismen ausgestattet, um einen Angreifer schneller erkennen zu können.[7]

[5] Vgl. [Whi21]
[6] Vgl. [BLR18, S.16f]
[7] Vgl. [Hon21]

Einrichtungen zur Risikosteuerung sind, ungeachtet ihres Typus, essentiell für die Quantifizierung eines Cyber-Risikos. Daher ist eine standardisierte Messung der IT-Landschaft des Versicherungsnehmers im Zuge des Underwriting-Prozesses erforderlich.

(Digitale) Vermögenswerte

Eine Attacke richtet erst Schaden an, wenn sie auf einen Vermögenswert trifft. Dieser Schaden muss bekannterweise gar nicht physisch sein, um in den Deckungsbereich einer Versicherungspolizze zu fallen; Ein Reputationsschaden zum Beispiel durch das Leaken von Daten fällt in vielen Cyber-Polizzen auch schon darunter (mehr dazu im entsprechenden Kapitel). Hier ist für Versicherungen besonders die Bewertung der Vermögenswerte anspruchsvoll, da ein Großteil der digitalen Assets einen schwer quantifizierbaren, immateriellen Wert besitzen.

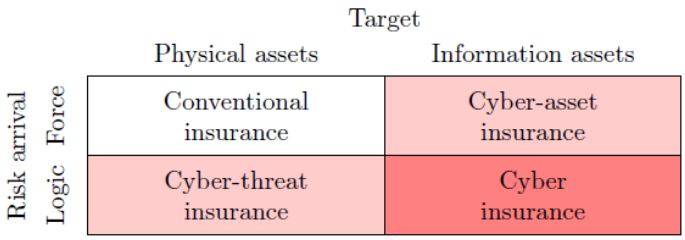
Auswirkungen

Abhängig davon, wie wertvoll und wichtig für den Geschäftsbetrieb eine betroffene Ressource ist, zeigen sich Auswirkungen von Attacken, deren wirtschaftlicher Schaden eine Cyber-Versicherung versucht zu ersetzen. Diese umfangen etwa Kosten infolge einer Geschäftsunterbrechung, Lösegeldzahlungen oder Reputationsschäden. Um den Schaden möglichst überschaubar zu halten, können Unternehmen hier zumeist Assistance-Services der Versicherer in Anspruch nehmen. Auch die Krisenkommunikation ist im Falle einer erfolgreichen Cyber-Attacke von hoher Wichtigkeit, an ihr hängen zu einem großen Teil die zukünftigen Umsätze des Unternehmens!

1.1.2 Abgrenzung

Da die Risikoankunft und -entwicklung von Cyber-Risiken nun illustriert wurde, widmen wir uns nun einer Abgrenzung und Unterteilung, an der sich auch diese Arbeit im Weiteren orientiert.

Die Risikoankunft im Sachversicherungsgeschäft kann über "konventionelle" Wege als auch über Wege der Logik in EDV-Systemen erfolgen (wie es bei Cyber-Attacken der Fall ist). Daneben kann das betroffene versicherte Risiko materieller oder immaterieller Natur sein. Der Cyber-Versicherungsmarkt lässt sich so leicht klassifizieren und abgrenzen, wie in der folgenden Grafik gezeigt wird:



Quelle: [BLR18, S.11]

Abbildung 1.2: Klassifizierung des Cyber-Versicherungsmarktes

Zum einen finden sich hier, klar abzugrenzen, Versicherungsrisiken die in den Bereich der klassischen ("conventional") Versicherung fallen, und die im großen Stil durch eine lange Schadenshistorie und erprobte Modellierungsansätze gekennzeichnet sind. Auch Haftpflichtversicherungen fallen hierunter.

Neben der ebenfalls erwähnten Cyber-Asset-Versicherung, etwa gegen das Risiko eines Datenverlustes infolge eines Wasserschadens oder Einbruchdiebstahls, sind die in der Grafik unteren beiden Bereiche für diese Arbeit besonders relevant.

Die klassische Cyberversicherung deckt unter Anderem das Risiko der Hackerattacke, wie sie in den vorigen Absätzen beschrieben ist. Darüber hinaus existieren jedoch eine Vielzahl weiterer Risiken, die hier im Zuge des Vertragsabschlusses an das Versicherungsunternehmen übertragen werden. Diese werden noch genauer im Kapitel der expliziten Cyber-Risiken beleuchtet.

1.2 Analyse und Einschätzung des Marktes

1.2.1 Entwicklung des Prämienvolumens

Das weltweite Prämienvolumen von "klassischen" Cyberversicherungen, wie oben beschrieben, belief sich laut Report der KPMG[8] im Jahr 2016 auf etwa drei Milliarden US-Dollar. Für 2020 wurde zum Wissensstand 2017 eine Verdreifachung jener Größe auf acht bis zehn Milliarden geschätzt. Ein neuerer Bericht der Munich Re[9] schätzt den Cyberversicherungsmarkt 2020 auf über sieben Milliarden US-Dollar, den Großteil mit 5,3 Milliarden davon am US-Amerikanischen Markt und über eine Milliarde US-Dollar am europäischen Versicherungsmarkt.

[8] Vgl. [WHSJ17, S.29]
[9] Vgl. [RK20]

Bis 2025 sieht der Münchner Rückversicherer den Markt der expliziten Cyberversicherung bei einem Prämienvolumen von über 20 Milliarden US-Dollar. Besonderes Wachstum wird hier im asiatischen und europäischen Raum, bis dato Regionen mit vergleichsweise geringerer Marktpenetration, gesehen. Ein starkes Wachstum bei europäischen Versicherern zeigt auch ein Dialog-Report der europäischen Versicherungs- und Pensionskassenaufsicht, *EIOPA*, mit führenden Versicherungsunternehmen der Europäischen Union[10]: Alle daran teilnehmenden Unternehmen berichteten hier von einer stark steigenden Nachfrage nach Versicherungsschutz im Cyberbereich, unter anderem auch wegen weltweiten Hacker-Attacken wie "NotPetya" oder "Wannacry", welche durch Medienberichte global bekannt wurden und den Versicherungsnehmern das Risiko und Ausmaß eines solchen Angriffs erst bewusst gemacht haben. Auch in der Rückversicherung wird ein Anstieg des diesbezüglichen Geschäftes antizipiert.

Betroffene Industriebranchen

Die größte Nachfrage nach Cyber-Produkten sieht die Munich Re verständlicherweise in den Geschäftszweigen, die am meisten unter den in dieser Arbeit beschriebenen Attacken leiden würden: Einerseits wären dies Unternehmen, die entweder mit hochsensiblen Daten arbeiten oder deren Umsatz stark von der IT-Architektur abhängt und für die eine Betriebsunterbrechung folgenschwer wäre. Auch bei Privaten lässt sich durch meist mangelnden Schutz ein zukünftig erhöhter Bedarf nach Cyber-Produkten annehmen. Der hohen Nachfrage steht hier laut EIOPA[11] jedoch eine vergleichsweise niedrige *Abschlussquote* gegenüber. Darunter versteht man das Verhältnis der Anzahl an Versicherungsnehmern, die ein Versicherungsprodukt kaufen, zu denen, die Interesse an jenem bekunden, etwa durch Anfragen eines Angebots bei den Versicherern. Als mögliche Gründe hierfür wurde etwa folgende ausgearbeitet:

- Vergleichsweise hohe Preise aus Konsumentenperspektive
- Unterschätzen der eigenen Risikosituaiton
- Der Versicherungsnehmer ist sich bezüglich des Deckungsumfangs noch zu unsicher

1.2.2 Entwicklung des Risikos

Einblick in die derzeitige Entwicklung von Cyber-Risiken, auch und vor allem beschleunigt durch die Corona-Pandemie, bietet "Cyber Security in Österreich 2021" des Beratungsun-

[10] Vgl. [EIO18, S.10]
[11] Vgl. [EIO18, S.11]

ternehmens KPMG[12]:

Die jährlich erscheinende Studie über Cyberrisiken in der österreichischen Unternehmenslandschaft berichtet von einem rasanten Anstieg der Cyberangriffe, besonders im Jahr 2020. So wurden beispielsweise 60% von 417 befragten Unternehmen im vorangegangenen Jahr Opfer von zumindest einem klassischen Cyberangriff, davon wurde auf 79% der betroffenen Unternehmen ein Phishing-Angriff verübt. Auf den weiteren Plätzen folgen CEO-Fraud und Schadprogramme. Es sei für jedes europäische Unternehmen (ein Drittel aller weltweiten Attacken hatten ein europäisches Ziel) demnach nur mehr eine Frage der Zeit, bis auch sie sich zu den Opfern von Cyber-Kriminellen zählen können[13].

Auch bei Anzeigen im privaten Bereich wurde 2020 ein Zuwachs von 26% gegenüber 2019 auf rund 36 000 verbucht.

Durch die Pandemie ist ein beträchtlicher Teil des Datenverkehrs im Internet aus sicheren Unternehmensnetzwerken heraus in private gewandert. Grund dafür ist die Arbeit von Zuhause aus, wo eine eventuell verminderte Netzwerksicherheit einen großen, schwer kontrollierbaren Risikofaktor darstellt. Auch Programme zum Abhalten von Online-Meetings tragen zur Komplexität dieser Systeme bei, welche in absehbarer Zukunft aus bekannten Gründen und Megatrends nicht sinken wird.

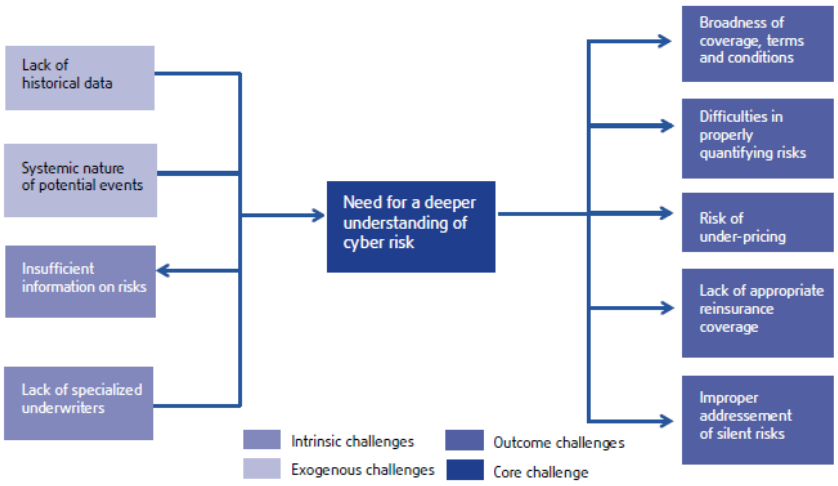
"Cyber Security in Österreich 2021" liefert auch ein aktuelles Bild zur Einstellung von Unternehmen gegenüber Cyberversicherungen[14]: Von den über 400 interviewten Firmen haben 31% bereits eine Versicherung gegen Cyberrisiken abgeschlossen, dies bedeutet ein Plus von 24% alleine zum Vorjahr. Für 17% der Unternehmen war die erstmalige Realisierung eines solchen Risikos der Grund für den Abschluss im Jahr 2020, 2019 lag dieser Wert noch etwa bei etwa 6%. Diese Trends unterstreichen auch die Prognosen zum Prämienvolumen in den vorigen Absätzen, die Situation in den österreichischen Unternehmen kann also in etwa auf den europäischen Versicherungsmarkt extrapoliert werden.

Hauptaufgaben in der Zukunft

Die EIOPA[15] fasst die hauptsächlichen Herausforderungen für die Zukunft der europäischen Versicherer in folgender Grafik treffend zusammen:

Der Kern der zukünftigen Herausforderungen liegt demnach laut Interviews mit führenden

[12] Vgl. [Lam21]
[13] Vgl. [Lam21, S.17ff]
[14] Vgl. [Lam21, S.47]
[15] Vgl. [EIO18, S.21ff]



Quelle: [EIO18, S.21ff]

Abbildung 1.3: EIOPA: Kernherausforderungen für Cyber-Risiken

europäischen Versicherungen darin, Cyberrisiken prinzipiell besser verstehen zu können. Diesem Problem stellen müssen sich nicht nur Versicherungsunternehmen, sondern auch die Endkunden: Bei Letzteren ist jedoch keine Risikomodellierung, sondern ein prinzipielles Verständnis für den eigenen Bedarf als auch die existierende Produktpalette gefragt.

Als dem obigen Kern zugrundeliegende Schwierigkeiten wird hier zwischen intrinsischen und exogenen Problemen unterschieden: Erstere umfassen den Mangel an auf Cyber spezialisierten Playern in der Versicherungsbranche, als auch unzureichende Informationen über die versicherten Risiken. Exogene Herausforderungen sind natürlich gegeben und mittelfristig nicht behebbar; Darunter fällt zum Beispiel die bis dato sehr kurze Schadenerfahrung, also die historische Datengrundlage. Weiters zählt hierzu die Natur der Schadenereignisse selbst: Durch die äußerst geringe Schadenfrequenz sowie ähnliche EDV-Architektur unter den Versicherungsnehmern (Betriebssysteme, Cloudservices) ist der Gesamtschaden, insbesondere hinsichtlich Kumulrisiken, nur schwer abschätzbar.

Aus dem Kernproblem folgende Herausforderungen werden in der Grafik als "Outcome challenges" betitelt. Darunter fallen:

- Fehler in der Risikomodellierung
- Das Unterschätzen der Risiken
- Fehlende Absicherung durch Rückversicherungsverträge

- Unzureichende Klarheit in bspw. Deckungen und Klauseln
- Mangelndes Befassen mit "Silent Cyber" - Risiken

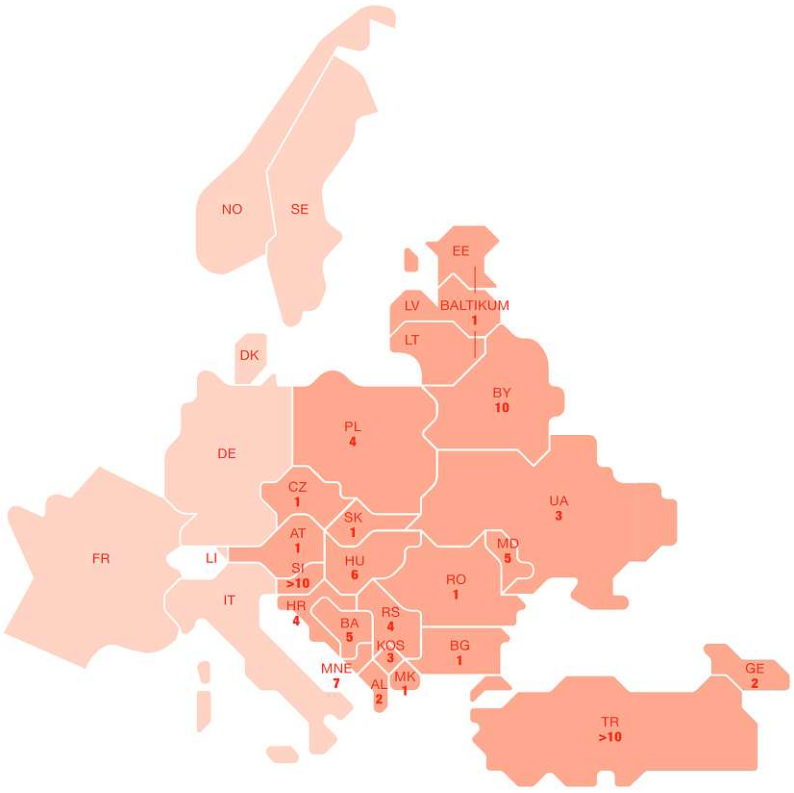
Besonders der Bewältigung von zweiterem und letzterem Problem wird sich diese Arbeit in den folgenden Kapiteln detailliert widmen. Dies geschieht am Beispiel der Wiener Städtischen Versicherung sowie ihrem Mutterkonzern, der Vienna Insurance Group.

1.3 Das Unternehmen

Diese Diplomarbeit wurde mit Unterstützung der Vienna Insurance Group, kurz VIG, verfasst. Nach dem Jahresbericht des Verbandes Österreichischer Versicherungen, VVO, ist die VIG die größte Versicherungsgruppe in Österreich mit einem Marktanteil von 23,01%[16]. Diese Kennzahl entspricht dem Anteil der verrechneten Prämien des Unternehmens am österreichischen Gesamtmarkt.

Durch eine intensive Expansionspolitik konnte sich die VIG nicht nur am österreichischen Versicherungsmarkt, sondern mittlerweile in 30 Ländern Zentral- und Osteuropas mit ihren Tochterunternehmen positionieren. Dies sowie die aktuelle Marktposition (Stand 1. bis 3. Quartal 2020, Ungarn 2019, Slowenien 1. Halbjahr 2020) der VIG-Unternehmen in den jeweiligen Ländern zeigt folgende Grafik aus dem Konzernabschluss des Unternehmens für das Jahr 2020:

[16] Vgl. [VVO21, S.64f]



Quelle: [VIG21, S.8]

Abbildung 1.4: Marktposition der VIG in CEE

Auf Konzernebene werden in dieser Arbeit Szenarien für Silent Cyber-Risiken betrachtet, quantifiziert und weiterentwickelt. Dies geschieht in Zusammenarbeit mit Zuständigen des Enterprise Risk Managements der VIG.

Die größte Tochter der Vienna Insurance Group in Österreich ist, mit einem verrechneten Prämienvolumen von derzeit knapp 3,2 Mrd. Euro, die Wiener Städtische Versicherung. In Zusammenarbeit mit dem dortigen Aktuariat für den Sachversicherungsbereich wird in dieser Arbeit die Analyse und Messung von Risikokumulen in der klassischen Cyber-Versicherung erarbeitet.

2 Explizite Cyber-Risiken

Aus dem eingangs erwähnten EIOPA-Bericht[1] ergibt sich ein repräsentatives Bild bezüglich des Umgangs mit expliziten Cyber-Risiken in europäischen Versicherungen:

Der Cyber-Studie nach zu urteilen verwenden de facto alle teilnehmenden Versicherer, welche Produkte zu jenen Risiken anbieten, zur Tarifierung ein eigenes Modell. Zwei Drittel der befragten Unternehmen greifen hier auf ein qualitatives Modell zurück, ein Drittel stützt sich auf quantitative Methoden.

Die qualitative Tarifierung basiert häufig auf Ratings mittels Fragebögen. Hier wird aufgrund von Schlüsselparametern ein Risiko-Exposure ermittelt, nach dem Standardprämien vorgeschrieben werden. Deren Höhe beruht mangels Schadenerfahrung und Wissen über das Risiko auf Expertenschätzungen und Empfehlungen von Rückversicherern: Da Cyber-Risiken oft rückversichert werden, setzt der Rückversicherer in diesen Fällen mit seinen Modellen und der entsprechenden RV-Prämie eine untere Prämienschranke für das direkte Geschäft. Auch mit dem Problem der fehlenden Daten können Rückversicherer besser umgehen, da sie die Bestands- und Rendementdaten all ihrer Kunden in die Schätzung einfließen lassen können.

Dem gegenüber steht die Tarifierung mittels quantitativer Methoden. Generell kann über diese gesagt werden, dass wirklich robuste, datenbasierte Verfahren derzeit noch in der Entwicklungsphase stecken. Gründe dafür sind wie so oft die spärlichen Datenbestände[2] sowie die sich schnell ändernde Cyber-Landschaft: Der technologische Fortschritt ist seit Jahrzehnten ungebrochen schnell und macht eine ehemals zuverlässige Analyse rasch nicht mehr zeitgemäß.

Faktoren, die laut EIOPA hier für beiderlei Tarifierungen bei Unternehmen essentiell sind, wären folgende:

- Unternehmensgröße (Umsatz und Anzahl an Mitarbeitern)
- Industriezweig/Branche

[1] Vgl. [EIO18, S.13f]
[2] (Wenngleich man sich hier durch Data Sharing helfen kann, dazu später in diesem Kapitel mehr)

- Historische Schadenerfahrung
- Deckungsumfang
- Haftungsbereiche (Geschäftssitz etc.)
- Einschätzung folgender Bereiche in Bezug auf den VN:
  - Sicherheitslevel des IT-Systems
  - Komplexität der IT-Prozesse
  - Abhängigkeit des Geschäftsbetriebes vom IT-System
- Haftungslimits und Versicherungssummen
- Rückversicherungsstruktur für das jeweilige Produkt

Für Endkonsumenten bietet es sich an, Kennzahlen für Firmenkunden wie beispielsweise die "Unternehmensgröße" evtl. durch die Anzahl der Endgeräte, den Datenverbrauch pro Monat etc. zu bestimmen.

Sollte ein Versicherungsunternehmen also überlegen, Bestands- und Rendementdaten zur Tarifierung zu sammeln, so sollten zumindest diese Merkmale enthalten sein. Dem werden wir uns später näher widmen.

In diesem Kapitel werden die derzeitigen Produkte und Klauseln der Wiener Städtischen vorgestellt, welche explizit Cyber-Risiken decken. Folgend werden Risikokumule im Allgemeinen näher beleuchtet und in Kontext mit Cyber gebracht. Dazu werden Methoden zur Kumulschätzung präsentiert sowie der derzeitige Ansatz der Wiener Städtischen zur Kumulkontrolle besprochen. Abschließend werden ein quantitativer Ansatz zum Risikomanagement im expliziten Cyber-Bereich ausgearbeitet und diesbezügliche Anforderungen an das Datenmanagement gestellt.

2.1 Formen von Cyber-Versicherungen in der WSTV

Grob wird in der Produktpalette der Wiener Städtischen Versicherung zwischen dem Geschäft mit Privatkunden und dem mit Firmenkunden unterschieden. Daraus ergeben sich die Bezeichnungen des "Zivilgeschäfts" respektive des "Firmengeschäfts". Für jeden dieser beiden Zweige existieren eigene Produkte, die an die Risikoexponierung der jeweiligen Kundengruppe angepasst sind, und bei denen Deckungen in Bezug auf Cyber-Risiken vorkommen:

2.1.1 Produkte im Zivilgeschäft

Internet-Rechtsschutz

Der "Internet-Rechtsschutz" ist ein Baustein in der klassischen Rechtsschutzversicherung. Er deckt die Kosten von Rechtsmitteln bei "typischen" Cybercrime-Fällen, diese wären[3]:

- Aktiver bzw. passiver Urheber-Rechtsschutz: Deckt die Konsultation eines Rechtsbeistands bei Verdacht respektive Vorwurf der Urheberrechtsverletzung im Internet[4]
- Unterlassungs-Rechtsschutz: Deckt Kosten für die Einbringung einer Unterlassungsklage, zum Beispiel bei Rufschädigung im Internet
- Aktiver bzw. Passiver Internet-Straf-Rechtsschutz: Übernimmt die Kosten bei einer Straftat im Internet. Der aktive oder passive Schutz unterscheidet hier, ob der Versicherungsnehmer Geschädigter oder Schädiger ist (eine Ausnahme gilt hier beim passiven Rechtsschutz bei Vorsatzdelikten)
- Schadenersatz-Rechtsschutz: Kommt bei der Realisierung von Ersatzansprüchen durch die missbräuchliche Verwendung personenbezogener Daten zum Tragen
- Internet-Vertrags-Rechtsschutz: Schützt die rechtlichen Interessen des Versicherungsnehmers hinsichtlich Vertragsstreitigkeiten
- Internet-Mobbing- und Stalking-Rechtsschutz: Sichert die rechtliche Erstberatung in Mobbing- und Stalking-Fällen

Eine Vielzahl an anschaulichen Fällen fällt in diesen Deckungsbereich, etwa Bestellbetrug oder Phishing-Mails. Die maximale Deckungssumme beträgt hier 2.500 Euro pro Versicherungsjahr.

Pay Protect (Haushalt, Eigenheim, Agrar)

Auch bei "Pay Protect" handelt es sich um einen Deckungsbaustein, der mittels Klausel rechtlich im Versicherungsvertrag verankert ist und bei Haushalts-, Eigenheim- und Agrarversicherungen optional inkludierbar ist. Hier wird ein Kostenersatz etwa bei folgenden Schadenereignissen vorgenommen[5]:

- Missbrauch bei Einzugsermächtigungen von Bankomatkarten

[3] Vgl. [WST20d]
[4] Anmerkung: Bei aktivem Rechtsschutz geht es zumeist um das Durchsetzen des eigenen rechtlichen Interesses beziehungsweise eigenen Ersatzansprüchen. Passiver Rechtsschutz behandelt andererseits das Abwehren von Forderungen, Klagen oder Abmahnungen Dritter.
[5] Vgl. [WST17]

- Missbräuchliche Verwendung von Kreditkarten, mit oder ohne PIN-Code
- Schäden durch Phishing im Online-Banking-Bereich
- Abhandenkommen von Zahlungsmitteln und Inhalten von Bankschließfächern bei Einbruchdiebstahl oder Beraubung

Wenngleich die obigen Versicherungsfälle nicht immer unmittelbar in Zusammenhang mit Cyber-Kriminalität stehen, so muss auch diese Klausel bei der Betrachtung von Kumulszenarien betrachtet werden. Diese partielle Exponierung gegenüber Cyberrisiken trifft bei einer Vielzahl von Versicherungsprodukten zu, weshalb hier erhöhte Sorgfalt in der Analyse gefragt ist. In diesem Fall ist die Deckungssumme mit 2.500 Euro pro Jahr gedeckelt.

Haushalt Extra

"Haushalt Extra" ist eine Deckungsvariante in der Haushaltsversicherung, welche sich ebenfalls in Form einer Klausel im Versicherungsvertrag manifestiert. Sie enthält einige Deckungsverbesserungen betreffend konventionellen Versicherungsbereich. Zusätzlich beinhaltet sie folgende, für diese Arbeit relevante Erweiterungen[6]:

- Telefon-/Internetmissbrauch: Deckt Folgeschäden aus einem Einbruch oder Raub in Form von missbräuchlicher Verwendung von Handy und Internet des Versicherungsnehmers
- Schutz vor Bankomat- und Kreditkartenmissbrauch im Zuge von Finanztransaktionen
- Schadenersatz im Fall von Phishing beim Online-Banking

Die Deckungsbereich des Produkts "Pay Protect" ist hier also in der Deckungserweiterung weitgehend inkludiert. Die maximale Deckungssumme beträgt auch hier 2.500 Euro pro Versicherungsjahr.

Sicherheit zum Recht

Der letzte hier besprochene Baustein betrifft ebenfalls die Rechtsschutz-Versicherung, die insgesamte Deckungssumme ist jedoch keine absolute Zahl, sondern vom Umfang der klassischen Rechtsschutzversicherung abhängig. Versichert sind hier folgende Sub-Bausteine[7]:

- Passiver beziehungsweise Aktiver Urheber-Rechtsschutz: Deckung bei Verletzung des Urheber-, Marken-, Muster- oder Patentrechts.

[6] Vgl. [WST19]
[7] Vgl. [WST20c]

- Unterlassungs-Rechtsschutz: Analog zu obigem für den Schutz des eigenen rechtlichen Interesses bei zum Beispiel Beleidigungen im Internet
- Aktiver Internet-Straf-Rechtsschutz: Kostenersatz für das Einbringen von u.A. Strafanzeigen
- Internet-Mobbing- und Stalking-Rechtsschutz: Deckt wie oben die rechtliche Erstberatung im Versicherungsfall ab

Die Deckungslimits sind hier pro Leistungsbaustein mit 0,6% der Rechtsschutz - Versicherungssumme begrenzt, insgesamt sind die Leistungen aus dem Baustein mit 3% der Versicherungssumme nach oben beschränkt.

2.1.2 Produkte im Firmen- und Gewerbegeschäft

Neben einem online abschließbaren Produkt für den grundlegenden Schutz von KMU gegen Cyber-Risiken, "Cyber Basic", bietet die WSTV mit "Cyber Protect" genauso ein maßgeschneidertes Produkt für Unternehmen, Gemeinden etc. gegen solche Gefahren an. Ergänzend findet sich mit "Cyber Industrie" ein Spezialprodukt mit eigener Rückversicherungsstrategie an.

Cyber Basic

Dieses Produkt bietet sich für KMU bis zu einem Jahresumsatz von 2 Millionen Euro an. Da es sich hier um ein eigenständiges Produkt handelt, fokussieren sich auch die vorvertraglichen Obliegenheiten auf das IT-System des Versicherungsnehmers: Unter anderem wird die Verschlüsselung aller mobilen IT-Geräte vorausgesetzt, ebenso die Installation einer Antivirus-Software. Gedeckt wird dafür folgendes[8]:

- Übernahme von Krisenmanagement-Kosten
- Ausgleich des wirtschaftlichen Schadens durch Betriebsunterbrechung
- Kosten, die durch die Wiederherstellung von Datenträgern entstehen
- Forderungen Dritter wegen Datenschutzverletzungen infolge einer Manipulation (also auch ein Baustein mit Haftpflicht-Charakter)

Zusätzlich bietet die Wiener Städtische den Versicherungsnehmern eine eigene Cyber-Hotline im Notfall an. Das Produkt ist online abschließbar und die Versicherungssummen sind fix vorgegeben.

[8] Vgl. [WST20b]

Ein großer Teil der versicherten Unternehmen greift oft nicht zu diesem Basis-Produkt, sondern schließt das folgende Premium-Produkt mit individueller Versicherungssumme ab:

Cyber Protect

"Cyber Protect" ist das meistgewählte Cyber-Produkt im Firmen- und Gewerbegeschäft. Grundlage für den Abschluss ist eine Bedarfserhebung durch einen dazu befugten Betreuer (z.B. Versicherungsmakler oder -agenten). Gedeckt werden von dieser Versicherung einige Hauptleistungen, die in ihrer Versicherungssumme von 100.000 bis 1 Million Euro angepasst werden können. Im Allgemeinen geht es hier um Vermögensschäden, die unter folgenden Umständen enstehen[9]:

- Datenverlust, -diebstahl oder Manipulation
- Offenlegung personenbezogener Daten
- Forderungen Dritter durch Weitergabe von Schadprogrammen auf fremde IT-Systeme
- Der Kostenersatz für die Bestellung von Cyber Security-Fachkräften
- Passive Rechtskosten beim Verdacht der Datenschutzverletzung
- Mitteilungskosten an Betroffene

Versichert sind hier reine Vermögensschäden und keine Sach- oder Personenschäden beziehungsweise Lösegeldzahlungen. Zusätzlich können Deckungserweiterungen je nach Bedarf des Versicherungsnehmers abgeschlossen werden. Solche wären beispielsweise der Versicherungsschutz bei Betriebsunterbrechung oder ein Kostenersatz für zusätzliches Krisenmanagement.

Cyber Industrie

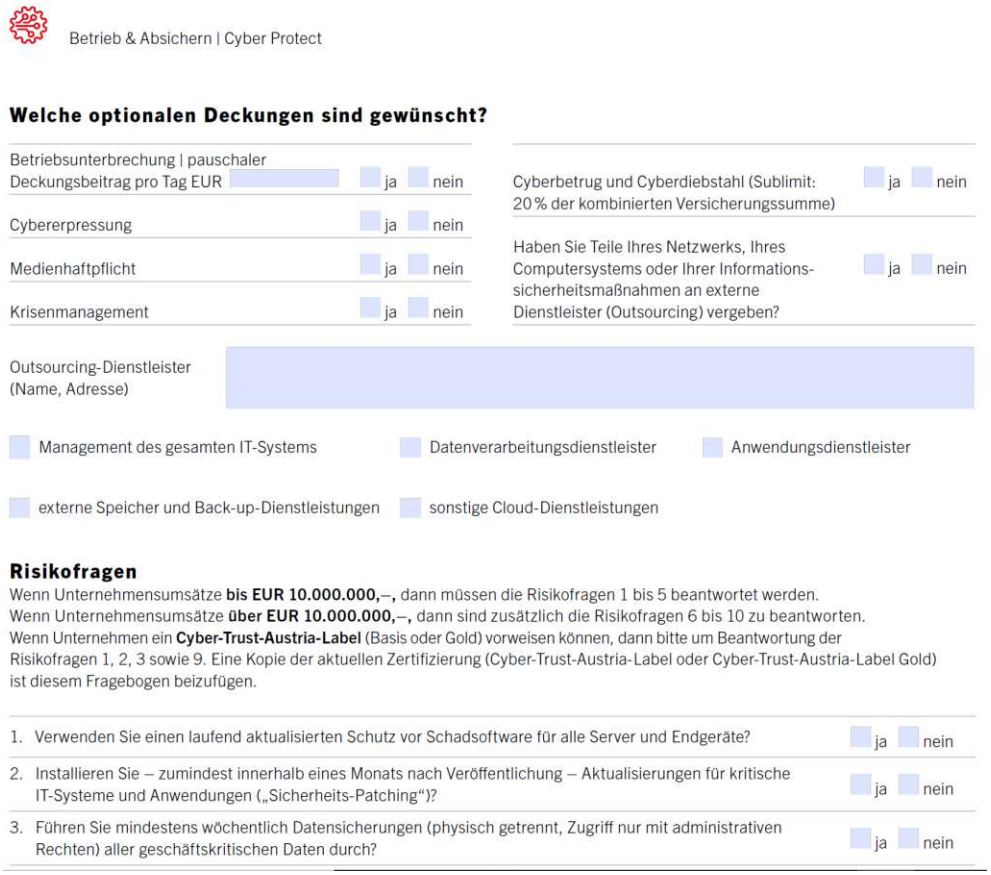
"Cyber Industrie" ist ein Spezialprodukt der Wiener Städtischen für große Unternehmen, bei denen die maximale Deckungssumme von "Cyber Protect" nicht ausreichen würde. Die Bedingungen für den Risikotransfer werden für jedes Unternehmen einzeln ausverhandelt, der Deckungsumfang bewegt sich jedoch in der gleichen Richtung wie die anderen beiden Cyber-Versicherungen für Unternehmen und Gemeinden.

[9] Vgl. [WST20a]

2.1.3 Derzeitige Tarifierung von Cyber-Risiken

Die Tarifierung von obigen Cyber-Produkten ist vielfältig und richtet sich hauptsächlich nach dem Wesen und der Rückversicherungsstrategie des Produktes. Beispielhaft betrachten wir im Folgenden das Produkt "Cyber Protect" für Firmen/Gemeinden beliebigen Jahresumsatzes:

Dieser Tarif wird verglichen mit den anderen Firmen- und Gewerbegeschäfts-Produkten am Häufigsten abgeschlossen. Ihm wird auch ein hohes Wachstum prognostiziert, dazu jedoch später mehr. Bei Antragstellung durch einen dazu befugten Außendienstmitarbeiter, Makler oder dergleichen wird zusammen mit dem zukünftigen Versicherungsnehmer ein Fragebogen ausgefüllt. Folgend ein Ausschnitt aus ebenjenem, das gesamte Dokument ist dieser Arbeit angehängt:



Betrieb & Absichern | Cyber Protect

Welche optionalen Deckungen sind gewünscht?

Betriebsunterbrechung | pauschaler Deckungsbeitrag pro Tag EUR ☐ ja ☐ nein

Cybererpressung ☐ ja ☐ nein

Medienhaftpflicht ☐ ja ☐ nein

Krisenmanagement ☐ ja ☐ nein

Cyberbetrug und Cyberdiebstahl (Sublimit: 20 % der kombinierten Versicherungssumme) ☐ ja ☐ nein

Haben Sie Teile Ihres Netzwerks, Ihres Computersystems oder Ihrer Informationssicherheitsmaßnahmen an externe Dienstleister (Outsourcing) vergeben? ☐ ja ☐ nein

Outsourcing-Dienstleister (Name, Adresse)

☐ Management des gesamten IT-Systems ☐ Datenverarbeitungsdienstleister ☐ Anwendungsdienstleister

☐ externe Speicher und Back-up-Dienstleistungen ☐ sonstige Cloud-Dienstleistungen

Risikofragen

Wenn Unternehmensumsätze **bis EUR 10.000.000,–**, dann müssen die Risikofragen 1 bis 5 beantwortet werden.
Wenn Unternehmensumsätze **über EUR 10.000.000,–**, dann sind zusätzlich die Risikofragen 6 bis 10 zu beantworten.
Wenn Unternehmen ein **Cyber-Trust-Austria-Label** (Basis oder Gold) vorweisen können, dann bitte um Beantwortung der Risikofragen 1, 2, 3 sowie 9. Eine Kopie der aktuellen Zertifizierung (Cyber-Trust-Austria-Label oder Cyber-Trust-Austria-Label Gold) ist diesem Fragebogen beizufügen.

1. Verwenden Sie einen laufend aktualisierten Schutz vor Schadsoftware für alle Server und Endgeräte? ☐ ja ☐ nein
2. Installieren Sie – zumindest innerhalb eines Monats nach Veröffentlichung – Aktualisierungen für kritische IT-Systeme und Anwendungen („Sicherheits-Patching")? ☐ ja ☐ nein
3. Führen Sie mindestens wöchentlich Datensicherungen (physisch getrennt, Zugriff nur mit administrativen Rechten) aller geschäftskritischen Daten durch? ☐ ja ☐ nein

Quelle: Wiener Städtische Versicherung AG

Abbildung 2.1: Ausschnitt aus dem Cyber Protect-Fragebogen

Fragebögen als Underwriting-Werkzeug dienen Versicherungsunternehmen in zweierlei Hinsicht: Zum Einen erhält die Versicherung so **Informationen über den Versicherungsnehmer und das versicherte Risiko**. Basierend darauf kann eine Annahmeentscheidung und später die Tarifierung stattfinden.

Zum Anderen können die Angaben aus dem Fragebogen, falls sie im späteren Vertrag übernommen werden einen **rechtlich bindenden Charakter** bekommen. Im Falle der Risikofrage Nummer 2 aus 2.1 zum Beispiel führt eine Beantwortung mit "ja" etwa zu einer Verpflichtung seitens des Versicherungsnehmers, Updates für die kritischen IT-Systeme zeitgerecht durchzuführen. Ist irgendwann das Gegenteil der Fall, so gilt dies als Änderung des Risikos. Bei entsprechender Vertragsgestaltung könnte dies sogar in einer Obliegenheitsverletzung enden; Dem Versicherer würden in diesem Fall Leistungsfreiheit sowie ein außerordentliches Kündigungsrecht zustehen[10].

Insgesamt werden im Risikofragebogen Informationen zum Unternehmen, Sensibilität der Datensätze, Deckungsumfang, Schadenshistorie sowie zum Verhalten des Kunden hinsichtlich Cyber-Sicherheit erfragt und an den Versicherer weitergeleitet. Verglichen mit den Faktoren, welche die EIOPA als besonders wichtig für das Risikomanagement und die Tarifierung sieht, überdecken sich beide Listen großteils. Zwei Faktoren werden jedoch nicht beziehungsweise nicht sehr detailliert erfragt:

- Die Abhängigkeit des Geschäftsbetriebes vom IT-System wird nur indirekt über den Umsatz durch E-Commerce eruiert
- Die Komplexität der IT-Prozesse oder die verwendeten Programme werden nicht aufgenommen

Nach den Angaben aus dem Versicherungsantrag wird ein Rating des Kunden durchgeführt. Darauf basiert dann die schlussendliche Versicherungsprämie. Dies erfolgt in einem eigenen Tarifierungstool. Die Gesamtprämie setzt sich aus einer Basisprämie B sowie der Prämie für optionale Deckung O zusammen, welche jeweils als Produkt aus einem Grundbetrag π_g multipliziert mit mehreren Zuschlags- oder Nachlassfunktionen $\mu_i(x_i)$ darstellbar ist:

$$B = \pi_g \cdot \prod_{i=1}^{6}(1 + \mu_i(x_i))$$

Der Grundbetrag richtet sich nach der gewählten Versicherungssumme und dem Risikoexposure des Kunden, welches je nach Industriezweig in drei Klassen eingeteilt ist.

[10] Vgl. §6 VersVG 2012

Analog zu oben berechnet sich die Prämie für die optionale Deckung, wobei die Berechnungsgrundlage hier als Summe der einzelnen gewünschten "Bausteinprämien" darzustellen ist.
Der Vektor $(x_i)_{1\leq i\leq 6}$ enthält hier alle für die Tarifierung wichtigen Daten aus dem Fragebogen. Diese wären:

- Jahresumsatz des Unternehmens
- Anzahl an Sätzen mit sensiblen Daten im IT-System
- Anteil des Umsatzes, der in den USA erwirtschaftet wird
- Gewählter Selbstbehalt
- Beauftragung eines Outsourcing-Providers
- Anzahl von "Ja"-Antworten auf die Risikofragen im Fragebogen

Da ein Großteil des versicherten Risikos in diesem Fall an einen Rückversicherer transferiert wird, orientiert sich die Wiener Städtische hier an den entsprechenden Prämienempfehlungen. Wie oben erwähnt, haben diese Unternehmen durch große Datenbanken und globale Expertise bei Cyberprodukten die Fähigkeit, qualitativ hochwertige Prämienempfehlungen an die Erstversicherer abzugeben.

Auch wie hoch und in welche Bereiche die Deckung eines solchen Produkts fällt, wird häufig von den Rückversicherungsunternehmen indirekt festgelegt.

In der Praxis leisten Rückversicherer sowie Rückversicherungsmakler zudem mehr als nur den reinen Risikotransfer: Sie helfen bei der Produktgestaltung, bieten Modelle für verschiedenste Szenarien (Naturkatastrophen, Kumulquantifizierung etc.) an und unterstützen mit verschiedensten Tools, Reports und Branchenvergleichen die Erstversicherer. Dies wird zum Teil kostenpflichtig, aber zu einem großen Teil auch kostenlos angeboten, um den Abschluss eines Rückversicherungsvertrages beim jeweiligen Unternehmen zu motivieren.

2.1.4 Bestandsprojektion für die Wiener Städtische

Im Folgenden wollen wir eine Bestandsprojektion für den Bestand an Cyberprodukten der Wiener Städtischen durchführen. Dazu betrachten wir für jedes der sieben Produkte bzw. Deckungsbausteine die Stückzahlen im Bestand der Wiener Städtischen pro Quartal seit dem 31.12.2018[11]. Die Anzahl an Verträgen ist aus Datenschutzgründen auf den ersten Stichtag, zu dem es einen Vertrag gibt, normiert. Der Ausgangswert beträgt hier 100.

Produkt	12/18	03/19	06/19	09/19	12/19	03/20	06/20	09/20	12/20	03/21	06/21
Internet-RS	100	108	120	127	133	145	145	144	144	145	145
PayProtect	100	104	108	112	114	112	115	114	112	109	105
Haushalt Extra	-	-	100	469	5753	15490	29288	46457	65369	86231	107055
Sicherheit zum Recht	-	-	-	-	-	-	100	1912	3810	6157	8320
Summe RS-Produkte	100	108	120	127	133	145	149	214	284	371	450
Cyber Protect	100	102	107	110	113	119	120	126	128	127	129
Cyber Basic	-	100	200	200	200	200	200	200	200	200	200
Cyber Industrie	-	-	100	100	150	200	200	200	200	200	250

Tabelle 2.1: Bestandsentwicklung der Wiener Städtischen in Stück aufrechter Verträge seit 2018

Die Bestandsentwicklung der Produkte ist durchaus verschieden: Bleiben die Zahlen des Produkts "PayProtect" seit Dezember 2018 beispielsweise eher konstant, so ist im Gegenzug im Breitenbereich bei den Rechtsschutz- und Haushaltsbausteinen ein starker Anstieg zu vermerken. Dies und die unterschiedlichen Charakteristika der verschiedenen Produkte machen eine Prognose auf Einzelproduktebene sinnvoll.

Nach einer Vorstellung der derzeitigen Prognosemethode wollen wir auf eben dieser granularen Basis eine Vertragsprojektion vornehmen. Hier ist ein Verständnis des Kontexts, aus denen manche Datenentwicklungen resultieren, essentiell. Nur mit ausreichend Hintergrundwissen und Expertise kann im Tätigkeitsbereich eines Aktuars fundierte Analysearbeit stattfinden.

Derzeitige Prognose

Die derzeitige Abschätzung der Vertragszahl und damit der Versicherungssumme findet bei der Wiener Städtischen derzeit in einer internen Excel-Datei statt. Sie wurde im Herbst 2020 vorgenommen, als "Sicherheit zum Recht" beispielsweise erst ein halbes Jahr am Markt war. DI Dr. Michael Schlögl stufte als Leiter des Aktuariats Sachversicherung eine vernünftige Prognose auf Basis der damals vorliegenden Daten als schwer möglich ein,[12] weshalb man sich hier eines simpleren, interimistischen Ansatzes bediente:

Je Produkt wurde das arithmetische Mittel aller absoluten Änderungen als Schätzer für den Zuwachs pro Quartal ermittelt. Mittels Expert Judgement adjustiert ergibt sich nach diesem linearen Ansatz folgende Einschätzung für die Bestandsentwicklung (entsprechend normiert, sodass die Zahlen mit der obigen Tabelle abgestimmt sind):

Produkt	Erwarteter Zuwachs pro Quartal in Stück
Internet-RS	-6,58
PayProtect	+2,1
Haushalt Extra	+12893,95
Sicherheit zum Recht	+1796,4
Cyber Protect	+3,55

Tabelle 2.2: Derzeitige Cyber-Bestandsprognose pro Quartal

Es wurde darauf verzichtet, eine Einschätzung zu den Produkten "Cyber Basic" und "Cyber Industrie" abzugeben, da hier der Bestand insgesamt nur wenige Verträge umfasst und

[11] Quelle: Interne Cyber-Analyse der WSTV
[12] Vgl. Interview mit Herrn Schlögl per E-Mail am 04.08.2021

damit eine Prognose ungeeignet erscheint. Auch der neue Prognoseansatz konzentriert sich auf die restlichen fünf Bausteine/Tarife:

Entwicklung einer neuen Projektion

Ausgehend von obiger Tabelle wollen wir nun ein neues Prognosemodell erstellen. Zur Modellierung bietet sich hier eine Sigmoidfunktion, also eine Affintransformation des Tangens Hyperbolicus an[13]:

$$s(t) := \frac{1}{1+e^{-t}} = \frac{1+\tanh(\frac{t}{2})}{2}$$

Als Generalisierung dieses Funktionentyps betrachten wir die logistische Funktion in Abhängigkeit von der Zeit t, einer Asymptote (=Marktkapazität) G, einem Wachstumsfaktor k und dem Zeitpunkt c, welcher die Wendestelle der Funktion markiert:

$$f(t) := \frac{G}{1+e^{-k\cdot(t-c)}}$$

Logistische Wachstumsmodelle werden in quantitativen Prognosen schon seit einiger Zeit verwendet. Klassische Anwendungsgebiete sind die Vorhersage des Absatzes langlebiger, nicht ersetzbarer Konsumgüter oder Abonnement-Services[14]. Ein Versicherungsvertrag ist durch seinen Laufzeit-Charakter und der klassischen Kundentreue hier ein geeigneter Anwendungsfall.

Wir betrachten je Produkt im Folgenden zuerst eventuelle Besonderheiten und leiten G aus Bestandsdaten der Wiener Städtischen und Analysen der Versicherungswirtschaft her. Den Wachstumsfaktor kalibrieren wir mittels der Bestandszahlen der letzten drei Jahre:

Wie oben schon erwähnt, werden wir die beiden Produkte "Cyber Basic" und "Cyber Industrie" keiner logistischen Modellierung unterziehen.

PayProtect

Im "PayProtect"-Produkt lässt sich in der Tabelle kein nachhaltiges Wachstum feststellen. Die ursprüngliche Prognose mit $+2,1$ Verträgen pro Quartal ist für das Jahr 2019 nachvollziehbar, über den gesamten Zeitraum ist jedoch eher eine Stagnation zu vermerken. Insbesondere seit dem Inkrafttreten der konkurrierenden Tarifbausteine "Sicherheit zum Recht" und "Haushalt Extra" aus den anderen Sparten ist sogar eine leichte Abnahme der Vertragszahl zu vermerken.

[13] Vgl. [Sig21]
[14] Vgl. [Sok08, S.2ff]

Aus der Bestandshistorie und der Konkurrenz durch eine neue Produktgeneration zu schließen, ist die Prognose für diesen Tarifbestand eine Stagnation mit Wert 105.

Rechtsschutz-Bausteine

Die beiden Cyber-Bausteine der Rechtsschutzversicherung, "Internet-Rechtsschutz" und "Sicherheit zum Recht" sind in ihrem Deckungsumfang recht ähnlich aufgebaut. Zusätzlich wird ersteres Produkt in einem älteren EDV-System verwaltet. Dieses soll in den nächsten Jahren durch eine neue SAP-Lösung komplett abgelöst werden. In ebenjenem System wird "Sicherheit zum Recht" verwaltet. Dies begründet das starke Wachstum beim neueren Produkt und die rückläufigen Bestandszahlen beim älteren Produkt.

Es würde demnach mittel- und langfristig keinen Sinn machen, sowohl "Internet-RS" (da dieses Produkt bald nicht mehr angeboten wird) als auch "Sicherheit zum Recht" (durch kurzfristig interne Konkurrenz zum Altprodukt) alleine zu modellieren. Daher prognostizieren wir den Bestand beider Rechtsschutzprodukte zusammen. In 2.1 ist diese Summe von Beständen bereits unter "Summe RS-Produkte" normiert worden.

Nun zur Obergrenze G: Beide Rechtsschutzprodukte stellen einen Zusatzbaustein zu einem klassischen Rechtsschutzprodukt dar. Zusätzlich ist die Rechtsschutzversicherung in Österreich und in der Wiener Städtischen schon lange etabliert. Es ist also anzunehmen, dass die Anzahl dieser Bausteine gegen die derzeitig Bestandszahl mal einer "Durchdringungsrate" konvergiert, was sowohl durch Neuabschlüsse, Produktwechsel oder auch Deckungserweiterungen stattfinden kann.

Um diese Rate zu schätzen, wurde aus allen bis zur Berechnung in 2021 produzierten Rechtsschutz-Verträgen der Anteil der Cyber-Bausteine ermittelt. Die Durchdringungsrate beträgt demnach aktuell 82%[15]. Die (normierte) Bestandszahl beträgt 3729, weshalb wir hier auf eine natürliche Obergrenze von

$$3729 \cdot 0.82 = 3057.78$$

kommen. Das Fitten der Modellfunktion erfolgt mittels R in der Version 4.0.3 unter Verwendung der internen iterativen Funktion "`nls`" und der Kleinsten-Quadrate-Methode. Die Funktion benötigt Anfangswerte, die durch "Ausprobieren" gewählt werden, sodass die erste Kurveniteration optisch in der Nähe der Datenpunkte liegt. Der Code dazu ist im Anhang unter 8.2 angefügt. Die vorläufige Wachstumskurve besitzt folgende Gestalt mit den optimalen Parametern $k = 0.2081$, $c = 19.7510$:

[15] Stand: 13. August 2021

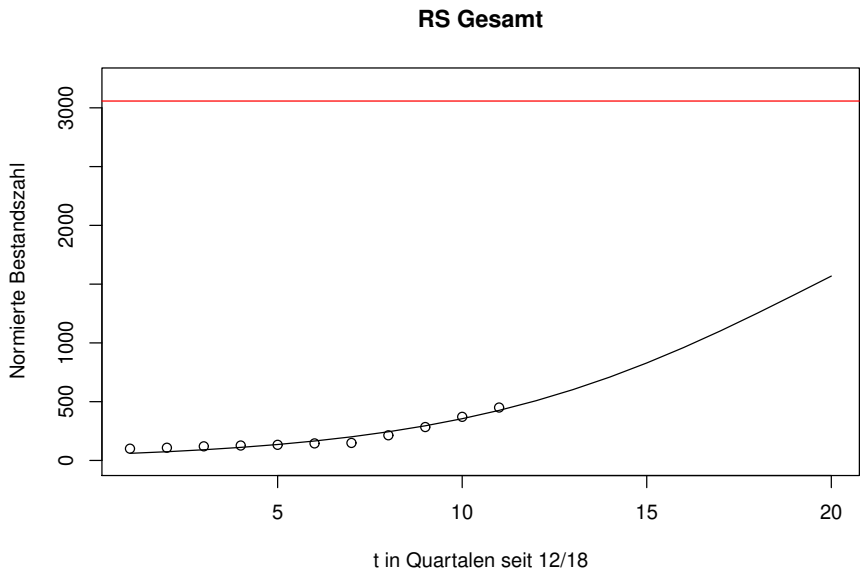


Abbildung 2.2: Bestandsprognose der Rechtsschutz-Cyberbausteine

Die rote Linie in der obigen Abbildung kennzeichnet die natürliche Grenze G.

Um die Kurve endgültig in Reports, Präsentationen etc. im Unternehmensumfeld einbauen zu können, fordern wir eine Nebenbedingung: Die modellierte Kurve muss den letzten Datenpunkt-IST zum Zeitpunkt t_{last} schneiden, um eine Extrapolation "aus diesem Punkt heraus" erklären zu können. Dazu modifizieren wir die Modellfunktion $f(t)$ um einen Strafterm mit Gewicht α:

$$f(t) := \frac{G}{1 + e^{-k \cdot (t-c)}} + \alpha \cdot (\frac{G}{1 + e^{-k \cdot (t_{last}-c)}} - Bestand(t_{last}))$$

Damit hat der Abstand der Funktion vom letzten Datenpunkt einen $\alpha + 1$ fachen Beitrag zum Gesamtfehler in den einzelnen Iterationsschritten. α ist in Abhängigkeit der Obergrenze G zu wählen, in diesem speziellen Fall konnte mit dem Gewicht $\alpha = 100$ eine ausreichende Annäherung gefunden werden. Die endgültigen Parameter betragen $k = 0.3603$ und $c = 15.8723$, und die Kurve sieht wie folgt aus:

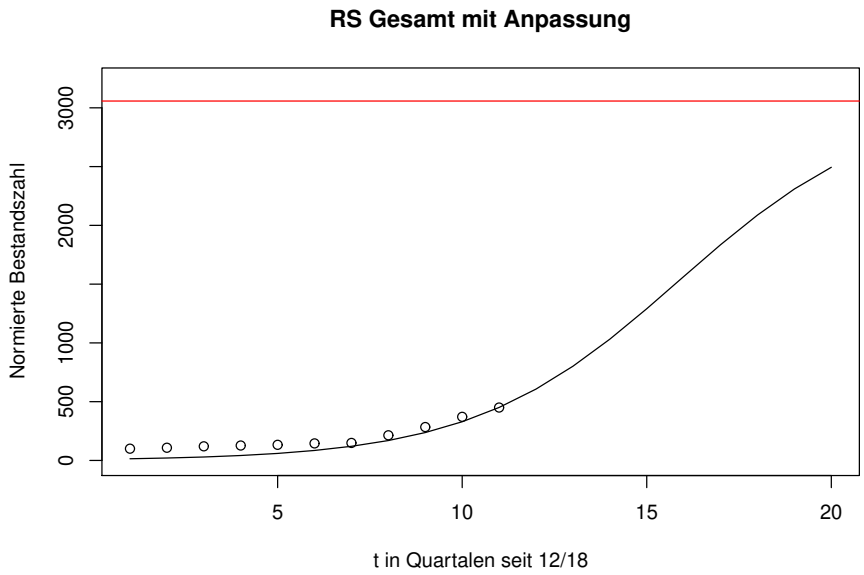


Abbildung 2.3: Bestandsprognose der Rechtsschutz-Cyberbausteine mit Anpassung

Durch die große Abhängigkeit vom letzten Datenpunkt ist zu erwarten, dass sich diese Kurve mit dem Hinzufügen eines neuen Datenpunktes zum nächsten Quartal stärker ändern wird als die Version ohne Nebenbedingung. Auf jeden Fall aber ist der Anstieg der Vertragsanzahl gut erklärbar abgebildet.

Durch Ablesen der Funktionswerte der Wachstumskurve kann nun eine fundierte Bestandsprognose in Präsentationen und Reports stattfinden. Ebenfalls werden wir die Bestandszahlen später für die Cyber-Kumulabschätzung verwenden.

Haushalts-Bausteine

Der Produktbaustein "Haushalt Extra" wird ebenfalls gesondert modelliert. Dabei kann die komplette Vorgangsweise, die bei den Rechtsschutz-Bausteinen angewandt wurde, analog verwendet werden:

Die Obergrenze G ergibt sich aus dem Produkt der normierten Bestandszahl an Haushaltsverträgen und der entsprechenden Cyber-Durchdringung. Erstere stammt aus einer internen Verlaufsauswertung und beträgt 578000. Die von 01. Jänner 2021 bis 31. August 2021 abgeschlossenen Verträge beinhalten laut SQL-Abfrage zu 92.7% den Baustein "Haushalt Extra", womit sich eine Grenze von $G = 535806$ ergibt.

Die Werte der Parameter k und c betragen in der Modellierung ohne Nebenbedingungen 0.3945 respektive 12.3246. Die daraus resultierende Kurve sowie das Ergebnis der angepassten Bestandsmodellierung ($k = 0.3465$, $c = 13.0044$) ist in den folgenden Abbildungen zu sehen:

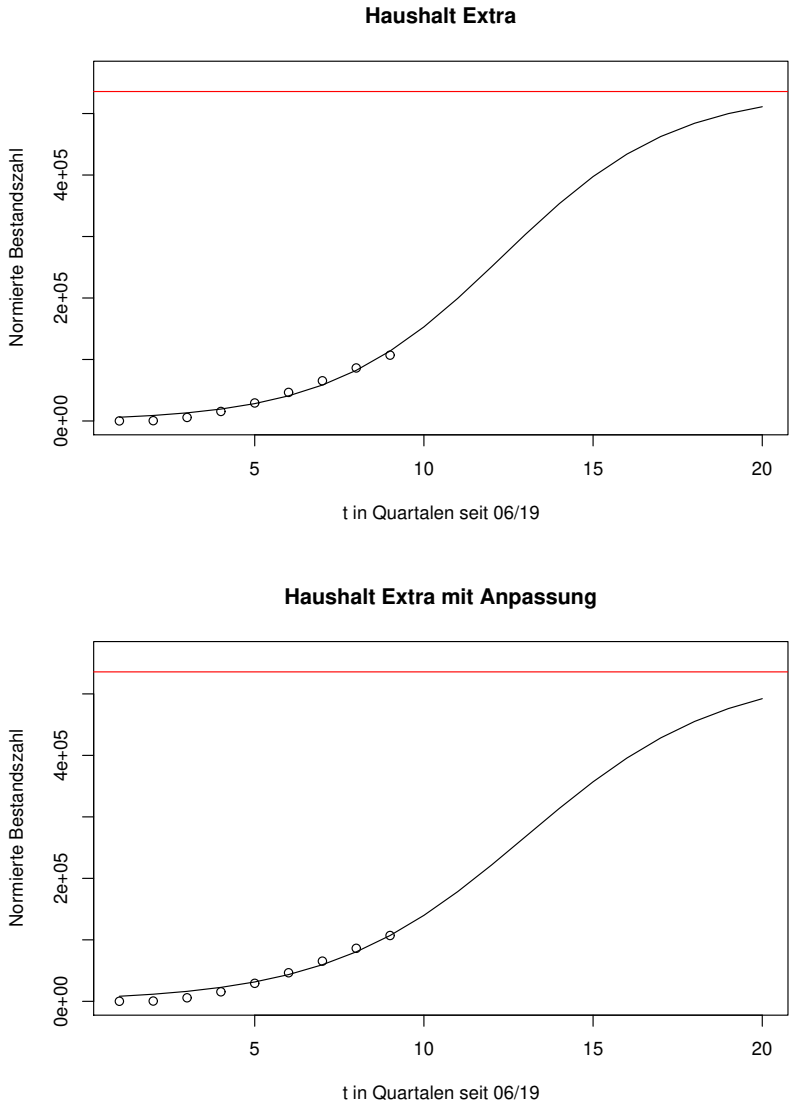


Abbildung 2.4: Bestandsprognose der Haushalts-Cyberbausteine mit und ohne Anpassung

Cyber Protect

Im Firmen- und Gewerbegeschäft bietet "Cyber Protect" ein absolutes Novum für den Aktuar: Es ist nur begrenzt bis gar nicht mit klassischen Produkten dieses Geschäftszweigs vergleichbar. Die Haftpflichtkomponenten von "Cyber Protect" ließen sich zwar mit der gewerblichen Haftpflichtversicherung vergleichen, das Hauptwesen der Produktschiene (Eigenschaden bei Hackerangriffen, Assistanceleistungen) ist jedoch in der Art nicht in der Historie der gewerblichen Versicherung vorzufinden.

So ist es auch kein Leichtes, bei diesem Produkt ein "Marktpotential" herauszufinden. Oft ist in der Literatur und in Experteninterviews von Prämieneinschätzungen die Rede, etwa in einem Interview des *Gesamtverbands der Deutschen Versicherungswirtschaft* mit Onnen Siems[16]: Der Gründer und Geschäftsführer einer großen Gesellschaft für aktuarielle Beratung erwartet in Deutschland ein Prämienpotential von über einer Milliarde Euro. Ähnlich sieht es die KPMG in ihrer Studie "Cyber-Versicherung: Versicherungssparte der Zukunft"[17]:

Die Cyber-Experten des Big Four-Unternehmensberaters erwarten eine Verfünffachung des Marktes in der DACH-Region, also in Deutschland, Österreich und Schweiz. Für diese Länder wird ein Prämienpotential von bis zu einer Milliarde Euro gesehen.

Prämienvolumina sind jedoch keine Kennzahlen, mit denen zuverlässige Bestandsschätzungen möglich sind. Im Cyber-Geschäft werden Prämien klassischerweise noch recht hoch angesetzt, da es viele Unsicherheiten am Markt gibt, insbesondere was die zukünftige Schadenentwicklung anbelangt. Deshalb und weil die Cyber-Produkte der deutschsprachigen Versicherungsunternehmen nicht immer direkt vergleichbar sind, lässt sich hier aus Prämienpotentialen kein zukünftiger Bestand ablesen. Auch ist der zukünftige Anteil der Wiener Städtischen an diesem Markt nicht genau abschätzbar.

Da es generell in der Literatur wenige Expertenschätzungen zu diesem Thema gibt, konzentrieren wir uns auf das Teilergebnis der KPMG-Studie: Die Verfünffachung des Marktes. Ein Vergleich mit den zuvor modellierten Produktbausteinen, den Rechtsschutz- sowie Haushaltsdeckungen unterstützt diese Größenordnung: Die Obergrenze G des logistischen Wachstums ist für die "Sicherheit zum Recht" und "Internet-Rechtsschutz" etwa das 6.8-fache des Letztstands an aufrechten Verträgen. Betreffend "Haushalt Extra" liegt dieser Quotient bei 5. Wir setzen für das gewerbliche Produkt also die Asymptote des Bestands gleich ebenjenem zum 30. Juni 2021 multipliziert mit 5, was $G = 645$ ergibt. Die Modellierung des Bestandswachstums erfolgt wieder über ein logistisches Modell. Da es sich bei

[16] Vgl. [Fro19]
[17] Vgl. [KPM21]

"Cyber Protect" um ein eigenständiges Produkt und keinen Baustein handelt, gibt es in diesem Fall keine Durchdringungsrate. Der Rest geschieht analog zu den obigen Produkten in mittels Code im Anhang. Als Ergebnis erhalten wir $k = 0.3356$, $c = 52.302$ und folgenden Plot des Wachstumsmodells (bereits mit der üblichen Anpassung und $\alpha = 10$):

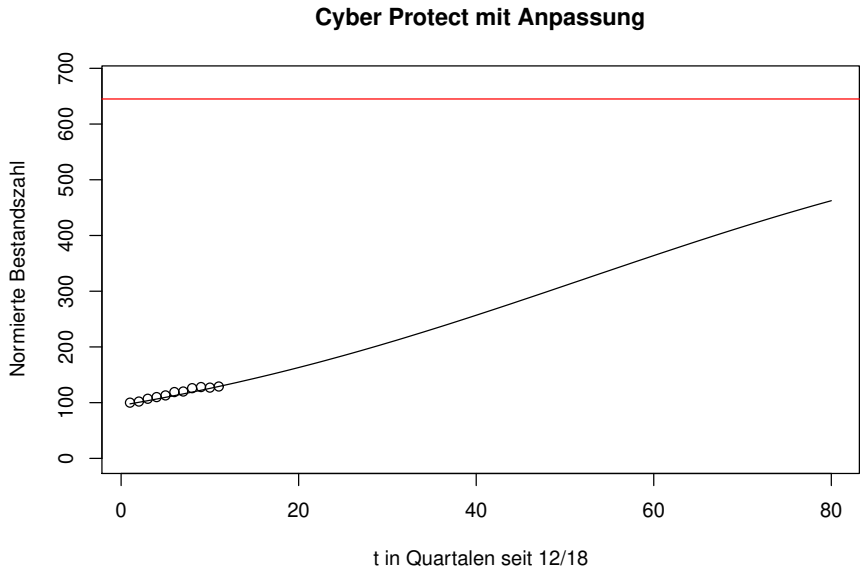


Abbildung 2.5: Bestandsprognose für "Cyber Protect" mit Anpassung

In rot ist hier die Asymptote eingezeichnet. Auffallend ist die vergleichsweise geringe Krümmung der Kurve, sowie der relativ gesehen große Wert für c.

Sowohl Obergrenze als auch weiteres Wachstum erscheinen ob der Neuheit dieser Produkte und des bisherigen Verlaufs plausibel. Als eigenständiges, neues Produkt braucht die Einführung und der Vertrieb im Markt bedeutend länger, besonders im KMU-Sektor. Ein Baustein, der in einer klassischen, etablierten Versicherungssparte vertrieben wird, findet am Markt anfangs ein entsprechend höheres Bestandswachstum, was die einzelnen Abbildungen 2.2, 2.4 und 2.5 bestätigen würden. Naturgemäß bieten derartige Analysen mit vergleichsweise wenigen Datenpunkten und einer qualitativen Argumentation des Modells zwar einen Mehrwert, sind jedoch mit großer Unsicherheit behaftet und sollten zukünftig auch kritisch hinsichtlich ihrer Verhältnismäßigkeit beobachtet werden; Eine wissenschaftliche Herangehensweise an das Thema sollte blindes Vertrauen an ein Modell stets ausschließen.

Auch diese Bestandsprojektion wird intern in ein Excel-File übertragen, um den Gesamtbestand und in weiterer Folge eventuelle Risikokumule abschätzen zu können. Hierzu rechtfertigt das Ziel einer konservativen Modellierung zudem die antizipierten Wachstumsraten, da eher auf eine Über- anstatt einer Unterschätzung der möglichen Bestandsentwicklung abgezielt werden sollte.

2.2 Rolle von Kumulen

Bevor zur Bestandsprojektion die Kumulschätzung durchgeführt werden kann, muss zunächst grundlegendes Verständnis über Risikokumule erlangt werden. Dazu bedienen wir uns klassischer Literatur, welche auch nach knapp 30 Jahren (mit einigen Anpassungen) auf aktuelle Risikomanagement-Problematiken anwendbar ist. Weiters lassen sich die vorgestellten Verfahren und Werkzeuge ebenfalls auf Cyber-Risiken anwenden.

2.2.1 Kumule und die Kontrolle von Risikokumulen

Ein Risikokumul bezeichnet eine "*...Anhäufung mehrerer Schäden aufgrund eines Ereignisses bei einem Versicherungsunternehmen...*"[18]. Es handelt sich also um einen Widerspruch zur klassischen Annahme im Versicherungsgeschäft, alle Risiken mit ihren Schadenverteilungen seien unabhängig voneinander. Für das "Ereignis" aus dem obigen Zitat existieren viele Beispiele aus der klassischen Versicherungsmathematik, etwa:

- Naturkatastrophen:
  - Sturm
  - Hagel
  - Erdbeben
  - Schneedruck
  - Hochwasser
- Überschlagen eines Brandes auf die nähere Umgebung
- Politische Unruhen
- Wirtschaftskrisen
- Cyber-Attacken über eine weit verbreitete IT-Systemschwäche

[18] siehe [Her92, S. 2]

Zwischen den verschiedenen Arten von Risikokumulen gilt es ebenfalls zu unterscheiden. So kann etwa ein Sturm alle Eigenheimversicherungen in einer speziellen Region betreffen. Anfällig für Risikokumule können aber viele verschiedene Versicherungssparten sein: Illustrative Beispiele sind hier Rechtsschutzkumule im Zuge des VW-Dieselskandals[19], oder ein Unglück während eines Firmenausflugs (Unfallversicherung).

Ebenso könnte aber auch ein sogenanntes Polizzenkumul auftreten[20]: Bei einem treuen Versicherungskunden etwa, der viele verschiedene Produkte bei einem Versicherungsunternehmen gekauft hat, entsteht bei einem Hausbrand eventuell nicht nur ein Schaden im Deckungsbereich der Eigenheimversicherung, sondern auch in der Haushalts- oder Haftpflichtversicherung. Daneben existieren auch Kumule auf Personen- oder Verkehrsmittelebene.

Die affirmativen Cyber-Versicherungen der Wiener Städtischen decken, neben bspw. Assistanceleisungen, Schäden an Daten beziehungsweise Vermögensschäden und Ansprüche Dritter. Da diese im Falle eines Hackerangriffs sowieso nicht von einer klassischen Versicherung gedeckt werden, ist ein solches Polizzenkumul sehr unwahrscheinlich.

Falls aber ein Blackout-Szenario aufgrund von Hackerangriffen eintritt, würden wir uns nicht mehr nur im rechten unteren Quadranten in der Abbildung 1.2 befinden, sondern müssen ebenfalls das linke untere Viertel betrachten: Hier können viele klassische Versicherungssparten hackerinduziert einem erhöhten Risiko ausgesetzt sein, welches in den Deckungsbereich der klassischen Versicherung fällt (und zwar fast alle gleichzeitig). Jenen "Silent Cyber"-Risiken widmet sich diese Arbeit im nächstfolgenden Kapitel.

Die klassische Kumulkontrolle[21] ist nun ein Teilgebiet des Aufgabenpools von Aktuaren und bezeichnet für den kompletten Versicherungsbestand die "Erfassung der voneinander abhängigen Haftungen"[22]. Es wird also ermittelt, wie die einzelnen versicherten Risiken bezüglich eines Ereignisses zusammenhängen, beispielsweise bei benachbarten Gebäuden. Das Analogon dazu in der Cyber-Welt wären miteinander verbundene Server, entweder direkt oder über einen gemeinsamen Cloudanbieter oder bspw. durch einen auf Viele gerichteten Cyber-Angriff. Das Befassen mit dieser Thematik liefert den Entscheidungsträgern der Versicherung Maßnahmen zur Verringerung des Kumulrisikos in Form von geeigneten Zielgrößen. Mittels dieser Zielgrößen kann das Versicherungsunternehmen die Gefahr eines Kumuls wirkungsvoll steuern:

[19] Vgl. [Bö21]
[20] Vgl. [Her92, S.110ff]
[21] [Her92, S. 15f]
[22] siehe [Her92, S. 15]

2.2.2 Steuerungsmaßnahmen für das Kumulrisiko

Die vier grundlegenden Maßnahmen, um das Kumulrisiko zu verringern bzw. zu kontrollieren teilt Mark Herbrich in seinem Standardwerk[23] in zwei Gruppen ein, deren Inhalt im Folgenden beleuchtet wird. Alle Maßnahmen lassen sich genauso auf mögliche Kumule bezüglich affirmativer Cyber-Risiken übertragen:

Reduktion der Abhängigkeit zwischen Risiken

Hierunter fällt die **Risikoselektion seitens des Versicherers**. Nach einer (quantitativen oder qualitativen) Analyse der prinzipiellen Ursachen von Abhängigkeiten in der spezifischen Versicherungssparte werden Interdependenzen im Bestand erfasst. Daraus resultieren Annahmerichtlinien, die eine Abnahme des langfristigen Kumulrisikos zur Folge haben. Herbrich nennt hier die Hagelversicherung als besonders erfolgreiches Beispiel dieser Maßnahme. Die zugehörige Zielgröße ist hier die Erfassung der Abhängigkeit im Bestand.

Verringerung der finanziellen Folgen von Kumulrisiken

Hierunter fallen die drei anderen Stellräder:

Zum Ersten können **Franchisen** das Versicherungsunternehmen in zweierlei Hinsicht entlasten: Falls der Versicherungsnehmer pro Schadenfall einen Selbstbehalt zu zahlen hat, sinkt auf der einen Seite die Höhe der Zahlungen seitens des Versicherers um diesen Betrag. Andererseits kann so, besonders im Kumulfall, die Gesamtschadenhöhe selbst (aus Sicht des VUs) reduziert werden. Dies optimiert die aus der Gesamtschadenverteilung entstehende "Gesamtentschädigungsverteilung"[24] und senkt den Bearbeitungsaufwand hinsichtlich Schadensbegutachtung etc. Die Franchise kann als klassischer absoluter Selbstbehalt, oder auch als Integralfranchise angesetzt werden. Dies bezeichnet eine Grenze, ab welcher der Versicherer den Schaden als solchen überhaupt deckt (dann jedoch vollständig). Prozentuelle Selbstbehalte oder Wartefristen haben im Kumulfall nur einen bedingten zusätzlich aufwandsmindernden Effekt. Zur Bestimmung der Franchisenhöhe wird ebenfalls eine Zielgröße benötigt. In diesem Fall sind dies Kenntnisse über die Schadenprofile für Kumulszenarien.

Zweitens bietet die **Rückversicherung** eines der bedeutendsten Mittel zur Kumulkontrolle und eine Alternative dazu, eine Kumulschadengrenze für die Deckung des Erstversicherers einzuführen. Der Unterschied zur Franchise besteht darin, dass das Risiko nicht mit dem Versicherungsnehmer geteilt wird, sondern mit einem spezialisierten Rückversicherungs-

[23] Vgl. [Her92, S.25ff]
[24] siehe [Her92, S.27]

unternehmen im rechtlichen Rahmen des Unternehmensgesetzes. Die "großen" Kumulereignisse in den letzten Jahrzehnten hatten meist die Form von Naturkatastrophen. Somit konnte durch mehrfache Rückversicherung (sogenannte Retrozession) mit Partnern auf der ganzen Welt seit jeher das Risiko für einen großen Teil der Kumulrisiken auf das Minimalste reduziert werden. Rückversicherungen existieren auf vielerlei Arten, welche in dieser Arbeit jedoch nicht weiter besprochen werden (außer sie sind explizit Teil der Rückversicherungsstrategie der Wiener Städtischen). Die Dimension des Rückversicherungsvertrags ist je nach Risikoapettit des Erstversicherers zu wählen. Außerdem richtet sie sich nach den Eigenschaften des Gesamtschadens. Falls diese Zufallsvariable und ihre Verteilung aufgrund mangelnder Daten (fehlende Bestandsbreite bzw. Historie) jedoch nicht genau modellierbar ist, bietet es sich an, die maximal zu erwartende Gesamtschadenhöhe im Kumulfall zu schätzen. Man spricht hier von der Zielgröße des Probable Maximum Loss, kurz PML. Dieser wird im Allgemeinen szenarienbasiert ermittelt, worauf wir später noch zu sprechen kommen.

Die dritte Methode zur Abschwächung des Verlusts im Kumulfall ist das Auffangen durch **Aufbau von Reserven und Berücksichtigung von Sicherheitszuschlägen**. Zur Bestimmung der entsprechenden Reservehöhe ist wie bei der Rückversicherung ein daten- oder szenariobasierter Ansatz zur Schätzung des PMLs im Kumulfall nötig. Neben dieser Kennzahl müssen hier natürlich auch "normale" Schäden zur Berechnung des Sicherheitspuffers hinzugezogen werden, um das natürliche Schwanken der Gesamtschadenhöhe abfedern zu können.

Anwendung auf Cyber-Risiken

Auch angewandt auf das affirmative Cyber-Geschäft würde jede dieser Methoden theoretisch eine effektive Maßnahme zur Kumulkontrolle darstellen. Die Risikoselektion seitens des Versicherers kann in Zukunft interessant sein, man stelle sich hier beispielswese einen maximalen Anteil an *Amazon Web Services*-Usern im Bestand vor. Die verfügbare Datenbasis aber auch die geringe Datenerhebung beim Versicherungsnehmer machen eine solche Abhängigkeitsanalyse jedoch derzeit schwer möglich. Will man jene durchführen, so bräuchte man beispielsweise umfangreichere Fragebögen zu verwendeter Hardware und Software im IT-System vor Vertragsabschluss, vor allem im Firmen- und Gewerbegeschäft, sowie ein unabhängiges Risikorating für ebenjene Komponenten.

Das Teilen des Risikos mit dem Versicherungsnehmer bietet sich zwar an, eine zu hohe Franchise aufgrund mangelnder Kenntnisse über das Schadenprofil im Kumulfall könnte jedoch das Produkt für den Versicherungsnehmer unattraktiv machen.

Viel eher bietet sich bei einem solch neuartigen Versicherungsgeschäft die Modellierung eines Kumulszenarios und damit eines Kumul-PMLs mit entsprechender Rückversicherungsstrategie an: Das Risiko des Versicherungsnehmers wird noch immer voll transferiert, und Rückversicherungen können durch weitaus größere Datenpools auch genauere Schätzungen zu Kumulrisiken abgeben. Wie auch früher in diesem Kapitel erwähnt, passiert sogar die Tarifierung des Erstversicherers zum Teil auf Empfehlungen eines Rückversicherers.

Doch auch für den Rückversicherer bergen Cyber-Risiken noch nie dagewesene Kumulgefahren: Hackerangriffe sind nicht an einen Industriezweig oder ein Land gebunden, somit kann keine Diversifizierung entsprechend dieser Kriterien stattfinden[25]. Der Ausgleich erfolgt dann hauptsächlich durch weitere Risikoteilung sowie in der Zeit. Aus Erstversicherersicht kommt mangels großer Bestände oft die erstere Möglichkeit infrage.

2.3 Methodik der Kumulschätzung

Die Kumulschätzung für versicherungstechnische Risiken orientiert sich für viele Sparten im Sachversicherungsgeschäft an einer ähnlichen Methodik und Anforderungsniveaus hinsichtlich der Daten. Je nachdem, ob ein mehr oder weniger anspruchsvoller mathematischer Ansatz den Berechnungen zugrundeliegt, richtet sich auch der Anspruch an Datenbreite, Schadenhistorie und Bestandsgröße. Wir behandeln in dieser Arbeit die drei wichtigsten Ansätze zur Kumulabschätzung[26]:

Worst Case-Analyse

Der einfachste und gleichzeitig pessimistischste Ansatz, welcher noch gänzlich ohne Kumulszenarien auskommt, ist die Betrachtung des absoluten Worst Case: Bei "Haushalt Extra", dem Cyber-Produktbaustein für die Haushaltsversicherung der Wiener Städtischen, besteht beispielsweise ein Deckungslimit von 2.500 Euro pro Versicherungsjahr und Vertrag. Dem Worst Case entspräche ein Ausreizen des Deckungslimits bis zur oberen Grenze für den gesamten Bestand. Abzüglich etwaiger Risikoteilungen über Rückversicherungsverträge ergibt sich so im Endeffekt die gesamte Versicherungssumme, also die Summe der einzelnen Deckungslimiten, im Eigenbehalt.

Der Hauptteil davon kommt im Falle der Wiener Städtischen aus den Produkten des Zivilgeschäfts, da hier bis dato keine gesonderte Rückversicherung abgeschlossen wurde. Beim Firmen- und Gewerbegeschäft bleiben nur etwa 10% der gesamten Versicherungssumme im Eigenbehalt über. Hier wurden für Cyber Protect und Cyber Basic Rückversicherungsver-

[25] Vgl. [CGGP20, S.3]
[26] Vgl. [Gla18]

träge mit einem Rückversicherer abgeschlossen, dessen Prämienempfehlungen die Wiener Städtische auch als Anhaltspunkt für ihre Tarifierung verwendet. Für das Spezialprodukt "Cyber Industrie", welches auf Einzelvertragsbasis ausverhandelt wird und Deckungssummen von im Schnitt 10 Mio. Euro umfasst, wurde ein eigener Rückversicherungs vertrag abgeschlossen. Die verwendeten Rückversicherungstypen entsprechen hier Quoten- und Schadenexzedenten-Rückversicherungen. Für weitere technische Definitionen dieser Rückversicherungsarten sei auf die Datenerhebung in Kapitel 4 verwiesen.

Deterministische Modellierung von Szenarien

Der nächste Schritt in Richtung komplexerer Schätzungsmethoden liegt in der deterministischen Szenarioschätzung. Dazu wird der Ablauf eines potentiellen Kumulereignisses beschrieben sowie deterministische Schätzungen dazu angeführt. Dies geschieht sowohl datengestützt als auch durch Expertenmeinungen. Für jede versicherte Sparte müssen hier mögliche Schäden evaluiert und ein durchschnittlicher Schaden geschätzt werden. Am Ende ergibt sich eine Zahl an im Schnitt betroffenen Versicherungsnehmer sowie dem durchschnittlichen Schaden pro Versichertem. Mögliche Optionen für Szenarien wären hier

- Eine Hacker-Attacke mittels eines Virus
- Die Veröffentlichung von persönlichen Daten aus dem Unternehmensumfeld, ein sogenannter "Data Breach"
- Ausfall eines IT-Providers bzw. Cloud-Anbieters

Ergebnis dieses Ansatzes ist ein PML, welcher als absolute Zahl bzw. bei standardisierten Produkten als Prozentsatz der Versicherungssumme im Eigenbehalt angegeben wird. Eine weitere illustrative Darstellung der Szenarien wird später unternommen. Ebenfalls wird in Kapitel 3 näher beleuchet, warum ein Szenario ein passendes Mittel zur Risikoabschätzung ist.

Probabilistische Modellierung von Szenarien

Das große Ziel in der Schätzung von Cyber-Risikokumulen ist eine stochastische Modellierung, in der Szenarien zufällig anhand von historischen Daten modifiziert werden. Hier ergibt sich ebenfalls mit einem PML eine Kenngröße für eine Art Solvenzkapitalanforderung im Kumulfall. Dieser Ansatz birgt derzeit jedoch auch die größten Herausforderungen: Sowohl die geringe Schadenerfahrung als auch das sich ständig ändernde Umfeld, in dem Cyber-Gefahren lauern, machen eine Kalibrierung von Schadenverteilungen und ihrer Abhängigkeitsstrukturen für einen Erstversicherer nur schwer möglich.

Folgend wollen wir tiefer in die von der Munich Re in [Gla18] erwähnten Szenarien eintauchen und eventuelle Auswirkungen auf das Portfolio abwägen. Nach der Diskussion, wie im deterministischen respektive stochastischen Fall die Frequenzschätzung vonstatten geht, wird das derzeitige Cyber-Kumulschätzungsverfahren der Wiener Städtischen erläutert. Ebenfalls wollen wir für eine weitergehende Szenarioanalyse die Struktur eines dafür zu erstellenden Datensatzes skizzieren.

2.4 Szenarienauswahl

Da die Szenarien, mit denen Cyber-Rückversicherer arbeiten meist nicht öffentlich verfügbar sind, lehnen wir uns hier für das Modell-Framework an die Empfehlungen des Cambridge Centre for Risk Studies an[27]. Die einzelnen vorgestellten, fiktiven Szenarien haben für die Wiener Städtische bei näherer Betrachtung eventuell eine untergeordnete Bedeutung, etwa wenn Lösegeldzahlungen bei Ransomware-Angriffen gar nicht gedeckt sind und hier nur Assistance-Leistungen zu zahlen sind. Dies ist zu einem späteren Zeitpunkt auf Einzelszenarien-Basis zu klären. Wir wollen hier primär die Szenarien vorstellen und ihre möglichen Auswirkungen auf verschiedene Deckungsarten beleuchten. Die Szenarienauswahl der Universität Cambridge deckt sich mit vielen Überlegungen von verschiedenen Beratungshäusern und Rückversicherern zu dieser Thematik, etwa der Munich Re[28] oder Willis Towers Watson[29]. Das Ausmaß der Szenarien folgt dabei dem Grundgedanken eines extremen, jedoch nicht unwahrscheinlichen Ereignisses.

2.4.1 Kompromittierung von Daten

Die Kompromittierung von digitalen Daten umfasst den Diebstahl und die Veröffentlichung von Daten über Unternehmen, Partner ihrer Wertschöpfungskette, Kunden oder Angestellten. Es können hier verschiedenste Arten von digitalen Daten zu einer Vielfalt von Ansprüchen gegenüber dem Versicherer führen. Eine Einteilung könnte wie folgt stattfinden:

- Persönliche Daten: Etwa der Name, Adresse, Nummer des Führerscheins oder Passwörter
- Zahlungsinformationen: zB Kontodaten, Kreditkartennummer und dazugehöriger PIN
- Gesundheitsdaten: Informationen über den Gesundheitszustand einer Person, Medikation und Therapie, Versicherungen diesbezüglich oder biometrische Daten

[27] Vgl. [Cam16, S.25ff]
[28] Vgl. [Gla18]
[29] Vgl. [WTW]

- Vertrauliche Unternehmensdaten: Unternehmensgeheimnisse und andere sensible Daten entlang der Lieferkette des Unternehmens
- Geistiges Eigentum: Patente, Markenrechte, Produktentwürfe und dergleichen

Der entstehende finanzielle Schaden kann sich in Form von

- Krisenkommunikation,
- Kompensationszahlungen,
- Schadensersatzansprüchen Dritter,
- Strafzahlungen oder
- Assistanceleistungen

niederschlagen.

Die Kompromittierung von Daten gehört zu den am meisten auftretenden Cyber-Schadenfällen und ist auch entsprechend in fast allen Cyber-Versicherungsprodukten für gewerbliche Kunden gedeckt. Die Gründe dafür sind laut *Centre for Risk Studies*[30] in den letzten Jahren verschieden gewesen: In der vorigen Dekade waren es noch hauptsächlich Versehen oder Insider, die einen Datenverlust oder -diebstahl ausgelöst haben. Dies bestätigen auch die Quellen aus Kapitel 1, [BSG15]. Nun zeigt der Trend jedoch in Richtung Diebstahl durch Hacker von außerhalb des Unternehmens. Man stützt sich hier auf Daten aus dem US-amerikanischen Markt aus 2015.

Entwicklung eines Kumuls in diesem fiktiven Szenario

Der Datenverlust in einem Unternehmen ist nicht zwingend mit einem Diebstahl in einer anderen Firma korreliert. Ein erfolgreicher "Data Breach" kann sich jedoch in seinem Ausmaß aufbauschen, etwa wenn durch gestohlene Passwörter weitere Schäden angerichtet werden können. Das Kumulszenario soll nun abbilden, inwieweit ein starker, aber plausibler Anstieg in den Schadenzahlen finanziell tragbar ist und welche systematischen Korrelationen oder besondere Angriffspunkte hier vorliegen können. Man spricht dabei von sogenannten "Single Points of Failure".

Jedes entwickelte Szenario folgt einer Geschichte, einem Narrativ, so auch dieses. Wir unterteilen das Event in fünf Phasen auf[31]:

[30] Vgl. [Cam16, S.27]
[31] Vgl. [Cam16, S.28f]

- Teil 1: Die Vorbereitung

  Ein Kollektiv an Hackern aus mehreren europäischen Ländern entdeckt im Darkweb drei Informationen über IT-Schwachstellen, die zum Kauf angeboten werden. Diese drei können mit Geschick zu einer effektiven Methode kombiniert werden, um bei unzähligen Firmen sensible Daten stehlen zu können. Sie kaufen diese Informationen und bereiten ihren Angriff vor.

- Teil 2: Auswählen von Zielen

  Die Hacker lesen die öffentlichen Server unzähliger deutschsprachiger Unternehmen aus, um ihre Konfiguration sowie Firewall-Informationen zu bekommen. Nach ihren Analysen besitzen 18% der Server eine Firewall von "Sophos", von welcher sie eine Systemschwäche kennen. Unter diesen Servern suchen sie die der größten Unternehmen aus, sowie die Server von Firmen im Gesundheitsbereich. Weiters haben die Angreifer Informationen über eine Schwachstelle in "Oracle SQL"-Datenbanken erworben. Es gilt nun, herauszufinden welche der Unternehmen eine solche verwenden.

- Teil 3: Der Datendiebstahl

  Mittels Trojanern späht die Gruppe alle Unternehmen der Zielgruppe aus. Dies ist durch die Firewall-Schwachstelle möglich. Nur ein kleiner Teil dieser Firmen verwendet auch "Oracle SQL" und "Microsoft Teams", in welchem die dritte Schwachstelle besteht. Die Hacker vergeben an sich selbst Administratorrechte für die Datenbank und extrahieren die Daten, indem sie sie als "Microsoft Teams"-Videostream tarnen. Das Ergebnis ist ein Diebstahl von 100 Millionen Datensätzen, die am Schwarzmarkt verkauft werden können.

- Teil 4: Entdeckung des Angriffs

  Der Angriff wird von IT-Security-Experten im Unternehmen entdeckt und gemeldet. Bald darauf meldet sich eine zweite Firma als Geschädigter mit einem Diebstahl von 60 Millionen Gesundheitsdatensätzen. Die Schwachstellen in den drei Programmen werden erkannt und behoben. Insgesamt melden sich über 300 Unternehmen, die öffentlich einen Datendiebstahl bekannt geben müssen.

- Teil 5: Die Auswirkungen

  Während dieses Angriffs wurden Milliarden von Datensätzen gestohlen. Die österreichische Regierung erlässt ein Gesetz, welches die Firmen zu höhen IT-Sicherheitsstandards verpflichtet. Daraufhin sinkt die Erfolgsrate für Angriffe kurzfristig. Die Verantwortlichen werden nur zum Teil entdeckt und festgenommen. Geschädigt sind

insbesondere große Unternehmen, die Gesundheitsbranche sowie KMU mit niedrigen Sicherheitsstandards.

Dieses Szenario wäre ein Beispiel für ein extremes, aber nicht unmögliches Ereignis einer großflächig angelegten Kompromittierung von sensiblen Daten. Größere Auswirkungen sind hier bei Produktbausteinen zu erwarten, die Schadenersatzansprüche Dritter sowie Kostenübernahme aufgrund von Datenverlust oder Verletzung der Persönlichkeitsrechte decken. Auch ein etwaiger Reputationsverlust sowie Massenklagen sind hier zu erwarten.

2.4.2 Großflächige DDoS-Attacken

Im Jahr 2015 ist auf die Hälfte aller US-Unternehmen eine *Distributed Denial of Service*-Attacke ausgeübt worden. Hier werden die Server der Unternehmen solange mit Anfragen überflutet, bis die dahinterstehenden Rechner überlastet und nicht mehr verfügbar sind. Es geht in diesem Fall primär nicht darum, Firewalls zu durchbrechen oder Zahlungsinformationen zu stehlen, sondern darum den Server einfach lahmzulegen. Der Schaden durch eine eventuell folgende Erpressung oder eine Geschäftsunterbrechung kann enorm sein.

Je größer ein Server dimensioniert ist, etwa für mehrere Millionen Besucher pro Monat, desto intensiver muss auch ein DDoS-Angriff durchgeführt werden, damit er "erfolgreich" ist. Gemessen wird der produzierte Datenverkehr in Gigabit pro Sekunde, bei über 100 Gbps spricht man von einer sehr hohen Intensität. Die Dauer einer solchen Attacke bewegte sich 2014 laut *Risk Management Solutions, Inc.* in 70% der Fälle im Bereich bis sechs Stunden, in 16% länger als zwölf Stunden. Die durchschnittlichen Kosten für kleine und mittlere Unternehmen aus einer DDoS-Attacke heraus betrugen 2014 etwa 44000 Euro, für große Unternehmen eher das 9-fache hiervon[32]. Ein möglicher Ablauf des Kumulereignisses wäre folgender:

- Teil 1: Vorbereitung

  Eine große Gruppe antikapitalistischer Aktivisten ruft dazu auf, sich das Internet von großen Firmen zurückzuholen, da jene das Webgeschehen dominieren und dabei wenig zur Gesellschaft beitragen. Sie koordiniiert mittels Veröffentlichung eines Manifests den ganzen Sommer über eine gemeinsame DDoS-Attacke auf besagte Unternehmen. Darin befinden sich Anleitungen zur Durchführung von Angriffen auf sämtliche Webserver sowie Quellen, wo entsprechende Rechner-Ressourcen erworben werden können.

- Teil 2: Ablauf der Attacke

[32] Vgl. [Cam16, S.35]

Die ersten Attacken treffen mittelgroße Finanzdienstleister. Benutzer können daraufhin ihre Konten nicht mehr einsehen und keine Überweisungen mehr tätigen. Die IT-Teams der Unternehmen sind überwältigt, die Services sind für mehrere Tage nicht erreichbar.

Das nächste Ziel sind die größten Online-Kaufhäuser: Trotz Vorkehrungen können auch sie den Attacken nicht lange standhalten. Tausende Webseiten sind mittlerweile betroffen. Die nächsten Ziele betreffen bekannte Unterhaltungs-, Telekom- und Software-Unternehmen. Während sich die Angriffe über mehrere Monate immer weiter ausbreiten, sinkt die Intensität der Attacken mangels verfügbarer Rechenleistung im Darkweb.

- Teil 3: Ende der Attacke

  IT-Spezialisten beginnen mit Gegenattacken auf die Verursacher. Die Aktivisten verkünden das Ende ihrer Attacken, da sie ihre Ziele erreicht haben.

- Teil 4: Die Auswirkungen

  In diesem Sommer gehen viele Millionen an Betriebsstunden wegen der DDoS-Attacken verloren. Die Zahl der Kunden, die ihre Waren online kaufen, sinkt gewaltig. Die Server hingegen werden massiv gegen zukünftige Angriffe aufgerüstet. Die Schäden aufgrund von Geschäftsunterbrechungen steigen immer weiter.

Eine DDoS-Attacke kann bei vielen Deckungsbausteinen Versicherungsfälle hervorrufen, allen voran die Geschäftsunterbrechung. Zusätzlich können diese Angriffe zur Erpressung, Rufschädigung oder zum Maskieren von größeren Datenkompromittierungen verwendet werden.

2.4.3 Ausfall eines Cloud-Anbieters

Mittlerweile benutzt die Mehrheit der Unternehmen an irgendeiner Stelle ihrer IT-Prozesse einen Cloud-Anbieter. Sei es, um Daten zu speichern, eine Analyseplattform zu nutzen oder zum Outsourcen von Geschäftsprozessen, die Cloud bietet einen unkomplizierten, und im Individualfall meist sichereren Weg, um IT-Kompetenzen an Spezialisten abzugeben. Auch das Tarifierungstool für "Cyber Protect" unterstreicht dies: Wird im Fragebogen etwa ein Outsourcing-Provider genannt, so verringert sich die Tarifprämie um 10%.

Fällt besagter Cloud-Anbieter jedoch aus, so sind gleichzeitig viele Unternehmen davon betroffen. Ebenfalls können bei einer Datenkompromittierung sämtliche Kundendaten des Providers geleakt werden. Somit bieten jene Unternehmen ein klassisches Beispiel für ein

Kumulszenario[33]. In diesem Fall sollen die Auswirkungen eines langwierigen Ausfalls eines Cloud Services-Anbieters mit großem Marktanteil erforscht werden, vor allem aus Sicht eines Versicherers, dessen Versicherungsnehmer Kunden dieses Cloudunternehmens sind. Beispiele für solch große Unternehmen wären *Amazon Web Services*, *IBM*, *Adobe* oder *Cisco* aus den USA respektive *SAP* aus Deutschland.

Für dieses Szenario und die Kumulkontrolle prinzipiell ist interessant zu wissen, welcher Versicherungsnehmer Services an welche Cloud-Anbieter ausgelagert hat. Eine grundlegende Diversifikation über alle möglichen Provider wäre für die Versicherung optimal, das Gegenteil würde ein Konzentrationsrisiko darstellen; Vergleichbar wäre dies dann mit lauter nebeneinander stehenden Häusern.

Kenntnisse über die Praktiken der einzelnen Outsourcer geben zusätzlich mehr Einblick in die Resilienz des eigenen Portfolios: *Amazon Web Services* zum Beispiel strukturiert all seine Geschäftstätigkeiten in 30 geografische Bereiche, welche komplett unabhängig voneinander sind. Ein wählbares Add-On bei Beauftragung des Unternehmens aus Seattle ist ein "dual-server service": Hier wird der Kunde an mehrere Datenzentren verbunden, um im Falle eines Ausfalls von einer Region noch immer geschäftstätig sein zu können. [Cam16] gibt im Falle eines Ausfalls auch einen Durchschnittsausfall pro Kunden an, also beispielsweise bei einem Cloud-Ausfall von 6-12 Stunden: Da in diesen Stunden laufend Kundenzugänge wiederhergestellt werden, beträgt der durchschnittliche tatsächliche Ausfall eines Kunden 8 Stunden.

Beschreibung des Kumulszenarios

Intensität und Länge des Cloud-Ausfalls können natürlich beliebig gewählt werden, im Folgenden wird ein Beispiel skizziert:

- Teil 1: Ein Versehen als Auslöser

  Der europaweit führende Cloud-Anbieter *Zorro* betreibt für seine österreichischen Kunden zwei Datenzentren in Wien und Salzburg. Um Security-technisch immer am neuesten Stand zu bleiben, beschäftigt *Zorro* Techniker, die in einem Labor versuchen, die eigenen Systeme zu knacken. Dabei entwickelt sie einen Virus, der die Verbindungen zwischen allen möglichen internen und externen Datenschnittstellen kappt. Der Virus kommt durch ein Versehen in die produktiven Systeme des Cloud-Anbieters in Salzburg. Von dort aus beginnt er, alle verfügbaren Verbindungen zu trennen.

- Teil 2: Vollständiger Systemausfall

[33] Vgl. [Cam16, S.40ff]

Innerhalb einer Stunde ist das komplette Salzburger Datenzentrum lahmgelegt. 3000 Kunden stehen vor einer Betriebsunterbrechung, 400 haben den Premium-Service des Anbieters gebucht und schalten auf das Wiener Datenzentrum um, von dem aus weitere 4000 Kunden bedient werden.

Durch Notfallprotokolle wird ein Teil des Wiener Datenzentrums unterstützend zur Sicherung des Salzburger Pendants eingesetzt, was sich als großer Fehler herausstellt: Der Virus zerstört die Verbindungen in beiden Zentren, 7000 Kunden leiden unter dem Cloud-Ausfall

- Teil 3: Wiederherstellung

  Der Virus kann endlich gefunden und gelöscht werden, und die großen Aufräumarbeiten beginnen. Nach 12 Stunden besitzen 60% der Kunden noch immer keinen Zugang zu ihrem Cloudspeicher. Viele Unternehmen untersuchen den raschen Wechsel zu einem von *Zorro*s Konkurrenten und prüfen eventuelle Reputationsschäden, die sie durch die Betriebsunterbrechung erfahren.

- Teil 4: Gesamte Auswirkungen

  Nach 24 Stunden hat der Großteil der Kunden wieder Zugriff auf ihre Systeme. Für etwa 5% können die Zugänge jedoch noch einige Tage lang nicht repariert werden. Bis alles wieder beim Alten ist, vergehen drei Wochen. Der gesamte Cloud-Markt ist in seinem Ruf schwer beschädigt, und *Zorro* verliert Kunden um Kunden. Weiters stehen jahrelange Gerichtsprozesse wegen Ansprüchen Dritter im Raum. Der Ausfall wird in Österreich als Lehrbeispiel gesehen, die nächste Generation an Cloud-Services wird um einiges resilienter geplant werden.

Der Ausfall eines Cloud-Providers kann in vielerlei Hinsicht massive Forderungen gegenüber Versicherern verursachen, hauptsächlich durch Betriebsunterbrechung, aber auch Haftungsthemen sowie der Verlust von Daten und Verstoß gegen Persönlichkeitsrechte sind hier deckungsrelevante Themen.

2.4.4 Überfall auf Finanztransaktionen

Für die Kontrolle von Cyber-Kumulen müssen ebenfalls Finanzdienstleister betrachtet werden: Versicherer bieten nämlich oft spezielle Deckungen zur Zahlungssicherung und bei Finanzbetrug im Internet an. Dadurch gilt es, zu schätzen, wie viele und wie hohe Schäden bei Cyberkriminalität in der Finanzbranche entstehen können. Dies betrachten wir durch ein Kumulereignis, welches noch nie dagewesene Ausmaße hat. Wir unterscheiden zuerst jedoch

zwischen drei Arten von Kriminalität über das Internet hinsichtlich Finanztransaktionen[34]:

- Angreifen von IT-Systemen von Banken um Zugriff auf verfügbares Geld auf Konten zu bekommen
- Marktmanipulation und Insiderhandel aufgrund von Diebstahl nicht-öffentlicher Bankdaten über zB Unternehmensübernahmen oder Börsengänge
- Aussenden von Schadprogrammen um

  Zugang zu Kundenkonten zu erlangen

  Zugang zur Zahlungsabwicklungs-Infrastruktur zu erlangen

  Ausnutzen von Wertpapier-Handelssystemen

  Schädigen eines Finanzunternehmens durch Betriebsunterbrechung

Schäden in Milliardenhöhe sind zwar ein Extremfall, aber nicht unmöglich wie ein Beispiel aus Brasilien zeigt[35]: Hier konnte ein beliebtes brasilianisches Zahlungssystem zwei Jahre lang durch Schadprogramme infiltriert werden. Unbemerkt konnten die Täter so kolportierte 3.75 Milliarden US-Dollar stehlen.

Widmen wir uns nun dem Kumulereignis, welches möglichst alle Angriffs- und Schadenarten im Finanzsystem kombiniert und bis dato unvergleichbare Ausmaße besitzt. Währenddessen bleibt es jedoch im Bereich des Möglichen.

Beschreibung des Kumulereignisses

- Teil 1: Vorbereitung

  Eine Gruppe von Hackern vereinigt sich zu einem Kollektiv. Mittels neuester Angriffstechiken und weltweiter Vernetzung ist es das Ziel, Geld aus Attacken auf zentraleuropäische Banken zu schlagen. Um ihre Schadprogramme in die Unternehmen einzuschleusen werden Phishing-Mails, gefälschte Anzeigen im Internet, das Imitieren des unternehmensweiten Telefonsystems inklusive automatischer Ansagen sowie das Ausspionieren von Bankmitarbeitern über freie WLAN-Netzwerke verwendet.

- Teil 2: Der Überfall

  Die Hacker-Vereinigung zielt auf eine große Zahl an Kreditinstituten ab und infiltriert die Datenbanken der Unternehmen. Zusätzlich wird die Bankomatensteuerung manipuliert, sodass diese zu bestimmten Uhrzeiten an bestimmten Orten Geld aus

[34] Vgl. [Cam16, S.46f]
[35] Vgl. [Bra14]

dem Bankomaten "kostenlos" ausgeben lässt. Mittels geheimer Firmeninformationen wird ebenfalls Insiderhandel betrieben sowie andere Arbitragemöglichkeiten ausgenutzt.

- Teil 3: Entdeckung der kriminellen Aktivität

  Die Kreditinstitute bemerken die großen Verluste durch den Überfall und kompensieren geschädigte Kunden. Sie veröffentlichen jedoch nicht, Opfer eines IT-Angriffs gewesen zu sein. Stattdessen teilen die Banken ihre Informationen untereinander und werden sich der Dimension des Überfalls bewusst. Die Meldung von 100000 gestohlenen Bonitätsdatensätzen sowie Ermittlungen im Zuge von Aktienpreismanipulationen bringen den Angriff endgültig ans Tageslicht. Interpol sowie private Forensik-Teams werden eingeschaltet. Die Ermittlungen laufen ein ganzes Jahr, bis die Hintergründe vollständig aufgearbeitet worden sind.

- Teil 4: Die Auswirkungen

  Das Ergebnis sind Hunderte Verdächtige, Prozesse für die Anführer der Gruppe in den einzelnen Staaten sowie eine Vielzahl an konfiszierten Servern und Rechnern. Vom Geld fehlt zum größten Teil jedoch jede Spur. Die Kreditinsitute haben große Verluste zu verkraften. Von öffentlicher Seite kommen mehr Forderungen, die Zahlungsabwicklung noch sicherer zu gestalten.

Der Großteil der durch dieses Ereignis verursachten Schäden fällt in den Bereich des Finanzbetrugs und -diebstahls. Weiters können Zahlungen wegen Rufschädigung oder Haftungsfragen entstehen.

2.4.5 Cyber-Erpressungswelle

Das letzte Kumulereignis, welches hier vorgestellt werden soll, behandelt Ransomware-Angriffe und die damit einhergehenden Lösegeldzahlungen. In der Einleitung schon ansatzweise beschrieben, werden bei einem solchen Angriff die Daten des Opfers verschlüsselt und nur gegen eine Zahlung wieder freigegeben. Im Jahr 2012 haben nur etwa 3% der Leute, deren Daten durch solch einen Angriff verschlüsselt wurden, das Lösegeld auch gezahlt. Dies betrifft sowohl KMU als auch Privatpersonen, das Szenario ist also im Firmen- und im Zivilgeschäft anwendbar. Wir gehen hier von einer neuartigen Standard-Ransomware und ihren Auswirkungen bei Unternehmen aus:

Beschreibung des Kumulszenarios

- Teil 1: Vorbereitung

Eine Gruppe von Cyberkriminellen hat bereits seit mehreren Jahren Erfolg mit dem Entwickeln von Ransomware für private Endbenutzer, und orientiert sich nun in Richtung Unternehmen um. Entwickelt wird die neueste Generation von Malware, welche von den klassischen IT-Sicherheitssystemen der meisten KMU nicht erkannt wird. Nach der Verschlüsselung erscheint ein Dauerbild am Monitor mit einem Countdown bis zur endgültigen Löschung der Daten. Die Höhe der Lösegeldzahlung wird automatisch festgelegt, beim Zahlen und Entschlüsseln hilft ein eigenes virtuelles Callcenter.

- Teil 2: Das Anlocken

  Das Ziel der Hacker besteht in österreichischen Unternehmen mit Jahresumsätzen zwischen 2 Millionen und 40 Millionen Euro. An das mittlere Management werden Mails geschickt, in deren Anhang sich eine gefälschte PDF-Datei befindet. Ein großer Teil dieser E-Mails landet zwar in Spam-Ordnern oder wird abgefangen, oft genug kommen sie jedoch im Posteingang an. Dateisysteme werden verschlüsselt, Krisensitzungen der Geschäftsführungen durchgeführt. Zusätzlich wird die Polizei verständigt, welche die Angreifer meist nicht ausmachen kann. Besorgte Kunden werden mit der Meldung technischer Probleme vertröstet

- Teil 3: Das Verhandeln

  Der Countdown läuft immer weiter. Versicherungen werden kontaktiert und Kosten-Nutzen-Rechnungen angestellt. In einigen Fällen finden Zahlungen statt, oft professionell unterstützt durch eigens eingerichtete Callcenter. Die Uhren stoppen, die Daten sind wieder da.

- Teil 4: Die Auswirkungen

  Selbige Szenarien finden gleichzeitig bei tausenden Unternehmen statt. Viele verweigern jedoch die Zahlung und bauen ihr Datensystem neu auf. Sie müssen dann einen Daten- und Reputationsverlust hinnehmen. Große Unternehmen sind nicht betroffen, da ihre IT-Infrastruktur sicherer aufgebaut ist. In den Medien hört man vielleicht Gerüchte, eine große Headline wird jedoch selten auftauchen: Viele Unternehmen kommen zu dem Schluss, Informationen über ein solch kompromittierendes Ereignis unter Verschluss zu halten, um sich selbst nicht noch mehr zu schaden.

Neben Reputationsschäden und Schäden durch Datenverlust ist die Lösegeldzahlung der wohl größte deckungsrelevante Teil dieses Szenarios. Ob und inwieweit dies auch von den Produkten der Wiener Städtischen gedeckt wird, muss auf Einzelfallbasis eruiert werden.

Jedes dieser Szenarien ist gesondert zu betrachten und in Korrespondenz mit Sachversicher-

ungs- und IT-Experten parametrisieren. Die Ereignisse sind a priori auf Sparten, durchschnittliche Schadenhöhen und weitere Parameter einzustellen, die zum Portfolio des Versicherers passen: Ein KMU-starker Bestand zum Beispiel würde unter dem Erpressungs-Szenario einen weitaus größeren Schaden nehmen als ein Portfolio mit großen Unternehmen, die sich entsprechend gegen solche Attacken wappnen.

Auswirkungen der Szenarien

Die Auswirkungen der obigen fünf Szenarien hat *Risk Management Solutions, Inc.* zusammen mit dem *Centre for Risk Studies* der University of Cambridge in einer Tabelle zusammengefasst:

Cyber Loss Process:	Data Exfiltration	Denial-of-Service	Cloud SP Failure	Financial Theft	Cyber Extortion
Accumulation Scenario:	Leakomania	Mass DDoS	Cloud Compromise	Financial Transaction Interference	Extortion Spree
Insurance Coverage Category					
Breach of privacy event	3	1	2	1	1
Data and software loss	3	2	2	1	2
Incident investigation and response costs	1	1	1	1	1
Liabilities	2	2	2	2	1
Financial theft	2		1	3	1
Business interruption	1	3	3	1	2
Cyber extortion	1	2	1	1	3
Intellectual Property (IP) theft	1		1		1
Impact on reputation	2	2	1	2	2

3	Potentially High Impact
2	Potentially Significant Impact
1	Potentially Some Impact
	No Impact Likely

Quelle: [Cam16, S.21]

Abbildung 2.6: Auswirkungen der einzelnen Szenarien auf verschiedene Deckungen

Soll also der Fußabdruck beispielsweise eines DDoS-Kumulereignisses quantifiziert werden, so können von 2.6 Annahmen über die Effekte in den einzelnen Deckungsbereichen getroffen werden. Diese decken sich auch in den wichtigen Punkten mit den Überlegungen am Ende eines jeden Szenarios in dieser Arbeit.

Parametrisierung der Szenarien

Die einzelnen Wahrscheinlichkeiten, etwa die Rate der erfolgreichen Datendiebstähle pro Industrie ist aus entsprechenden Statistiken zu extrahieren, etwa Cyber Risk Reports von großen Unternehmensberatern. Die Verteilung der Schadenhöhe kann aus bestehenden Schadenstatistiken hergeleitet werden, basiert in den meisten Fällen jedoch auf Durchschnittswerten mit einer zusätzlichen Verteilungsabschätzung von Experten mangels ausreichend Schadendaten. Insbesondere sind eigene Verteilungen für Privat- und Unternehmenskunden anzugeben.

Die Frequenz der Szenarien muss derzeit ebenfalls von Experten geschätzt werden. In der derzeitigen Kumulschätzung für die Wiener Städtische werden etwa Szenarien mit einer jährlichen Eintrittswahrscheinlichkeit von 0.1% angenommen, das heißt dass sich das angenommene Narrativ einmal innerhalb von 1000 Jahren realisiert. Falls zu einem späteren Zeitpunkt ein stochastischer Ansatz datenseitig möglich wird, so kann die erwartete jährliche Eintrittswahrscheinlichkeit mittels vergleichbarer Szenarien und ihrer jährlichen Inzidenzrate geschätzt werden. Um den Schätzer herum wird in beiden Fällen für die Schadenzahl eine klassische Verteilungsannahme getroffen, etwa eine Poissonverteilung.

Datenanforderung für die Szenarienanalyse

Will die Wiener Städtische eigene Szenarienanalysen durchführen und nicht nur auf Empfehlungen von Versicherungspartnern zurückgreifen, so ist eine entsprechende Cyber-Datenbank aufzubauen, welche die Risikofaktoren der einzelnen Versicherungsnehmer dokumentiert. Dazu wird die Datenanforderung, welche die Judge Business School der britischen Cambridge University stellt, modifiziert und auf realistische Maße reduziert[36]. Sofern nicht vorhanden, können die Attribute folgender zwei Tabellen im Zuge der Antragstellung oder mittels einer jährlichen Datenerhebung abgefragt werden:

[36] Vgl. [Cam16, S.13f]

Unternehmensprofil und -kennzahlen	
Geschäftszweig	Jahresumsatz
Mitarbeiterstand	Anzahl und Art bisheriger Cyber-Vorfälle
Abhängigkeit des Umsatzes von Online-Aktivitäten	Abhängigkeit des Umsatzes von der IT-Struktur generell
Anteil des Umsatzes von Online-Geschäft	Anteil des Umsatzes von Privatkunden
Interne Cyber-Awareness	
Vorhandensein und Rating eines Notfallplans bei Cyber-Vorfällen	Existenz einer dezidierten Risikomanagement-Funktion
Existenz eines Chief Information Officer o.Ä.	Existenz einer dezidierten Compliance-Funktion
Regelmäßige Unterweisung des Personals hinsichtlich Cyber-Vorfälle	Existenz von Prozeduren für Fernzugriffe (Remote Office etc.)
Beschaffenheit des Datensystems	
Arten von verwalteten Datensätzen gemäß Szenario "Datenkompromittierung"	Durchschnittsanzahl an Sätzen der jeweiligen Typen
Maximalzahl an Sätzen der jeweiligen Datentypen	Art der Daten, die an Dritte (Cloud) weitergegeben wird
Existenz wertvollen geistigen Eigentums	Rating des Verschlüsselungsstandards der Datenbank
IT-Systemkonfiguration und -Standards	
Struktur und Größe der IT-Systems anhand von verschiedenen Kennzahlen	Name und Hersteller des Betriebssystems
Beschaffenheit der Firewall	Größe der von der Firewall geschützten Server
Name des Herstellers des IT-Sicherheitssystems	Name der Software für das IT-Sicherheitssystem
Name des/der Cloud-Provider/s	Hersteller und Namen der wichtigsten verwendeten Programme und Systemkomponenten
Existenz von Prozeduren, wie mit Systemschwächen umgegangen wird	

Tabelle 2.3: Nötige Attribute für eine ausführliche Cyber-Szenariomodellierung, Teil 1

Interne IT-Sicherheitspraktiken	
Anzahl an IT-Spezialisten	Existenz von internen sowie externen IT-Serviceteams
Name und Hersteller des Antivirus-Systems	Existenz einer Testprozedur der eigenen Cybersicherheit
Angabe der E-Mail-Protokolle und -Programme	Rating der Backup-Prozeduren
Verschlüsselungsstandards von mobilen Endgeräten und Laptops	Rating des Passwortmanagements
Ergebnis eines evtl. Assessment-Fragebogens	
Versicherungsinformationen	
Deckungssummen für die einzelnen Risiken aus den Szenarien (genauer die Deckungskategorien aus Abbildung 2.6)	Selbstbehalte für die einzelnen Risiken aus den Szenarien

Tabelle 2.4: Nötige Attribute für eine ausführliche Cyber-Szenariomodellierung, Teil 2

Derzeitige Kumulschätzung der Wiener Städtischen und Ausblick

Die Wiener Städtische verwendet für ihre Kumulschätzung derzeit eine Abschätzung auf Basis einer Risikokumulabschätzung des Rückversicherers, mit dem bezüglich des Cyber-Geschäfts eine Risikoteilung vereinbart wurde. Dieser verwendet zur derzeitigen Analyse einen deterministischen szenariobasierten Ansatz mit drei Szenarien, welche sich mit dem oben erwähnten Szenarienkatalog großteils decken. Seit dem Herbst 2018 wird hier das Portfolio im Zivil- und Firmen- und Gewerbegeschäft auf Kumulrisiken geprüft und ein möglicher Eigenbehaltsschaden der Wiener Städtischen ermittelt. Die Ermittlung erfolgt durch eine Multiplikation der Versicherungssummen im Eigenbehalt je Sparte mit spartenspezifischen Schätzern des Kumulschadenspotentials. Nach der Methode aus 2018 kommt die Wiener Städtische hier auf einen Schadenpotential im Eigenbehalt[37] im mittleren zweistelligen Millionenbereich.

Ein kurzer Blick auf 2.1 zeigt, dass sich seitdem jedoch viel getan hat: Durch das starke Bestandswachstum und neue Abschätzungsmethoden kommt der Rückversicherer mittlerweile zu einer realistischeren Kumulabschätzung von etwa einem Drittel des ursprünglich veranschlagten Betrages.

Die verwendeten spartenspezifischen Schätzer wurden ebenfalls verwendet, um zusammen mit der Bestandsprojektion je Sparte eine Kumulprognose abgeben zu können. Diese

[37] Stand 30.06.2021

wird monatlich im Report "Kumulsicht Cyber" vom Aktuariat Sachversicherung der Wiener Städtischen aufgearbeitet. Die dort verwendeten Datenpunkte[38] wurden in *RStudio* übertragen, ebenfalls wurde die neue Bestandsprojektion als weitere Option in das hinter der Auswertung liegende Excel-File eingebettet. Folgend wurde das Ergebnis der bisherigen Kumulprojektion im Vergleich mit der neuen Methode aus dieser Diplomarbeit, aus Datenschutzgründen affin transformiert. In der Auswertung selbst ist die Prognose zwar nur bis zum 31. Dezember 2022 angegeben, wir extrapolieren hier jedoch weiter und sehen uns die Methoden mittelfristig innerhalb der nächsten drei Jahre an:

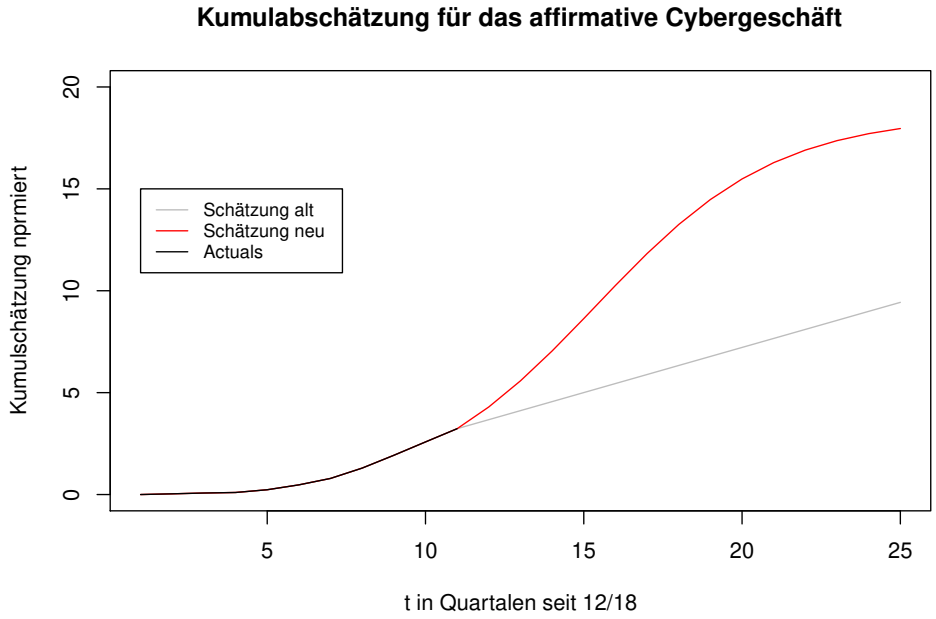


Abbildung 2.7: Vergleich der Kumulprojektionsmethoden

Bis zum 31. Dezember 2022 ($t = 17$) hin unterscheiden sich die Verläufe der Projektionen gravierend, was sich bis zum 31. Dezember 2024 ($t = 25$) nicht ändert. Dies ist hauptsächlich mit der antizipierten Verfünffachung des Produkts "Cyber Protect" sowie den hohen Wachstumsraten im Privatgeschäft zu begründen. Die neue Kumulprojektionsmethode sieht hier ein Einpendeln des Kumulpotentials bei einem Wert von etwa 20. Die sigmoidförmige Kurve ist durch die logistische Wachstumsannahme begründet. In diesem Kapitel wurden die je-

[38] Vgl. interne Auswertung "Kumulsicht Cyber per 2021-06-30"

weiligen Obergrenzen aus den eigenen Bestandsdaten realistisch geschätzt beziehungsweise von Experteneinschätzungen hergeleitet. Ebenfalls wirkt die logistische Wachstumsannahme mittelfristig durch die entsprechende Literatur[39] gerechtfertigt und wird durch die These unterstützt, dass Cyber-Risiken in der näheren Zukunft immer mehr an Relevanz gewinnen werden.

Plausibilisierung des Prognosemodells

Ob die obigen Überlegungen auch ein robustes Modell mit gutem Fit zu den bestehenden Datenpunkten liefern, wollen wir nun näher untersuchen:

Dazu wird zunächst die Passgenauigkeit des neuen, logistischen Modells mit der des alten, linearen Modells verglichen. Da wir das Marktpotential G nicht aus den Daten, sondern qualitativ schätzen, besitzen beide Schätzungsmethoden zwei Freiheitsgrade. Dies gibt uns die Möglichkeit, beide mittels ein- und demselben *Goodness of fit*-Maß zu vergleichen.

Hierzu wäre es naheliegend, das Bestimmungsmaß R^2 des linearen Modells heranzuziehen, welches wie folgt definiert ist:

$$R^2 := 1 - \frac{\sum_{i=1}^{n}(y_i - x_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2},$$

mit y_i den gemessenen Werten, x_i den Schätzwerten sowie $\bar{y}$ dem arithmetischen Mittel der gemessenen Werte.

Für den Vergleich mit einem nonlinearen Modell, wie das logistische Wachstum eines ist, liefert R^2 jedoch keine aussagekräftigen Werte. Dies ist der Methodik der kleinsten Quadrate geschuldet, auf der diese Kennzahl basiert. Für diesen Fall, insbesondere bei monotonen Modellfunktionen, bietet es sich alternativ an, die Pearson-Korrelation der gemessenen mit den geschätzten Daten zu betrachten, welche im Nachhinein quadriert wird. Je näher dieser Wert bei 1 liegt, desto besser erklärt die gewählte Modellfunktion die zugrundeliegenden Messdaten. Diese Kenngröße notieren wir mit qR^2 und definieren sie wie folgt:

$$qR^2 := \frac{(\sum_{i=1}^{n}(y_i - \bar{y})(x_i - \bar{x}))^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2 \sum_{i=1}^{n}(x_i - \bar{x})^2}$$

Folgend die Werte des Bestimmtheitsmaßes, aufgeteilt nach Wahl des zugrundeliegenden Modells sowie der zu modellierenden Produktgruppe:

[39] Vgl. [Sok08]

Gewählte Methode	qR^2 Rechtsschutz	qR^2 Haushalt	qR^2 Cyber Protect
Lineares Modell	0.7919	0.9408	0.967
Logistisches Modell	0.9865	0.987	0.9607

Tabelle 2.5: Vergleich des Bestimmtheitsmaßes der Modelle

Wie zu sehen ist, erklären sowohl das lineare als auch das logistische Modell die derzeit vorhandenen 11 Datenpunkte je Produktgruppe gut. Das fast explosive Wachstum der Rechtsschutz-Produkte (vgl. dazu Tabelle 2.1) lässt sich jedoch mit letzterer Modellfunktion besser beschreiben, was sich in einem höheren Wert von qR^2 ausdrückt. Dies, die betriebswirtschaftlichen Grundüberlegungen und die antizipierte hohe Absatzsteigerung von Cyber-Produkten in der Zukunft rechtfertigt derzeit die Einführung des logistischen Modells. Ein Vergleich verschiedener Extrapolationsverfahren sollte in diesem Fall jedoch laufend angestellt werden, um Fehler in der Modellwahl zu minimieren.

Weiters wollen wir den einzigen qualitativ gewählten Parameter im logistischen Wachstumsmodell einer Sensitivitätsanalyse unterziehen: Genauer ist es von Interesse, wie sich eine Fehleinschätzung des Marktpotentials der modellierten Produkte mittelfristig in der Kumulprognose auswirkt. Hierzu betrachten wir, zusätzlich zu unserer Grundannahme, sechs Szenarien, in denen der Parameter G als 10, 20 und 30% niedriger oder höher als bisher angenommen verwendet wird.

Mit den verschiedenen, neuen Werten für die Obergrenze G der Wachstumskurven der Rechtsschutz-, Haushalts- und Firmen-Cyberprodukte wurde in *RStudio* analog zum Basis-Szenario das Bestandswachstum modelliert und eine neue Cyber-Kumulprognose ausgewertet. Die relativen Änderungen ebendieser in % zum Basisszenario sind in der folgenden Grafik ersichtlich:

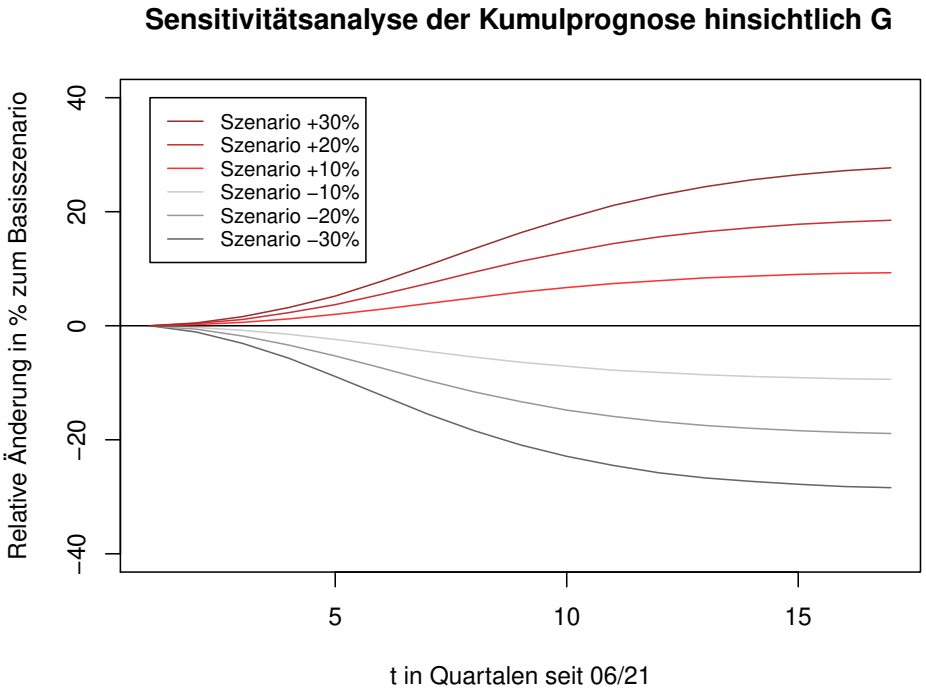


Abbildung 2.8: Sensitivitätsanalyse der Kumulschätzung

Im Falle einer Über- respektive Unterschätzung nähert sich die relative Änderung klarerweise genau dem Wert an, mittels dem die natürliche Grenze G modifiziert wurde (also +/-10, 20 oder 30%). Bis 31.12.2023 ($t = 10$) würde sich etwa ein Fehler von +/-30% in einem Prognosefehler von 20% auswirken, wobei sich die mittelfristigen Folgen einer Unterschätzung des Marktpotentials schwächer auswirken als die einer Überschätzung. Bis zum 31.12.2022 ($t = 6$) würde eine Fehleinschätzung des Potentials im extremsten angenommenen Fall einen Prognosefehler um etwa 10% ergeben. In den Fällen eines geringeren Schätzfehlers bewegt sich diese Zahl in einem wesentlich kleineren Bereich.

Bei einem Fehler in der Schätzung der natürlichen Grenze G kann also mittelfristig mit einem Kumulprognosefehler in der Größenordnung um 10 bis 15% gerechnet werden. Solange also eine Unter- bzw. Überschätzung frühzeitig erkannt wird, hält sich der dadurch resultierende Prognosefehler aufgrund spärlich vorhandener Daten in Grenzen. Eine solche Abweichung kann etwa durch ein Absinken des Bestimmungsmaßes und das Plotten der einzelnen Prognosefehler je Datenpunkt, der sogenannten *Residuen*, passieren.

Selbst wenn die Expertenmeinungen zum Prämienvolumen im Cyber-Geschäft sowie die Modellierung aus betriebswirtschaftlicher Sicht wie oben bemerkt ebenfalls Unsicherheiten in sich tragen, so ist der Unterschied in den beiden Ergebnissen zumindest ein Warnsignal: Mit der derzeitigen Projektionsmethode besteht ein Risiko des Unterschätzens des eigenen Kumulpotentials.

Inwieweit die eigentliche Modellierung für den Bestand der Wiener Städtischen passend ist, lässt sich noch nicht beurteilen: Einerseits bieten die Rückversicherer nur selten tiefe Einblicke in die internen Modelle und Methoden. Andererseits müsste für ein internes Kumulmodell eine Szenarioentwicklung und -parametrisierung, eventuell angelehnt an diese Arbeit stattfinden. Ebenso sollte hierzu eine entsprechende Datenschnittsstelle aufgebaut werden, sowie für die Modellierung unverzichtbare Attribute bei den Versicherungsnehmern eingehoben werden. Der Problematik der Datenlage hinsichtlich Bestandsgröße und Schadenhistorie widmen wir uns im folgenden Abschnitt:

2.5 Problematik: Datenlage

Kumulschätzungen im Speziellen, aber auch das Bepreisen von Versicherungstarifen und Quantifizieren des Rückstellungsbedarf als "Alltagsgeschäft" bedürfen einer ausgiebigen Datenlage. Will man aus historischen Daten, am naheliegendsten natürlich aus dem eigenen Versicherungsbestand, also qualitativ hochwertige Prognosen für die Zukunft abgeben, so ist klarerweise die Anzahl an Beobachtungen maßgebend hierfür. Dies kann durch einen großen Bestand, wie etwa bei einem Marktführer der Fall, oder durch eine lange Schaden- und Bestandshistorie gewährleistet werden, etwa bei der etablierten Feuerversicherung. Dem Wesen der Cyberrisiken geschuldet, gibt es hier zumeist weder das eine, noch das andere. Da eine Vergrößerung des Blicks in die Vergangenheit unmöglich ist, bietet sich hier nur das Teilen der Daten unter einzelnen Versicherungsunternehmen an:

In der Wertschöpfungskette eines Versicherungsunternehmen entstehen viele verschiedene Arten von Daten. Einige von ihnen sind es wert, geteilt zu werden, so die britische Unternehmensberatung *Willis Towers Watson*[40]. Trotz der verschiedenen Eigenheiten der einzelnen Versicherungszweige lassen sich die Informationskategorien in sieben breitere Klassen einteilen:

- Kundendaten
- Informationen über das versicherte Objekt
- Historische Schadendaten

[40] Vgl. [WTW21]

- Telemetrie-Informationen über Kunden und Objekte (z.B. Gebäude, KFZ)
- Eigenschaften und Daten von internen Geschäftsprozessen
- Risikokalkulationen für Tarifierung und Reservierung
- Sonstige versicherungsrelevante Daten (bspw. Wetterinformationen)

Den Vorteilen, die das Teilen von Geschäftsdaten in der Wertschöpfungskette bringt, stehen jedoch auch verschiedenste Hindernisse gegenüber, die in drei Gruppen eingeteilt werden können:

- Kommerzielle Barrieren
- Rechtliche Hürden
- Wirtschaftliche Hindernisse

Unter Erstere fallen insbesondere Problematiken, die den Schutz des geistigen Eigentums und Wettbewerbsvorteile entsprechen. Ein Marktführer ist beispielsweise eventuell nicht daran interessiert, seine frisch um hohe Kosten optimierten Geschäftsprozesse und Informationen seines großen Bestands mit der Konkurrenz zu teilen.

Rechtliche Hürden betreffen hauptsächlich datenschutzrechtliche und kartellrechtliche Belange, mit denen sich jedoch die Anbieter dieser Pools intensiv befassen. Dadurch, dass das Thema auch im deutschsprachigen Raum seit einiger Zeit präsent ist, ist hier rechtliche Sicherheit mittels Gutachten gegeben[41].

Mit wirtschaftlichen Hindernissen sind Kosten gemeint, die bei komplexen Themen den jeweiligen Nutzen durchaus übersteigen können. Diese Aufwände entstehen durch Vorbereitung der Daten für die jeweilige Schnittstelle, die Anpassung an technische Standards sowie die Integration einer solchen Pool-Datenlandschaft in die unternehmensinternen IT-Systeme und -Applikationen.

Ob der Nutzen eines solchen Projekts nun für das einzelne Unternehmen die Kosten übersteigt oder nicht, hängt letzten Endes von einer Vielzahl an Faktoren ab. Die Wiener Städtische hat sich bewusst gegen eine solche Maßnahme entschieden:

Anwendbarkeit bei der Wiener Städtischen

Konkret wurde im Aktuariat für die Sachversicherungssparten die Teilnahme an einem angebotenen Cyber-Datenpool eines deutschen Marktführers überlegt. Vor allem für ein

[41] Vgl. [Koh21]

neuartiges Risiko wie Cyber wäre der Wissensgewinn mangels Schadenerfahrung vergleichsweise groß. Dennoch haben die Kosten/Risiken in dieser Rechnung überwogen, und zwar aus folgenden Gründen:

- Der eigene Vertragsbestand war zum Zeitpunkt der Überlegung bereits entsprechend groß, sodass zusammen mit den Wachstumsprognosen mit einer ausreichenden Datenbasis für die nächsten Jahre gerechnet werden konnte
- Die volle Verfügbarkeit der Datenbasis war erst nach einer Bindungsfrist gegeben, in den ersten Jahren wäre diese nur eingeschränkt verfügbar gewesen
- Ein Datenpool beherbergt oft übersehene **Einschätzungsrisiken**: Nicht berücksichtigt wurden in diesem Fall bei den Daten anderer Versicherungsunternehmen die verschiedenen Reservierungsverhalten, weshalb ein Vergleich mit den eigenen Reservehistorien nicht treffend wäre. Zudem werden die Details der Deckungsgestaltung der einzelnen Teilnehmer nicht weiter berücksichtigt, was die Schadenzahlungen ebenfalls schwer vergleichbar macht. Insgesamt existiert in den bereitgestellten Daten der anderen Unternehmen einiges an Unschärfe.

Zuletzt waren es die Kosten für Bereitstellung der eigenen Daten sowie der begrenzte Nutzen aus den Pooldaten über die ersten Jahre, welche das Unternehmen überzeugt haben, nicht an einem Cyber-Datenpool teilzunehmen.

Ausblick

Anders als im affirmativen Cyber-Geschäft besteht in "klassischen" Versicherungssparten kein Problem der mangelnden Bestandsgröße und Schadenhistorie. Doch auch diese Sparten können unter Umständen von neuartigen Cyber-Risiken betroffen sein. Dies wollen wir in den folgenden Kapiteln näher beleuchten und ein bestehendes Kumulszenario der Vienna Insurance Group weiterentwickeln:

3 Nicht-affirmative Cyberrisiken

3.1 Einführung

Cyber-Risiken sind für viele Versicherungssparten und Deckungen relevant. Im vorigen Kapitel wurden Versicherungsprodukte behandelt, welche jene Risiken explizit decken. Bei klassischen Versicherungsprodukten, etwa der KFZ-Kaskoversicherung, sind Bedrohungen dieser Art zumeist weder explizit ausgeschlossen noch eingeschlossen. Man spricht in diesem Fall von nicht-affirmativen beziehungsweise "Silent"-Risiken.

Nur wenige Versicherungsunternehmen widmen sich bisher dieser Problematik mittels expliziter Risikoausschlüsse: Laut einer europaweiten Befragung von Versicherungen durch die EIOPA haben nur fünf Versicherungsgruppen im Bereich der Schaden- und Unfallversicherung solche Exklusionen in ihre Polizzen eingebettet.[1] Die Gründe dafür sind verschieden. Zum Einen wird argumentiert dass es keinen Mehrwert biete, manche Versicherungszweige mit Cyber-Vorfällen in Verbindung zu setzen, etwa die Eigenheim- oder Unfallversicherung. Zum Anderen werden Cyber-Risiken von einigen Versicherungen nicht als für den Geschäftsbetrieb interessante Gefahr eingestuft und bedürfen keiner weiteren Beachtung. Doch auch wenn das Verbinden jener Risiken mit beispielsweise der Krankenversicherung derzeit eher abstrakt erscheinen mag, so ist durch den raschen technologischen Wandel in jeder "klassischen" Versicherungssparte ein Cyber-Exposure früher oder später realistisch.

Silent Cyber-Risiken wirken sich im Bestand eines Versicherers besonders auf zweierlei Arten aus: Sie können etwa eine Quelle für höherfrequente Normalschäden sein. In diesem Fall geht also dieser Risikofaktor nicht in die Tarifierung mit ein und kann die Schadenquote langfristig auf ein unprofitables Niveau heben. Durch die fehlende Berücksichtigung versichert das Versicherungsunternehmen diesen Teil des Risikos also "kostenlos".

Andererseits können Cyber-Attacken Auslöser für Großevents sein, welche durch unbeobachtete Risikokumule katastrophale Gesamtschadenhöhen hervorrufen können. Genau jene Gefahr versuchen wir im zweiten Teil der Arbeit mittels Szenarioanalyse zu quantifizieren.

Darüber hinaus berichtet die europäische Versicherungs- und Pensionskassenaufsicht aus

[1] Vgl. [EIO19, S.18f]

ihrem Dialog[2] über verschiedene Ideen und Vorgangsweisen in den europäischen Versicherungen zur Risikominimierung, welche wir folgend beleuchten wollen:

3.1.1 Derzeitige Herangehensweise an das Thema Silent Cyber

In obiger Marktstudie haben sich 59% der Versicherungsgruppen bereits mit der Möglichkeit auseinandergesetzt, sich Cyber-Risiken im eigenen Bestand zu widmen. Ihre Herangehensweisen unterteilt die EIOPA in zwei Gruppen: Lösungsorientierte und risikomindernde Maßnahmen.

Lösungsorientierte Maßnahmen zur Silent Cyber-Risikokontrolle

Bei Ersteren geht es um ein proaktives Auftreten des Versicherers gegenüber nicht-affirmativen Cyber-Risiken. Die EIOPA nennt hier als Beispiele

- die Versorgung des Bestandes mit affirmativen Cyber-Deckungsbausteinen
- den Ausschluss von bestimmten Risiken im Zuge von Verlängerungen oder Tarifwechsel
- die Gestaltung und Tarifierung neuer Versicherungsprodukte/Klauseln unter Rücksichtnahme von Silent Cyber-Risiken
- das weitere Analysieren der Auswirkung bestandsinterner, nicht-affirmativer Risikoexponierungen

Risikomindernde Maßnahmen zur Silent Cyber-Risikokontrolle

Die Maßnahmen letzterer Art in obiger Aufzählung unterteilen sich in

- Risk Assessment durch Szenarioanalysen
- das Anwenden von Rückversicherungsstrategien und vertraglichen Haftungsgrenzen
- das Optimieren des eigenen Risikoprofils durch aktives Underwriting

Zusätzlich wurden im Bericht Argumente angegeben, mit denen die noch nicht geplanten Risikomanagement-Tätigkeiten der vier Zehntel begründet wurden. Diese decken sich weitestgehend mit den Ausführungen am Anfang dieses Kapitels.

Prinzipiell wurden zwar einige verschiedene Maßnahmen im Dialog mit der europäischen

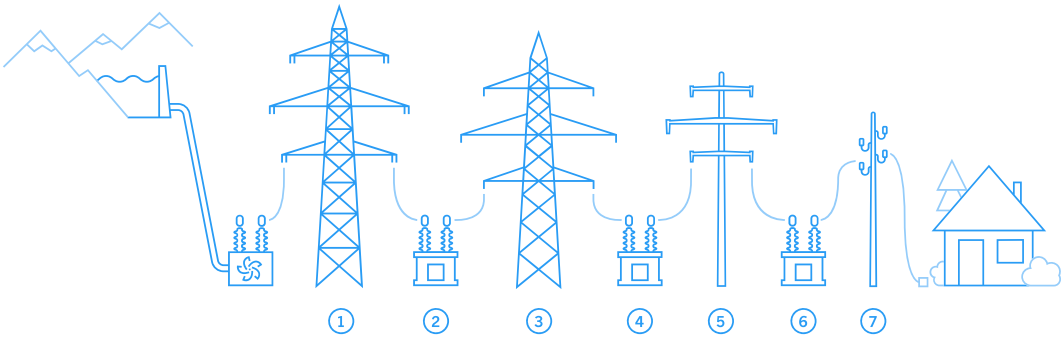
[2] Vgl. [EIO19, S.19]

Versicherungsaufsicht genannt, die quantitativen Ansätze werden jedoch nur von einem geringen Anteil der Versicherer wirklich verfolgt. Die Maßnahme der Szenarioanalyse bietet hier einen idealen Einstieg, um die eigene Risikotragfähigkeit sowie eventuelle Risikokumule sichtbar zu machen. Die in dieser Arbeit in dem Kontext erwähnten Rückversicherer, Berater sowie die EIOPA schlagen in ihren Werken hier allesamt als Szenario einen flächendeckenden Ausfall von Infrastruktur vor, wie etwa bei einem Blackout. Die technischen Hintergründe hierfür wollen wir nun erläutern:

3.2 Cyber-Risiken für das österreichische Stromnetz

3.2.1 Das österreichische Stromnetz

Das Stromnetz in Österreich gehört zu den Infrastrukturbereichen mit den höchsten technischen Standards. An vielen Punkten dieses engmaschigen Konstruktes wird elektrische Energie eingespeist und entnommen[3]. Dies geschieht im DACH-Raum (Deutschland, Österreich, Schweiz) auf insgesamt sieben Netzebenen, wie in der folgenden Grafik veranschaulicht wird:



Quelle: [Swi21]

Abbildung 3.1: Darstellung der Netzebenen im DACH-Raum

Ebenen gerader Nummerierung bezeichnet man als *Transformatorenebenen*, jene mit ungeraden Nummern sind *Spannungsebenen*. Was in den einzelnen Netzebenen zweiter Art passiert, wollen wir hier kurz näher erklären[4]:

[3] Vgl. [Wik21b]
[4] Vgl. [Ver21]

Netzebene 1 - Höchstspannungsnetz

In der obersten Netzebene wird mit Spannungen von 220 und 380 Kilovolt gearbeitet. Sie wird als Übertragungsnetz verwendet, auch der Stromhandel mit anderen Staaten und die Einspeisung aus beispielsweise Wasserkraftwerken geschieht hier.

Netzebene 3 - Hochspannungsnetz

Hochspannungsleitungen arbeiten mit 110 kV Spannung. Hier findet eine erste, überregionale Verteilung des Stroms statt. Weiters speisen viele Kraftwerke diese Spannung ein, und große Industriebetriebe, etwa Stahlwerke, entnehmen ihren Strom direkt aus diesem Netzniveau.

Netzebene 5 - Mittelspannungsnetz

Auf der vorletzten Ebene wird der Strom von regionalen Kraftwerken, etwa von Stadtwerken, eingespeist. Dabei treten Spannungen von einem bis 36 Kilovolt auf.

Netzebene 7 - Niederspannungsnetz

Von der regionalen Ebene wird nun auf die letzte, lokale Verteilungsebene transformiert. Hier speisen Energiegemeinschaften, Windparks und Photovoltaikanlagen ein, und der Strom kommt am Ende mit 400 bzw. 230 Volt aus der Steckdose.

Da wir im (inter-)nationalen Kontext bleiben und die Folgen von Blackouts im ganzen Staatsgebiet (und weiters in CEE) betrachten wollen, ist für uns vorwiegend der Ausfall der Netzebenen 1 und 3 von Interesse. Blackout-Risiken, die durch Cyber-Events ausgelöst werden, lauern aber auch und besonders in den engmaschigen lokalen Netzen; Dazu jedoch später mehr.

3.2.2 Wie kommt es zu Blackouts?

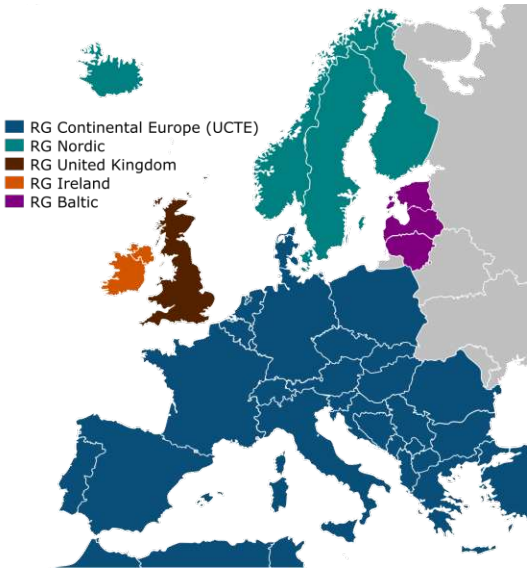
Die nationalen Stromnetze, gleich ob in Österreich oder in einem anderen europäischen Land, basieren großteils auf einem Nullsummenprinzip: Zu jeder Tages- und Nachtzeit, an jedem Tag im Jahr müssen die Stromzufuhr und der Stromverbrauch exakt gleich sein. Die dafür zu beobachtende Zielgröße ist die sogenannte *Netzfrequenz*. Sie beträgt im Normalfall 50 Hertz, die Wechselspannung weist also 50 Polaritätsumkehrungen in der Sekunde auf. Fällt die Frequenz ab oder steigt sie an, findet eine Unter- beziehungsweise Überspeisung des Netzes statt[5].

[5] Vgl. [Net21]

Das europäische Frequenzregelungssystem

Die Toleranz seitens des österreichischen Stromregulators *E-Control* liegt wie in ganz Kontinentaleuropa hier bei 200 Millihertz. Wird diese Grenze überschritten, wird innerhalb von 30 Sekunden die sogenannte **Primärregelreserve** aktiviert. Diese Reserve (in Form von ungenutzter Leistung einzelner, zuverlässiger Kraftwerke) steht neben der Sekundär- und Tertiärreserve als Backup innerhalb solidarischer Staatenverbände, welche sich gemeinsam zur Regelung der Netzfrequenz verpflichtet haben, zur Verfügung. Im europaweit größten jener Primärregelmärkte befinden sich Deutschland, Belgien, die Niederlande, die Schweiz und Österreich.

Darüber hinaus hängen jedoch weit mehr Staaten stromtechnisch voneinander ab. Die folgende Grafik illustriert sämtliche Netzverbände in Europa, die sich auf eine gemeinsame, synchronisierte Frequenz geeinigt haben:



Quelle: [Wik21d]

Abbildung 3.2: Darstellung der europäischen Regelverbände

Fällt also beispielsweise irgendwo im blau eingefärbten, kontinentaleuropäischen Raum die Frequenz ab, so senkt dies ebenfalls die Frequenz in allen Mitgliedsländern kurzfristig ab.

Auswirkungen von Frequenzänderungen

Eine nachhaltige Frequenzänderung um mehr als 200 Millihertz hätte in Europa weitreichende Konsequenzen: Nicht nur das Stromnetz selbst, sondern auch die meisten elektronischen Komponenten seitens Stromerzeuger (Kraftwerke, Generatoren) und -verbraucher (Regelmechanismen, Leiterplatten) sind auf eine Frequenz von 50 Hertz ausgelegt. Umspannwerke etwa können die erhöhte Stromlast bei einem Anstieg der Frequenz nicht dauerhaft mittragen, und würden sich irgendwann vom Stromnetz abkoppeln. Ebenso erleidet ein Großteil filigraner Steuerungselektronikteile Defekte, wenn er mit einer Spannungsspitze konfrontiert wird. So auch geschehen im Frühjahr 2021, als die größte Störung des europäischen Stromnetzes seit 2006 stattgefunden hat. Der Flughafen Wien beispielsweise musste infolgedessen mehrere Hunderttausend Euro an Hardware-Komponenten austauschen, berichtet die Tageszeitung "Kurier"[6]. Dieser Vorfall kommt der Charakteristik eines klassischen Blackout-Triggers sehr nahe, weshalb wir ihn näher betrachten wollen:

Das Beinahe-Blackout vom Jänner 2021

Am 8. Jänner 2021 kam es zu einem Fluss von unerwartet hohem Strom im Ausmaß von ca. 6000 Megawatt von Südosteuropa in Richtung Zentral- und Westeuropa. Diese Last verteilte sich zwar auf mehrere Leitungen und Umspannwerke, war im Endeffekt jedoch so stark, dass eine Kupplung eines Werks in Kroatien sich selbst aus Schutzzwecken vom Netz genommen hat. Infolgedessen verteilte sich selbige Last auf die übrigen Leitungen, und im Zeitraum einiger Sekunden gingen mehrere wichtige Übertragungsleitungen vom Netz. Die Frequenz stieg dabei im Balkanraum um bis zu 600 Millihertz an, im übrigen Teil der Union für die Koordinierung des Stromtransports, kurz UCTE (siehe 3.2), sank er um etwa 250 Millihertz. Durch

- den Einsatz von Primärregelenergie
- die Trennung der UCTE in zwei Teile, sowie
- das Abschalten großer Stromverbraucher

konnte in Sekundenschnelle seitens der Netzregulatoren reagiert und ein Blackout abgefangen werden. Es kam ausschließlich zu regionalen Stromausfällen[7].
Nichtsdestotrotz konnte im Jänner 2021 ganz Europa sehen, wie leicht das eigene Stromnetz ins Wanken gerät. Dass dies auch mutwillig passieren könnte, liegt absolut im Bereich des Möglichen:

[6] Vgl. [Kur21]
[7] Vgl. [Moe21]

Cyber Events als Trigger von Blackouts

Als energietechnisch klassischer Auslöser großflächiger Netzstörungen, die bis zum Blackout reichen können, werden Spannungsspitzen identifiziert. Wie beim Vorfall in Kroatien kann dies zur Überlastung einzelner Bauteile von Netzanlagen und infolgedessen zu einer Kettenreaktion führen. Ein künstliches Stromüberangebot kann zum Beispiel durch gezieltes Manipulieren großer Kraftwerksregler oder Windparksteuerungen, sowie das Abkoppeln von Großverbrauchern hergestellt werden. Ein gleichzeitiger Angriff auf die österreichische (bzw. europäische) Primärregelreserve würde diesen Effekt dazu um ein Vielfaches verstärken.

Doch auch in die andere Richtung können Hacker das Stromgleichgewicht ins Wanken bringen: Hier muss etwa kein großer Verbraucher, sondern ein großer Stromerzeuger abgekoppelt werden, um eine Unterversorgung des Stromnetzes zu initiieren. Da viele Elektronikkomponenten aber mehr unter einem Stromüber- als einem -unterangebot leiden, wäre der erstere Trigger für Hacker als attraktiver einzustufen.

Der Zusammensetzung der Regelmechanismen und Risiken im österreichischen Stromnetz selbst wollen wir uns in den folgenden Absätzen widmen:

3.2.3 Das österreichische Stromnetz im (inter-)nationalen Kontext

Um den österreichischen Strombedarf zu Spitzenzeiten bedienen zu können, gibt es zweierlei Mittel, derer sich der nationale Netzbetreiber bedienen kann: Einerseits besteht die Möglichkeit des Stromimports aus Nachbarstaaten. Dieser ist bis zu gewissen Kapazitätsgrenzen spontan möglich. Viel resilienter ist jedoch die Produktion bzw. gezielte Verwendung von Strom (bei einem Überangebot) innerhalb der eigenen Grenzen. Österreich hat hier einen immensen Vorteil gegenüber einer Vielzahl anderer europäischer Staaten:

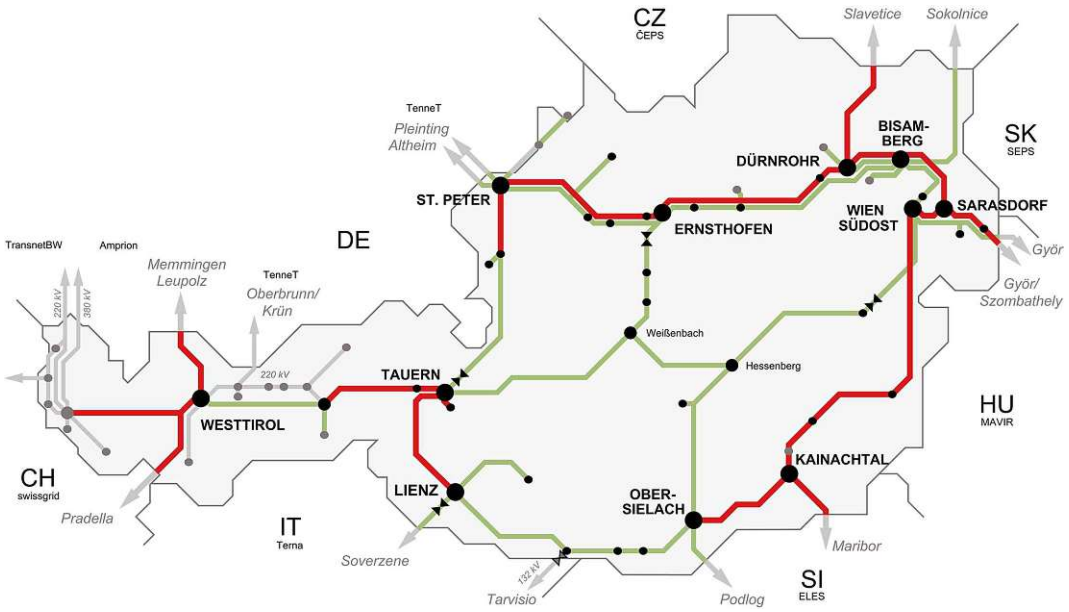
Es besitzt in den Alpen Pumpspeicher, etwa die Stauseen in Kaprun, die bei kurzfristigem Strommangel Wasser durch Turbinen ins Tal lassen und damit Strom erzeugen. Bei einem Überschuss können ebenjene Speicher wieder gezielt mittels Strom mit Wasser befüllt werden. Weiters können Laufkraftwerke, etwa die entlang der Donau, ebenfalls innerhalb kurzer Zeit ihre Leistung erhöhen. Auch Gaskraftwerke stehen für diese Aufgabe zur Verfügung (dezidiert Strom verbrauchen können diese jedoch naturgemäß nicht).

Die Pumpspeicher Österreichs alleine können, wenn man ihre mögliche Pump- als auch Einspeiseleistung zusammenzählt, derzeit die Strombilanz um etwa 7 Gigawatt bewegen[8]. Zum Vergleich: Die Lastspitze in Österreich beträgt derzeit etwa 11 Gigawatt.

[8] Vgl. [Moe21]

3.2.4 Die energietechnische Risikolage und -faktoren in Österreich und CEE

Der Großteil der vorhin beschriebenen Regelleistung ist geografisch im Alpenraum situiert. Um den hier entstehenden Strom im Extremfall in die verbrauchsstarke Ostregion befördern zu können, benötigt es Höchstspannungsleitungen. Folgend eine Karte des Höchst- und Hochspannungsnetzes in Österreich:



Quelle: [APG21]

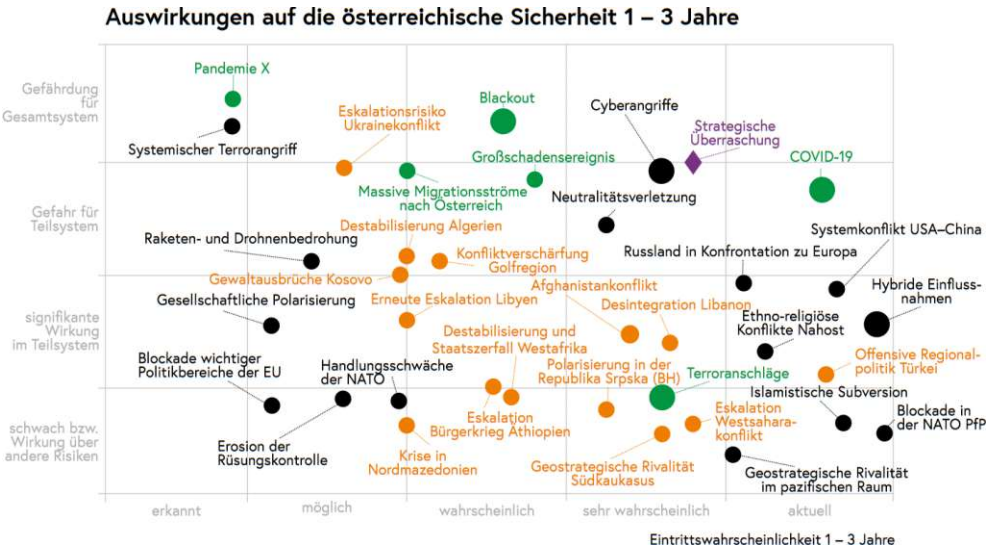
Abbildung 3.3: Das österreichische Stromnetz

In der Grafik rot eingezeichnet sind die stärksten derzeit verfügbaren Stromleitungen mit 380 Kilovolt Spannung. Grün markiert sind die 220 kV-Leitungen. Was derzeit laut Alfons Haber, Vorstand des mit der Stromsteuerung beauftragten Unternehmens E-Control, noch fehlt, ist der Ausbau der stärkeren Leitungen, um eine Art Höchstspannungs-Ring in Österreich zu installieren[9]. Dieser würde die großen Notfall-Einspeiser im Alpenraum mit der Ostregion verbinden, und bei einer Unterbrechung der Leitungen immer noch funktionieren. Derzeit sei dies zwar auch gegeben, aber die förderbare Leistung entspräche nicht dem realistisch installierbaren Maximum. Ebenfalls in der Ostregion beheimatet wären zu den großen Stromverbrauchern zudem große Windparks und Photovoltaikanlagen, wel-

[9] Vgl. [Moe21]

che etwa an bedeckten Tagen weniger Leistung bringen. Jene Energiegewinnungsmethoden bringen generell viel mehr Volatilität in den Strommarkt, als wir mit konventionellen, fossilen Energiequellen gewohnt sind.

Auch das österreichische Bundesheer analysiert häufig die Risikolage Österreichs bezüglich verschiedenster Gefahren. Die Gefahr eines prinzipiellen Blackouts wird hier als "wahrscheinlich" gesehen, mit erwarteten Auswirkungen auf die gesamte österreichische Infrastruktur. In der Risikomatrix für die nächsten drei Jahre stellt es daher ein entscheidendes Risiko dar:



Quelle: [Bun21]

Abbildung 3.4: Risikomatrix des Verteidigungsministeriums

Die Nähe des Blackouts zu den Bedrohungen "Großschadensereignis" und "Cyberangriffe" ist ein Indiz, dass Versicherer dieses Risiko auch als solches sehen und Maßnahmen zum Managen von Silent Cyber-Risiken setzen sollten. Das Ministerium für Landesverteidigung ortet auch weitere Kernthemen hinsichtlich Blackouts; Unter Anderem die mangelnde Vorbereitung der Bevölkerung auf dieses Szenario als auch die verbesserungswürdige Kommunikation der politischen Organe im Krisenfall könnten Schäden bei europaweiten Stromausfällen größer ausfallen lassen als anzunehmen ist.[10]

Um einen Vergleich zu haben, wie die österreichische Netzresilienz im Vergleich mit anderen europäischen Staaten aussieht, betrachten wir kurz die Werte des "SAIDI" (=*System*

[10] Vgl. [Bun21, S.313ff]

Average Interruption Duration Index) für diese Länder: Hierbei handelt es sich um die durchschnittliche Länge von ungeplanten Unterbrechungen der Stromversorgung pro versorgtem Verbraucher in einem Jahr. Der Index wird durch Störungsdaten errechnet und zeigt, dass Österreich, vor allem im Vergleich mit anderen Ländern im VIG-Portfolio, vergleichsweise sehr gut dasteht:

Land	SAIDI in Minuten
Österreich	34
Tschechien	98
Slowakei	111
Ungarn	67
Kroatien	176
Rumänien	635
Lettland	621
Litauen	73

Quelle: [Wik21e]

Tabelle 3.1: Vergleich des SAIDI Österreichs mit ausgewählten europäischen Ländern

Dies ist wichtig, um die energietechnische Relevanz von beispielsweise Höchstspannungsleitungen und genug Primärregelreserve nachvollziehen zu können. Diese Kenntnisse könnten auch für eine lokale Abschwächung der Blackout-Szenarien als Risikoparameter stellvertretend für die Resilienz des nationalen Stromnetzes Verwendung finden.

3.2.5 Zukünftige Risikofaktoren für Blackoutszenarien in Österreich

Bevor wir Blackouts aus versicherungstechnischer Perspektive betrachten, wollen wir abschließend einen Ausblick darauf geben, wie sich die energietechnische Risikolandschaft in naher und mittlerer Zukunft verändern kann und wird, und was hier in Richtung Silent Cyber zu beachten ist:

Umstieg auf erneuerbare Energien

In Österreich sowie in ganz Europa wird ein Umstieg von fossiler Stromgewinnung auf erneuerbare Energien forciert. Die Stadt Wien etwa[11] will bis zum Jahr 2040 klimaneutral werden. Betrachtet man die Umwelterklärung des wichtigsten Energielieferanten in Wien, der *Wien Energie*, so erhält man Einblick in die Größenordnung dieses Vorhabens, die Wärmeproduktion einmal außen vor gelassen:

[11] Vgl. [Aue21]

Stand 2020 betrug der Anteil erneuerbarer Energien der Wien Energie 19,7%. Im Zuge einer Anhebung dieses Anteils bis zur Klimaneutralität würde (etwa durch Umstieg von Gasthermen auf elektrische Wärmepumpen) der prinzipielle Strombedarf der Stadt Wien bis 2040 um 63% ansteigen, so "die Presse". Die dafür nötigen Stromimporte in das Stadtgebiet würden sich dafür von circa 2 auf über 11 Terawattstunden erhöhen. Um das in einen weiteren Kontext zu bringen: Dies würde über 10% der derzeitigen Lastspitze in ganz Österreich entsprechen!

Um einen solchen Strombedarf bedienen zu können, müssen viele Anlagen zur Energiegewinnung aus zum Beispiel Solarenergie oder Wasserkraft erbaut werden. Zusammen mit dem Ausbau privater Photovoltaikanlagen und der Elektromobilität werden in Zukunft immer mehr stromerzeugende und -verbrauchende Anlagen an das Netz angeschlossen, was einem Hacker zusätzliche Angriffspunkte für eine Frequenzmanipulation liefert. Nebenbei steigt damit natürlich auch das rein systeminterne Risiko eines Blackouts durch erhöhte Komplexität.

Schwarzstartfähigkeit und Primärregelleistung

Durch den oben beschriebenen Ausstieg aus fossilen Energiequellen steigt natürlich nicht nur in Wien, sondern in ganz Europa der allgemeine Strombedarf (Stichwort Heizen/Kühlen, Elektromobilität). Dem gegenüber stehen die Primärregelreserven, deren Leistungsausbau das Potential hat, eher übersehen zu werden.

Dazu wird durch das Abdrehen von "konventionellen" Kraftwerken eine Vielzahl an sogenannten *schwarzstartfähigen* Kraftwerken eingestellt. Dieser Begriff bezeichnet die Fähigkeit eines Kraftwerks, von sich aus ohne Stromzufuhr den Betrieb aufnehmen zu können. Glaubt man den Einschätzungen des deutschen Energieberaters "Stromdao"[12], so ist diese Fähigkeit bei den Erneuerbaren am ehesten bei der Wasserkraft gegeben; Auch derzeit besitzen viele Lauf- und Pumpspeicherkraftwerke die Schwarzstartfähigkeit. Bei Wind- und Solarenergie, auf deren Ausbau derzeit Fokus gelegt wird, gibt es hier jedoch Probleme: Wechselrichter von Photovoltaikanlagen zum Beispiel brauchen eine vorhandene Netzfrequenz, um ihren Strom aus Sonnenenergie einspeisen zu können. Strom aus Windkraft hat diese Probleme laut dem Expertenteam, welches auch Simulationen zum Neustart von Stromnetzen anbietet, nicht. Windkraftanlagen werden jedoch häufig per Fernzugriff betrieben. Diese Einrichtung wäre bei einem Blackout ohne Notstromversorgung der Anlage und ohne eigene Telekommunikation (über Speicher oder Aggregate) nicht funktionsfähig.

[12] Vgl. [Cor21]

Smart Grids

Ein weiterer Effekt des Modernisierens und Digitalisierens der Stromnetze ist die Etablierung sogenannter *Smart Grids*. Diese intelligenten Steuerungsmechanismen im elektrischen Energiebereich werden mit der Zeit immer komplexer: Endverbraucher nehmen mit ihrer PV-Anlage am Hausdach am Strommarkt als Erzeuger und Verbraucher teil, es bilden sich eigene Energiegemeinschaften auf den unteren Netzebenen, lokale Energiespeicher zum Lastenmanagement werden errichtet. Dadurch entstehen immer mehr Kontroll-, Mess- und Steuerungspunkte in einem System, das häufig über das Internet kommunizieren muss. Dies erhöht die Vulnerabilität für einen Hackerangriff auf die österreichische Energie-Infrastruktur um Dimensionen, und dies nachhaltig[13].

Generell steigt durch vielerlei Faktoren die Komplexität im Stromnetz an, dadurch sinkt entsprechend die Resilienz, wie man sie in den letzten 30 Jahren gewohnt war. Herbert Saurugg, Präsident der österreichischen Gesellschaft für Krisenvorsorge, fasst die zukünftigen Risiken treffend zusammen:

> *Grundproblem ist die steigende Instabilität des Systems. Waren im Jahr 2011 noch zwei Eingriffe bei Kraftwerken nötig, um alles zu stabilisieren, gab es 2018 Eingriffe an 301 Tagen. Wenn ein System schon permanent unter Stress läuft, steigt die Gefahr, dass irgendeine Kleinigkeit das ganze zum Kippen bringt. Das kann eine technische Störung sein, aber auch ein Extremwetterereignis. Auch Cyberangriffe oder Sonnenstürme zählen dazu. Mein erwartetes Szenario ist ein Systemkollaps durch Komplexitätsüberlastung.*[14]

3.3 Analyse des Blackouts und seine Effekte

Wir wollen im Folgenden nun erarbeiten, welche Auswirkungen ein Blackout gemäß sowohl britischen als auch österreichischen Expertenschätzungen auf das tägliche Zusammenleben und ein versichertes Risiko im Bestand eines Versicherers hat. Zusätzlich plausibilisiert werden diese Erwartungen durch Erkenntnisse aus der Energiekrise in Texas, welche sich im Februar 2021 ereignet hat. Hierbei kam es zwar "nur" zu einem Teil-Blackout, doch vor allem das menschliche Verhalten bei einem solchen Ereignis ist zeichnend für die Abschätzungen, die bei einem totalen Infrastrukturausfall zu tätigen sind:

[13] Vgl. [Cam15, S.50f]
[14] aus [Gra21]

3.3.1 Verlauf eines Blackouts

Vielerorts befassen sich mittlerweile Versicherungsunternehmen, Risikomanager, Ministerien und sogar Armeen mit dem Thema Blackout und seinen Folgen. Ergebnis dieser Überlegungen ist ein recht genaues Bild davon, wie man sich die Folgen eines überregionalen, flächendeckenden Stromausfalls in der gesamten UCTE vorstellt:

Die Forscher der Judge Business School der Universität Cambridge haben etwa gemeinsam mit dem Versicherer *Lloyds* das amerikanische Stromnetz in Zusammenhang mit Blackouts analysiert[15]. Einige ihrer Erkenntnisse lassen sich auch in den kontinentaleuropäischen Raum übersetzen und zusammen mit nationalem Wissen ([Bun21], [Ser21]) weiter für unseren Anwendungsbereich, den CEE-Raum mit Fokus auf Österreich, konkretisieren.

Wir teilen den Ablauf eines Blackouts in drei Phasen ein:

Teil 1: Die ersten 24 Stunden

Das Blackout macht sich zunächst über die "klassischen" Charakteristika bemerkbar: Es gibt keinen Strom, kein elektrisches Licht. Kühlungen und elektrische Heizungen fallen sofort aus, Aufzüge bleiben stecken, U-Bahnen ebenso. Fehlende Verkehrsampeln führen zu einem sofortigen Verkehrschaos.
Weiters fallen Mobilfunk sowie Festnetz-Verbindungen aus, sofern diese nicht notstromversorgt sind. In Spitälern und Feuerwehren springen Notstromaggregate an.

Dadurch, dass dem Stromausfall eine heftige Frequenzabweichung zuvorgegangen ist, ist zudem anzunehmen, dass ein beträchtlicher Teil der ans Netz angeschlossenen Elektronik hiervon Schaden nehmen wird. Besonders bei Bauteilen im 24-Stunden-Betrieb ist hier mit Ausfällen zu rechnen.[16]

Teil 2: Die darauffolgenden 6 Tage

Der Zeitraum von bis zu einer Woche nach dem Eintritt des Blackouts ist geprägt von Unruhen: Die Videoüberwachung kritischer Infrastruktur funktioniert nicht mehr, daher müssen Supermärkte, Tankstellen oder Banken bewacht werden. Es kommt zu Plünderungen und Vandalismus, vor allem in Ballungszentren. Erste Brände machen sich bemerkbar, da die Bevölkerung versucht mit Holz und dergleichen zu heizen und zu kochen, besonders im Winter. Durch einen Abwasserrückstau überfluten die Kanäle.

Auch einige Notstromaggregate könnten nun langsam den Betrieb einstellen müssen, damit sind vielerorts Pflegedienste und medizinische Dienstleistungen nicht mehr verfügbar,

[15] Vgl. [Cam15]
[16] Vgl. dazu [Gra21] und [Kur21]

was sich in einer erhöhten Mortalität der Bevölkerung auswirkt. Viehwirtschaften müssen Notschlachtungen durchführen, etwa bei Milchkühen und Geflügelbetrieben.[17] Auch der Handel und Transport stehen still, nach eventuellen Panikkäufen sinkt der Konsum. Dies macht sich durch einen massiven Einbruch über die gesamte Wertschöpfungskette bemerkbar.

Dem gegenüber stehen erste Versuche, das Stromnetz wieder aufzubauen. Im Idealfall, also ohne weitere Behinderung seitens Schadsoftware oder technischer Schäden, sollte damit in Österreich bereits nach einem Tag zumindest begonnen werden. Das heißt jedoch noch lange nicht, dass überall Strom verfügbar ist, hier würde ein Inselbetrieb stattfinden, um ein kleines Netz mit wenig Last vorerst stabil halten zu können. Nach etwa einer Woche sollen diese Versuche in ganz Europa stattfinden.[18]

Teil 3: Die Zeit bis zur Wiederherstellung

Die Synchronisierung der einzelnen Inseln wird ab der zweiten Woche nach dem Blackout anlaufen. Damit wird auch wieder mit der Produktion von Waren begonnen, es bestehen jedoch noch immer beträchtliche Einschränkungen hinsichtlich der Kommunikation. Spitäler und Wasserwerke funktionieren wieder, anschließend wird an einer rudimentären Grundversorgung der Menschen gearbeitet. Bis die Versorgung wieder ernsthaft anläuft, vergeht laut Herbert Saurugg noch einige Zeit: An vielen Punkten hat die Wirtschaft erheblichen Schaden genommen, Millionen Nutztiere sind europaweit gestorben. Besonders Regionen, die vom Tourismus oder Dienstleistungen leben, werden mittelfristig noch stärker betroffen sein.

3.3.2 Mögliche Auswirkungen für Versicherer

Um den möglichen Schaden für Versicherer abwägen zu können, gilt es zunächst, sich zu überlegen, welche Parteien bei einem Blackout zu Schaden kommen könnten. Der Schaden kann hier direkt an eigenen Aktiva/Besitztümern, aus einer Betriebsunterbrechung heraus oder durch Ansprüche Dritter entstehen. Beispiele hierfür lassen sich aus vielerlei Quellen zusammentragen, jedoch auch durch intensiven Austausch mit Branchenexperten und Brainstorming erarbeiten. Eine mögliche Aufteilung wird in dieser Arbeit in den folgenden Absätzen vorgenommen (Wir betrachten hier nur Schäden für Versicherer, für Schäden an der Volkswirtschaft wird beispielsweise [RSS13] empfohlen):

[17] Vgl. [Ser21]
[18] Vgl. [Gra21]

Vandalismus, soziale Unruhen

Das Bundesheer rechnet nach 72 Stunden ohne Strom mit gewalttätigen Auseinandersetzungen und Plünderungen, speziell im urbanen Raum. Schäden, die hieraus entstehen, treffen beispielsweise

- KFZ-Kaskoversicherungen
- Wohngebäude- und Eigenheimversicherungen
- Einbruch-/Diebstahlversicherungen

Speziell bei KFZ-Kaskoversicherungen wird sich in den ersten Minuten und Stunden des Blackouts in urbanen Räumen durch das Verkehrschaos ein erhöhtes Kumulrisiko realisieren.

Elementarversicherungen

Sowohl im zivilen als auch im gewerblichen Geschäft gibt es einige Deckungen, die in einem Blackout schlagend werden, etwa die **Feuerversicherung**, Versicherungen gegen **Überspannung** und **Wasserleitungsbruch** (Frostschäden im Winter).

Verderbliche Güter

Durch den Ausfall aller Kühlungseinrichtungen kommt es im Industriebereich, etwa bei Transportversicherungen, zu hohen Forderungen. Doch auch im Zivilbereich ist bei der Haushaltsversicherung der Kühlbehälterinhalt oft mitversichert.

Rechtsstreitigkeiten und Ansprüche Dritter

Nach Wiederherstellung kann ein Anstieg in der Zahl geführter Gerichtsprozesse vermerkt werden, sei dies zum Durchsetzen von Schadenersatzansprüchen oder wegen Vertragsstreitigkeiten innerhalb der wirtschaftlichen Wertschöpfungskette. Hier bestehen Kumulrisiken in sowohl gewerblichen als auch privaten Rechtsschutzversicherungen.

Auch ein versicherter Einkommensausfall Selbstständiger wäre in hohem Ausmaß von einem Blackout betroffen.

Spezialprodukte: Veranstaltungen und All-Risk

Bei der Veranstaltungs-Ausfallversicherung wären im Falle eines Blackouts alle zu diesem Zeitpunkt versicherten Events betroffen.

Einen Sonderfall bieten All-Risk- bzw. *Extended Coverage*-Versicherungen: Sie decken sogenannte "Unbenannte Gefahren". Das heißt, dass alle Gefahren für zB ein Gebäude gedeckt sind, die bei Vertragsabschluss nicht explizit ausgeschlossen wurden. Auch hier ist eine entsprechend hohe Schadenanzahl zu erwarten.

Personenversicherungsansprüche

Nicht zu vergessen sind neben den Schadenversicherungs- auch die Personenversicherungsansprüche: Infolge eines Verkehrschaos könnten in den ersten Stunden des Blackouts Unfallverletzungen passieren. Ebenso kann es besonders im Winter und Sommer zu Hypo-/Hyperthermien kommen. Auch soziale Unruhen, verschlechterte Hygienebedingungen, fehlende Medikamente und überlastete Krankenhäuser können das versicherungstechnische Risiko in der Kranken-, Lebens- und Unfallversicherung erhöhen.

Dazu bestehen mit der Betriebsunterbrechungs- und Maschinenbruchversicherung zwei besonders betroffene Versicherungszweige in den Beständen der meisten Versicherer. Auch die Covid-Krise hat gezeigt, dass die Betriebsunterbrechungsversicherung bei großen Katastrophen einem Klumpenrisiko ausgesetzt ist. Gegensteuern kann man hier mit Abschluss einer Rückversicherung und entsprechendem Wording in den Versicherungsbedingungen.

Versicherungstechnische Überlegungen

Generell ist ein Deckungsbaustein dann einem Blackout-Risiko ausgesetzt, wenn dies die Vertragsbestimmungen auf Polizzenebene auch zulassen. Daher ist eine Deckungs- und Klauselanalyse als initialer Schritt für Cyber-Analysen unerlässlich.

Weiters ist es sinnvoll, in einzelnen Sparten zwischen Frequenzschäden und Großschäden zu unterscheiden. Dies geschieht in der aktuariellen Tätigkeit oftmals sowieso, und bietet uns hier einige Vorteile: Unter Anderem können dann spezielle Rückversicherungskonstruktionen berücksichtigt werden, um nicht nur den Bruttoschaden im Bestand abbilden zu können, sondern auch den, wirtschaftlich weitaus wichtigeren, Schaden im Eigenbehalt.

3.3.3 Reales Beispiel: Die texanische Energiekrise

Eine Extremversion eines Blackouts, nämlich die in Hitze-/Kälteperioden, konnte im Februar 2021 mitsamt seinen Folgen im US-Bundesstaat Texas beobachtet werden. Wir werden Berichte zu dieser Stromkrise verwenden, um die Annahmen in dieser Arbeit zu validieren:

Der Grund für den Stromausfall war ein "Blizzard", ein Schneesturm, der zusammen mit extrem kalten Temperaturen 75% der texanischen Haushalte stromlos gemacht hat.[19]

[19] Vgl. [Wik21c]

Zusätzlich bedeutete eine unerwartete Lastspitze den Todesstoß für das Stromnetz. Aufgrund der Kälte barsten Wasserleitungen, die Bevölkerung stand zudem vor einer Nahrungsmittelknappheit aufgrund unzulänglicher Vorbereitung.

Auch soziale Unruhen ließen nicht lange auf sich warten, waren durch die niedrigen Temperaturen und mangels Organisationsmöglichkeiten jedoch eher gedämpft. Ebenso waren durch dieses Ereignis Hunderte Todesopfer zu beklagen, sowohl durch Kohlenmonoxidvergiftungen, Unterkühlung, Autounfälle als auch verschiedenste Brände. Die Einschätzungen der verschiedensten Experten, wie in 3.3.1 angeführt, erscheinen also durchaus realistisch.

3.4 Schätzung mittels Szenarioanalyse

Wir wollen uns nun der Szenarioschätzung annähern, in der wir genau die Erkenntnisse der letzten Abschnitte in eine Szenarioschätzung der VIG einfließen lassen wollen. Zunächst befassen wir uns etwas mehr mit der Methodik der Szenarioanalyse an sich:

3.4.1 Warum eigentlich Szenarioanalyse?

Szenarien sind "Geschichten" darüber, wie sich die Zukunft eventuell entwickeln könnte. Die Risikokontrolle mittels Szenarien ist eine von vielen (siehe Kapitel 2) Methoden für Versicherungen, sich auf zukünftige Risiken besser einstellen zu können. Besonders bei Risiken und Systemen, die man zum derzeitigen Zeitpunkt versicherungstechnisch noch nicht hinreichend versteht, bietet die Auswertung des Gewinns/Verlustes in einem gewissen Szenario einen systematischen Ansatz, um das Verständnis über Kumule im eigenen Bestand zu verbessern.[20]

Dazu ist der Prozess der Szenarioerstellung alleine für den Aktuar und Entscheidungsträger im Unternehmen schon ein wichtiger Schritt um sich intensiv mit einem bis dahin wenig beleuchteten, komplexen Problem der realen Welt auseinanderzusetzen. Im Umfeld des quantitativen Risikomanagements spricht man hier von sogenannten "Emerging Risks".[21]

Zudem ermöglichen Szenarien einen gewissen kreativen Prozess und Austausch mit verschiedensten Stakeholdern, was dem Risikoverständnis zuträglich ist. Sind Szenarien erstellt, hilft zudem ein Vergleich der einzelnen Ansätze mit anderen Parteien, die sich jenem Problem ebenso mittels dieser Methode angenommen haben: So können Denkfehler und Wahrnehmungsverzerrungen, etwa basierend auf der vergangenen und derzeitigen Unternehmensstrategie, rasch aufgedeckt werden.

[20] Vgl. [Jud20, S.6f]
[21] Vgl. [Jud20, S.15f]

3.4.2 Beginn eines Szenarioaufbaus

Vor Initiieren des klassischen Erstellungsprozesses eines szenariobasierten Modellansatzes gilt es, sich von unerwünschten Szenariotypen abzugrenzen[22]:

Trendrisiko - Stressrisiko

Zuerst muss geklärt werden, ob es sich um einen plötzlichen Schock für das Portfolio handeln soll (wie bei einem Blackout), oder Langzeitfolgen abgeschätzt werden sollen, etwa in Verbindung mit der Klimakrise.

Deterministisch - Probabilistisch

Diese Unterscheidung haben wir bereits in 2.3 behandelt, die Entscheidung für einen dieser Typen hängt meist von der Datenlage und dem geplanten Arbeitsaufwand ab.

Explorativ - Normativ

Zusätzlich ist das Ziel der Modellierung festzulegen: Die *explorative* Szenarienentwicklung hat das Motiv, das Wissen über den zugrundeliegenden Prozess zu erweitern und sich im kreativen Prozess plausible Ereignisverläufe zu überlegen. Dem gegenüber stehen *normative* Szenariomodellierungen, welche technisch formuliert werden und dafür erstellt werden, aus dem Versicherungsportfolio Kennzahlen abzuleiten. Klassische Beispiele für Letztere finden sich in den EIOPA-Stresstests[23] sowie bei der Errechnung des SCR[24].

3.4.3 Ablauf der Szenariomodellierung

Wie der Ablauf einer Szenarioentwicklung im Idealfall aussieht, wurde im Jahr 2020 vom Cambridge Centre for Risk Studies gemeinsam mit dem *Lighthill Risk Network*[25] dokumentiert. Auch wenn sich andere Prozeduren von dieser leicht unterscheiden können, so haben sie alle einen gemeinsamen Kern.

Die Schritte dieser repräsentativen Aufteilung wollen wir kurz näher beleuchten:

[22] Vgl. [Jud20, S.18ff]
[23] Vgl. [EIO21]
[24] Vgl. [AVo21]
[25] Vgl. [Jud20]

Quelle: [Jud20, S.9]

Abbildung 3.5: Best Practice: Arbeitsablauf bei der Szenarioentwicklung

Schritte 1 & 2: Risikoselektion und Recherche

Die ersten beiden Schritte sind geprägt von der Orientierung in der betroffenen Risikolandschaft: Es gilt, eine Forschungsfrage aufzustellen und dadurch das zu untersuchende Risiko zu definieren. Dies kann von der tatsächlichen Gefahr selbst ausgehen (zum Beispiel einem Erdbeben), aber auch im Zuge einer Vulnerabilitätsanalyse geschehen. Hier betrachtet man ein potentiell betroffenes Objekt, und überlegt sich welchen Risiken es ausgesetzt sein könnte. Die Ergebnisse dieser Selektion werden im Laufe der Modellierung laufend verfeinert.

Danach folgt eine Recherche, bei der Informationen bei Experten und in wissenschaftlicher Literatur eingeholt werden. Genauer sollte das betroffene Risiko aus jedem Blickwinkel und Niveau beleuchtet werden: Sind die Einzelrisiken einem Trend unterworfen? Wie wirken sie sich auf eine Einzelperson aus, wie auf die verschiedenen Geschäftsbereiche, in denen die Versicherung Kunden hat? Wie ist die Meinung der eventuell betroffenen Industrien sowie der wissenschaftliche Konsens dazu?

Schritte 3 & 4: Abgrenzung des Szenarios und Entwicklung erster Prototypen

Anschließend zur Definition des Risikos müssen weitere Eckpfeiler des Szenarios festgelegt und dokumentiert werden, etwa Ziel, Zweck und Nutzen dieser Analyse. Der Typ des Szenarios wird fixiert, idealerweise gab es dazu schon vorher Überlegungen, siehe 3.4.2.

Danach folgt die Entwicklung erster Szenario-Prototypen: Hier ist es entscheidend, die

Wiederkehrperiode und Stärke des Ereignisses abzuwägen. Ebenfalls werden die Folgen des Auslösers bei jedem Kandidaten etwas verändert, was zu mehreren Varianten von Szenarien führt. Aus diesem Ereignis-Pool wählt der Aktuar/Risikomanager dann eine Teilmenge aus, die ihm für die weitere Beobachtung sinnvoll erscheint.

Schritte 5 & 6: Entwicklung eines Narrativs und Erhebung der Auswirkungen

Darauffolgend wird eine Geschichte um das Szenario gebaut, um die einzelnen Folgen argumentieren und einen Bezug zur Realität herstellen zu können. Prinzipiell geht es dabei darum, was das Szenario auslöst, wo und wann es stattfindet, wie das Szenario sich entwickelt, welche Parteien wie schwer davon betroffen sind und wie das Szenario sein Ende findet. Danach können die verschiedenen Parameter entsprechend verändert werden, um weitere Blickwinkel auf mögliche Verläufe zu erlangen.

An nächster Stelle steht das Erheben aller möglicher Auswirkungen, die direkt als auch indirekt in den Scope des Versicherers fallen. Ein Erdbeben etwa kann in weiterer Folge einen Tsunami auslösen, der wiederum andere Katastrophenszenarien zur Folge hat. Auch auf mögliche Wechselwirkungen und systemische Abhängigkeiten ist hier zu achten.

Schritte 7 & 8: Präsentation zur Entscheidungsfindung und Aktualisierung

Um die Effektivität und Wirkung der Entwicklung zu fördern, ist eine klare und einfache Darstellung der Analyse und ihrer Ergebnisse nötig. Das Szenario soll eventuell einen Denkanstoß für Entscheidungsträger liefern, also ist es auch so zu präsentieren. Besonders das Motiv der Szenarioanalyse ist anzugeben, damit man ihre Ergebnisse entsprechend interpretieren kann.

Zuletzt steht die Evaluierung des Prozesses an: Wurde die Forschungsfrage erfüllt? Kann man irgendwo das Szenario noch nachfeilen? Dient die Analyse auch wirklich dem Zweck, für den sie gedacht ist? Da die Risikolandschaft und auch der eigene Bestand sich stetig verändern, müssen Anforderungen, Verläufe und Daten periodisch aktualisiert werden, um die Aussagekraft der Szenarioanalyse laufend zu gewährleisten[26].

[26] Vgl. [Jud20, S.35]

4 Modellierung eines Blackout-Szenarios in der VIG

Im letzten Abschnitt dieser Arbeit beschäftigen wir uns mit der Implementierung eines Blackout-Szenarios in der VIG, sowie verschiedenen Weiterentwicklungsmöglichkeiten. Aufgrund des Datenschutzes wird dieses als generelles Konzept für europäische multinationale Versicherungskonzerne technisch beschrieben. Nach einer initialen Entwicklung gemäß der in Kapitel 3 vorgestellten Schritte und dem Beleuchten der entsprechenden Datenlage werden die mathematische Implementierung sowie etwaige Optionen zur Verbesserung der Modellgüte besprochen.

Folgende Analysen basieren auf Überlegungen des Enterprise Risk Managements der VIG. Besonders ein europaweites Event ist für sie von größter Relevanz hinsichtlich des Quantifizierens von Kumulrisiken.

Sowohl angenommene Ausmaße, betroffene Länder und alle weiteren Basiszahlen sind frei erfunden. Sie bewegen sich von der Größenordnung her jedoch im Rahmen des Möglichen. Will man also als Versicherer plausible Ergebnisse aus der Analyse erhalten, so sind hier jeweils eigene Daten einzusetzen.

4.1 Ansatz und Narrativ

Die Überlegungen zur Implementierung eines Blackout-Szenarios begannen in der VIG bereits im Jahr 2018. Ziel war es, den versicherungstechnischen Schaden bezüglich Cyberangriffe im Worst Case abzuschätzen. Durch qualitative Untersuchungen wurde das Blackout als das für einen Versicherer schädlichste Szenario bestimmt: Hier wären alle Versicherungsnehmer direkt bzw. indirekt getroffen, und das in einer unvergleichbar großen Bandbreite von Schäden.

Arbeiten wir das angedachte Modell nun nach den Prozessthemen der Szenariomodellierung aus 3.4.3 auf:

Risikoselektion und Recherche

Die zugrundeliegende Forschungsfrage der Analyse beschäftigt sich damit, welcher versicherungstechnische Schaden für einen Versicherungskonzern im Falle eines hackerinduzierten Blackouts in Europa im Worst Case auftreten kann. Genauer sind die Schäden zu beobachten, welche die einzelnen Tochterunternehmen in Zentral- und Osteuropa in sowohl dem Bestand des Zivil-, als auch des Firmen- und Industriegeschäfts erfahren. Die betroffenen Versicherungsunternehmen (Namen in Klammern) operieren nach Annahme in

- Österreich (Versicherung AT1),
- der Tschechischen Republik (Versicherung CZ1, Versicherung CZ2, Versicherung CZ3)
- Polen (Versicherung PL1)
- Ungarn (Versicherung HU1, Versicherung HU2)
- Slowakei (Versicherung SK1)
- Rumänien (Versicherung RO1)

Zusätzlich wurden mittels Internetrecherche und Austausch mit verschiedensten Experten weitere Blickwinkel auf das Szenario erarbeitet, etwa durch [Pet11] oder [Pre18]. Auch erste Überlegungen hinsichtlich der Länge des Blackouts fanden hier statt. Der Zeitraum von einer Woche entwickelte sich hier als realistische Kenngröße, was sich mit den Analysen dieser und anderer Arbeiten deckt[1].

Abgrenzung des Szenarios und Prototypenentwicklung

In der Szenarioabgrenzung wurden Ziel, Zweck und Nutzen der Analyse implizit definiert. Das gesamte Unterfangen soll hier den Entscheidungsträgern in der VIG und den Tochterunternehmen dienen, das eigene Bewusstsein hinsichtlich Kumulrisiken im Silent Cyber Bereich zu stärken. Genauer wird dem Schadenpotential eines Blackouts hier zum ersten Mal eine Zahl zugeordnet, um die Dimension des Risikos besser verstehen zu können. Es soll hier also ein

- explorativ**es**,
- deterministisch**es**,
- von Experten vorangetrieben**es**

[1] Vgl. dazu etwa [Gra21] oder [Cam15]

- Schock-Szenario

analysiert werden.

Das Gesamtszenario besteht im behandelten Fall aus mehreren Einzelszenarien. Weiter präzisiert wurde das Gesamtszenario dahingehend, dass das Blackout im Winter bei Tiefsttemperaturen von -10 Grad Celsius passiert, und eine Woche dauert. Hier wurden jeweils gesondert eine Folge des Blackouts und die dahingehenden Auswirkungen auf einzelne Versicherungssparten betrachtet. Diese betreffen etwa

- Lastspitzen und plötzlicher Stromausfall: Dadurch könnten besonders hoch versicherte Maschinen oder andere Elemente der Wertschöpfungskette eines Unternehmens zerstört werden. Infolgedessen kann es ebenso zum Ausbruch eines Feuers kommen, was in Summe zu mehreren Großschäden führt.
- Versorgungsmangel und eingeschränkte Sicherheit: Entstehende Unruhen sowie die Knappheit an Nahrungsmitteln und Treibstoff haben mehrere Auswirkungen. Es wird bspw. angenommen, dass es bei Kraftfahrzeugen vermehrt zu Einbrüchen und Benzindiebstahl kommt. Das unsachgemäße Heizen mit Holz, Gaslampen etc. führt zu Brandschäden und Explosionen. Auch das Ausmaß dieser Schäden wird größer als "normal" eingeschätzt, da Notrufnummern nur bedingt bis gar nicht funktionieren. Einbrüche in Supermärkte, Trafiken und Zweitwohnsitze nehmen zu, um an Nahrungsmittel zu gelangen.

Die genauen Überlegungen und Annahmen hinsichtlich Schadenfrequenz sowie -höhe werden in einem späteren Abschnitt behandelt.

Abstufungen des Szenarios bezüglich Länge und geografischer Intensität wurden vorerst nicht unternommen. Ansätze hierzu werden in dieser Arbeit gesondert eruiert.

Entwicklung eines Narrativs, Auswertung, Präsentation und laufende Evaluierung

Ein "schulbuchmäßiges" Narrativ, so wie in dieser Arbeit an verschiedenen Stellen ausführlich beschrieben, wurde seitens der VIG leicht modifiziert entwickelt: Dies geschah nämlich parallel mit der Entwicklung der Einzelszenarien. Was hier jedoch deutlich fehlt, ist eine Beschreibung des Recovery-Prozesses der Infrastruktur (z.B. wann wieviele Haushalte wieder an das Netz angeschlossen werden); Hier ist Bedarf für eine Überarbeitung der Schadenannahmen während der zweiten Hälfte des einwöchigen Blackouts gegeben.

Die laufende Evaluierung findet bei der VIG derzeit jährlich statt, zuletzt im Oktober 2021.

Die Auswertung des Szenarios selbst wird qualitativ als auch quantitativ in den folgenden Abschnitten beschrieben:

4.2 Datenlage und -erhebung

Die Berechnung des Schadens im Eigenbehalt erfolgt einerseits mithilfe verschiedener Annahmen und andererseits mittels Datenerhebungen bei den betroffenen Versicherungsunternehmen. Um Letztere geht es in diesem Abschnitt: die für dieses Modell der Gesamtschadensberechnung notwendigen Daten gliedern sich grob in vier Typen, welche kurz beleuchtet werden.

4.2.1 Bestandsdaten

Von den zu untersuchenden Versicherungsunternehmen wird für das Blackout-Szenario jedes Jahr die Anzahl der versicherten Risiken zum Jahresletzten in verschiedenen Sparten benötigt. Dies kann beispielsweise im Zuge des Solvency II-Reportingprozesses stattfinden: Bei der SCR-Berechnung sind nämlich ebenfalls detaillierte Kenntnisse über den eigenen Versicherungsbestand erforderlich.

Vor der Verwendung der Daten sind grundlegende Fragen bezüglich versicherungstechnischer Definitionen zu klären: Etwa die jeweils nationale Einschätzung, was denn nun ein "versichertes Risiko" darstellt: Zum Beispiel kann beim österreichischen Versicherer ein KFZ in der Kaskoversicherung für ein versichertes Objekt stehen. Beim ungarischen Pendant wiederum könnte jedes einzelne Teil eines Autos (Windschutzscheibe, Reifen, Karosserie etc.) als eigenes versichertes Objekt zählen. Nationale Besonderheiten können das Ergebnis ungemein verfälschen, wenn sie nicht ordentlich erkannt und aufgearbeitet werden.

In der aktuellen Datenanforderung der VIG aus dem August 2021 wurde das "versicherungstechnische Risiko" von den betrachteten Versicherungsunternehmen standardisiert abgefragt, um die Portfoliodaten homogener zu gestalten, unter anderem in folgenden Sparten:

- KFZ-Kaskoversicherung: Anzahl der versicherten Fahrzeuge. Flotten sollen nach Möglichkeit in einzelne KFZ zerlegt werden.
- Haushaltsversicherung: Anzahl an einzelnen versicherten Häusern und Wohnungen. Ein Wohngebäude mit 20 Appartements sollte also in den Daten 20 Risiken wiederspiegeln.
- Einkommens-Ausfallversicherung: Anzahl an ausgegebenen Versicherungspolizzen. Sowohl Polizzen lautend auf Familien als auch auf Einzelpersonen bedeuten jeweils ein Risiko.

Um die gelieferten Zahlen vor der Weiterverarbeitung zu plausibilisieren, werden ebenso jährlich die Marktvolumina und -anteile der betrachteten Länder herangezogen. Aufgrund der vielen involvierten Unternehmen und Parteien sowie der heterogenen Datenbasis ist die Beschaffung der jährlichen Portfoliodaten laut Experten des VIG Enterprise Risk Managements der komplizierteste Teil der Datenerhebung.

4.2.2 Schadendaten

Um höchste Datenqualität und Plausibilität des Gesamtschadens zu gewährleisten, verwenden wir für die Schadenhöhen- und -frequenzschätzung nur das Rendement von *Versicherung AT1*. Diese werden in der Szenarioanalyse für die vorangegangenen 10 Jahre benötigt, um einen Durchschnittsschaden je betroffener Sparte für die Normalschäden zu bestimmen, sowie um eine entsprechende Abschätzung für Frequenz und Ausmaß potentieller Großschäden vorzunehmen.

Sind die Daten für eine andere Versicherungsgruppe über mehrere Länder hin homogen und miteinander vergleichbar, so können diese Kennzahlen auch je Land oder Unternehmen ermittelt werden.

4.2.3 Informationen über Rückversicherungsverträge

Zur Umrechnung des Brutto-Gesamtschadens auf den Netto-Gesamtschaden sind pro Sparte und betroffenem Land die jeweils gültigen Rückversicherungsstrategien zu erheben. Die verwendeten Absicherungskonstrukte folgen in der Praxis drei prinzipiellen Formen, welche im Folgenden anhand von anschaulichen Beispielen kurz erklärt werden:

Summenexzedenten-Verträge

Die erste Rückversicherungsart fällt in die Gruppe der *proportionalen Rückversicherungsverträge*. Bei Summenexzedenten-Verträgen (englisch: Surplus Treaty) gibt es eine Risikoteilung anhand der Versicherungssumme. Der Erstversicherer legt hier einen Selbstbehalt fest, bis zu dem er haften will. Der Rückversicherer haftet dann für den dieses Maximum übersteigenden Teil der Versicherungssumme bis zu einer Haftungsgrenze, die meist ein ganzzahliges Vielfaches des Selbstbehaltes darstellt. Das Verhältnis des Selbstbehalts (plus eventuellem Überschuss über der Haftungsgrenze) zur tatsächlichen Versicherungssumme des Risikos entspricht dann der Quote, zu der der Erstversicherer sowohl Prämien erhält als auch Schäden zahlt. Genauer ist die Quote α, zu der der Rückversicherer das Risiko übernimmt:

$$\alpha = \frac{VS - SBH - \max(VS - HG, 0)}{VS}$$

mit VS gleich der Versicherungssumme, SBH gleich dem Selbstbehalt sowie HG gleich der Haftungsgrenze. Nun ein anschauliches Anwendungsbeispiel mit zwei rückversicherten Gebäuden:

Bezeichnung	**Wert**
Erstversicherer: Rückversicherer:	*ABC Versicherung AG* *XYZ Rück AG*
Selbstbehalt: Haftungsgrenze:	100.000 EUR 1.000.000 EUR
Wert Gebäude 1: Ergibt Anteil, zu dem der RV das Risiko übernimmt:	500.000 EUR $\frac{500.000-100.000+0}{500.000} = 80\%$
Wert Gebäude 2: Ergibt Anteil, zu dem der RV das Risiko übernimmt:	1.100.000 EUR $\frac{1.100.000-100.000-100.000}{1.100.000} \approx 82\%$

Tabelle 4.1: Rechenbeispiel zur Summenexzedenten-Versicherung

Excess of Loss-Verträge

Weiters finden sich in der Rückversicherungspolitik der VIG-Töchter nicht-proportionale Schadenexzedenten-Verträge (englisch: Excess of Loss, kurz *XL*). Hierbei werden weitere Untertypen daran unterschieden, wie genau der *Schaden* für den Erstversicherer definiert ist: Auf Einzelschadenbasis spricht man hier von einem "klassischen" XL-Vertrag. Ist die Deckung an den Eintritt einer bspw. Naturkatastrophe gebunden, nennt man den Vertrag einen *Cat-XL*-Vertrag. Wird der Gesamtschaden einer oder mehrerer Versicherungssparten als Berechnungsbasis herangezogen, spricht man vom *Aggregate-XL*-Vertrag respektive von einem *Multiline-Aggregate-XL*.

Bei Schadenexzedenten-Verträgen übernimmt der Rückversicherer ab einem Selbstbehalt den Schaden des Erstversicherers entlang einer Haftungsstrecke. Diese können, zusätzlich zu der in der Lehre verwendeten "Selbstbehalt-Haftungsstrecke"-Aufteilung in verschiedene Ebenen, sogenannte *Layer*, unterteilt werden. Dies ist in folgender Tabelle beispielhaft illustriert:

Bezeichnung und deckende Partei	Schadenhöhenintervall in EUR
Überhalb der Haftungsgrenze: Erstversicherer	$(500.000; +\infty)$
Layer 2: Rückversicherer	$(300.000; 500.000]$
Layer 1: Rückversicherer	$(100.000; 300.000]$
Unterhalb des SBH: Erstversicherer	$(0; 100.000]$

Tabelle 4.2: Illustration einer Schadenexzedenten-Versicherung

Fällt nun ein Schaden in eine der Ebenen, etwa im oberen Fall ein Großschaden in der Höhe von 400.000 Euro, so gelten Layer 1 und der 400.000 Euro nicht übersteigende Teil von Layer 2 als "verbraucht". Hier besteht im nächsten Schadenfall prinzipiell keine Deckung. Der Erstversicherer hat jedoch die Möglichkeit, mittels *Reinstatement*-Zahlungen diese Layer wieder aufzufüllen (wobei die Anzahl der zulässigen Reinstatements begrenzt sein kann). Die Höhe dieser Auffüllungsprämien setzt sich in der Praxis aus einem Layer-spezifischen Prozentsatz multipliziert mit der Breite des Intervalls zusammen; Zusätzlich kann der Rückversicherer die ersten x Reinstatements bereits in der intialen Prämie berücksichtigen, welche im Falle des Falles automatisch geschehen und für den Erstversicherer dann kostenfrei sind.

In unserem Szenario findet sich im Falle klassischer Schadenexzedenten ein solcher Ebenen-Aufbau wieder. Im Falle der Aggregate-Schadenexzedenten nehmen wir an, die Verträge der Tochterunternehmen seien mit klassischen Selbstbehalten und Haftungsstrecken gestaltet. Hier findet auch bei der Abrechnung auf Basis eines Gesamtschadens das Ebenen-System keine Anwendung, da immer nur "ein" Schaden betrachtet wird.

In der Rückversicherungsbranche gibt es zudem unzählige komplexere Vertragskonstruktionen, die jedoch außerhalb des Scopes dieser Arbeit liegen. Für eine vertiefende Auseinandersetzung mit der Thematik wird [Ger18] empfohlen.

Quoten-Rückversicherung

Die letzte Rückversicherungsart findet im Falle dieses Blackout-Szenarios keine Anwendung. Prinzipiell besteht die Quoten-Rückversicherung in einer Prämien- und Schadenaufteilung in gleichen Verhältnissen zwischen Erst- und Rückversicherer. Dieser Typ fällt damit auch in die Gruppe der proportionalen Rückversicherungen und findet etwa im klassischen Cybergeschäft der Wiener Städtischen Anwendung.

4.2.4 Zusätzliche Daten

Weiters müssen die zu analysierenden Schäden in zwei Richtungen angepasst werden: Einerseits in Richtung der Zeit, etwa durch die Inflation. Diese wird in der Analyse vom

österreichischen Verbraucherpreisindex beziffert. Hinzu kommt in einzelnen Sparten beispielsweise der Baukostenindex für den Wohnhaus- und Siedlungsbau sowie der KFZ-Sachschaden-Kostenindex, entlang derer entsprechend skaliert werden muss. Die einzelnen Indizes beziehen wir für dieses Szenario von der *Statistik Austria*[2], ebenfalls nehmen wir an, dass diese Indexentwicklungen in etwa auf ganz Europa übertragen werden können.

Andererseits müssen die Durchschnittsschadenhöhen der Normalschäden und die Großschäden an die wirtschaftlichen Verhältnisse der anderen Länder angepasst werden: Bei Fremdwährungen benötigt man hier gegebenenfalls stichtagsbezogene Devisenkurse (in unserem Fall die des 31.12.2020). Zusätzlich ist eine Kaufkraftanpassung mittels der *Purchasing Power Parity*, kurz *PPP*, vorzunehmen. Diese Daten sind öffentlich von der Homepage des europäischen Statistikamts, *Eurostat*, abrufbar[3].

4.3 Betroffene Versicherungssparten

Wir nehmen im Blackout-Szenario an, dass sowohl Sparten im Privat- als auch im Firmen- und Gewerbegeschäft betroffen sind. Die Geschäftszweige, die hier im Fokus liegen, wurden parallel zur Prototypenentwicklung festgelegt, und folgen auch aus diesen Überlegungen. Beispielhaft nehmen wir an, dass in folgenden Branchen valide, homogene Daten vorliegen:

KFZ-Kaskoversicherung

Im KFZ-Bereich wird im Falle des Blackouts besonders die Kaskoversicherung betroffen sein. Ursachen hierfür liegen in den Einzelszenarien, die als Folgen von Chaos und möglichen Unruhen Einbruchdiebstahl, Benzindiebstahl oder Vandalismus aufweisen.

Transportversicherung

Auch Firmen und die Industrie können von Diebstahl betroffen sein. Vor allem im Transport- und Logistikwesen liegt hier ein Kumulrisiko vor. Zusätzlich würden verderbliche Güter durch fehlende Infrastruktur irgendwann ungenießbar werden (im Sommer wäre dieses Zusatzrisiko natürlich weitaus höher, es ist im Winter jedoch auch gegeben).

Feuer- (Zivil) und Haushaltsversicherung

Besonders im Winter werden durch ein Blackout zunehmend Feuer aufgrund behelfsmäßiger Heizmethoden erwartet. Da die Menschen daheim sind, umfasst dies nur den zivilen

[2] Vgl. [Ind21a], [Ind21d] als auch [Ind21c]
[3] [Ind21b]

Bereich der Feuerversicherung. Weiters kann es zu Gasexplosionen kommen. Dazu kommt mit Einbrüchen in private Haushalte eine zusätzliche Gefahr für diese, meist in Bündeln mit Haushaltsversicherungen verkauften, Produkte.

Feuer- (Industrie) und Betriebsunterbrechungsversicherung

Im gewerblichen Bestand werden sowohl Normal- als auch beträchtliche Großschäden erwartet. Diese können aufgrund von (elektronischem) Maschinenbruch, Betriebsunterbrechung oder Überspannungsschäden an der internen IT-Struktur entstehen.

Einbruch-/Diebstahlversicherung

Abseits der Haushalts- und Transportversicherung ist natürlich auch eine Vielzahl an Einbruch-/Diebstahlschäden im Handel, Finanzinstituten oder bspw. bei Tankstellen zu erwarten. Auch Vandalismus zählt hier meist zu den gedeckten Risiken, was eine weitere Kumulgefahr darstellt.

Leitungswasserversicherung

Im Winter wird eine Vielzahl an Wasserleitungen bersten, sei dies bei Versorgern, Betrieben oder in Privathaushalten. Die angenommenen Tiefsttemperaturen erhöhen dabei das Schadenpotential ungemein.

Allgemeine Haftpflichtversicherung

Nach Wiederherstellung der "Normalität" ist mit einer vermehrten Geltendmachung von Ansprüchen, etwa gegenüber Stromanbietern, zu rechnen.

Rechtsschutzversicherung

Unter anderem obigem Haftpflicht-Kumul zur Folge wird die Sparte der Rechtsschutzversicherung mit einer erhöhten Anzahl an Schäden konfrontiert sein.

Aus obigen Versicherungssparten wurden 17 Einzelszenarien generiert, auf deren Basis der Gesamtschaden berechnet wird:

4.4 Methodik

Im Folgenden wird das Herzstück der Szenariomodellierung beschrieben: Die Methodik, mithilfe derer die Input-Daten mit Rückversicherungs- und Schadenannahmen zu einem Netto-Gesamtschaden für die gesamte Gruppe verarbeitet werden. Ein solches Tool in Form

einer Microsoft Excel-Datei besteht innerhalb der VIG, besitzt jedoch kleinere Fehler und Abschnitte mit vertraulichen Passagen. Dies wurde zum Anlass genommen, ein von der Idee her ähnliches, jedoch verallgemeinertes Tool für eine beliebige europäische Versicherungsgruppe in Microsoft Excel komplett neu zu erstellen. In diesem Kapitel wird der Aufbau des Modells, die dazugehörigen Annahmen sowie die dahinterliegende Mathematik ausführlich erklärt. Ausschnitte aus der Datei selbst werden in dieser Arbeit verwendet, das gesamte Modell ist im Anhang verlinkt.

4.4.1 Aufbau

Die Excel-Datei ist in 4 Tabellenblätter aufgeteilt, welche wir nach ihrer Reihenfolge im Modellierungsablauf betrachten wollen:

Blatt "Einführung"

Im ersten Tabellenblatt wird ein Überblick über das Tool gegeben, sowie die Beschreibung des Szenarios und betroffener Sparten analog zur zugrundeliegenden Arbeit vorgenommen. Weiters sind hier Erstellungs- und das letzte Bearbeitungsdatum vermerkt.

Blatt "Einzelszenarien-Annahmen"

Hier werden die Einzelszenarien genannt sowie die Schätzungsmethoden und Ergebnisse eingetragen. Input-Werte, wie die angenommene Frequenz und Durchschnittsschadenhöhe, sind in der Datei konsistent lachsrosa eingefärbt. Ein Auszug dieses Blattes findet sich in 4.4.2.

Blatt "Hauptberechnung"

Im Blatt "Hauptberechnung" müssen vom Versicherungsunternehmen die Portfoliodaten der Tochterunternehmen in den betroffenen Sparten in den Zeilen 5 bis 13 eingetragen werden. Außerdem finden sich in den Spalten "O" bis "AA" die in 4.2.4 geforderten Indexwerte. Danach berechnet sich in den Zeilen 42 bis 244 je Einzelszenario und Tochterunternehmen ein Bruttoschaden, welcher gesammelt in den Zeilen 21 bis 39 dargestellt wird.

Blatt "Rückversicherungsberechnung"

Ebenfalls nach Einzelszenario und in weiterer Folge nach Tochterunternehmen aufgeteilt ist die darauf folgende Berechnung des Rückversicherungsanteils im entsprechend benannten

Tabellenblatt. Als Input werden Durchschnittsschaden und Schadenanzahl benötigt. Weiters sind je Tochterunternehmen die durchschnittliche Abgabequote der Summenexzedenten-Verträge, die Layers und Reinstatements der klassischen XL-Vereinbarungen sowie die Haftungsgrenzen eines eventuellen Aggregated XL im Extremfall anzugeben. Die Berechnung liefert in Spalte "R" den rückversicherten Schaden in Euro, welcher wieder im Blatt "Hauptberechnung" in den je Block letzten Spalten für die Nettoschadensberechnung benötigt wird.

Illustrationen sowie die mathematische Beschreibung der jeweiligen Berechnungsverfahren folgen in den nächsten Absätzen:

4.4.2 Annahmen zu Schadenfrequenz und -höhe

Wir nehmen in dieser Arbeit an, dass zum Zeitpunkt der Analyse keine eigene Szenario-Frequenzschätzung aufgrund mangelnder Datenmengen möglich ist. Mittels Expert Judgement und den "üblichen" Frequenzen im eigenen Bestand als Anhaltspunkte kann man sich hier jedoch Abhilfe verschaffen. Die zu verwendenden Schadenfrequenzen und -höhen muss in jedem Fall jedes Versicherungsunternehmen, jeder Anwender für sich selbst festlegen. Diese Arbeit liefert hier zwar nur Beispieldaten, diese bewegen sich jedoch in einer plausiblen Größenordnung.

Die Annahmen zu Schadenfrequenz und -höhe werden im Excel-Tool großteils über die Rendementdaten des (fiktiven) österreichischen Tochterunternehmens der letzten 10 Jahre geschätzt. Die angenommene Frequenz wird dann als relativer Anteil an der regulären Schadenhäufigkeit angesetzt; Dieser Prozentsatz wird von aktuariellen Experten geschätzt. So bedeuten etwa "50% der Jahresfrequenz", dass allein im Rahmen des Blackouts die Hälfte der normalerweise in einem Jahr beobachteten Schäden erwartet werden.

So geschieht dies auch in der Praxis bei der VIG. In 6 Fällen kommt eine grundlegende Einschätzung durch Expert Judgement zum Einsatz, sei dies aufgrund unzureichender Datenqualität oder (wie z.B. bei der Leitungswasserversicherung aufgrund flächendeckender Heizungausfälle) aus der Unvergleichbarkeit der Schockszenario-Frequenz zur regulären Schadenfrequenz aus dem Bestand. Die Schadenhöhe berechnet sich ebenfalls aus dem Durchschnittsschaden der letzten 10 Jahre. Diese Zahlen sind pro Jahr jedoch mittels in 4.2.4 genannter Indizes zum 31.12.2020 anzupassen, weshalb die Indexwerte aus Transparenzgründen in der Berechnungsdatei angegeben werden sollten.

Weiters nehmen wir an, dass für die Allrisikoversicherung keine verlässliche Anlieferung von Portfoliodaten möglich ist, weshalb hier bei der Anzahl der Schäden eine manuelle Eingabe im Hauptberechnungs-Blatt vonnöten ist.

Die folgende Tabelle zeigt die angenommenen Schadenfrequenzen (in Prozent), Durchschnittsschadenhöhen in Euro sowie die angenommenen Berechnungsgrundlagen:

Name Einzelszenario	Frequenz: Schätzung basierend auf AT1	Wert mit 31.12.2020 in EUR	Durchschnittsschaden: Schätzung basierend auf AT1	Wert mit 31.12.2020 in EUR
KFZ-Kasko: Einbruchdiebstahl/Benzindiebstahl	1/2 der regulären Jahresfrequenz im 10-Jahres-Schnitt	0,60%	Durchschnittsschaden der letzten 10 Jahre	700
KFZ-Kasko: Fahrzeugdiebstahl	1/2 der regulären Jahresfrequenz im 10-Jahres-Schnitt	0,07%	Durchschnittsschaden der letzten 10 Jahre	8 000
KFZ-Kasko: Vandalismus	1/2 der regulären Jahresfrequenz im 10-Jahres-Schnitt	0,28%	Durchschnittsschaden der letzten 10 Jahre	1 100
Transportversicherung: Diebstahl	1/3 der regulären Jahresfrequenz im 10-Jahres-Schnitt	4%	Durchschnittsschaden der letzten 10 Jahre	7 500
Transportversicherung: Verderb von Gütern	Reguläre Jahresfrequenz im 10-Jahres-Schnitt	1,10%	Durchschnittsschaden der letzten 10 Jahre	3 200
Feuer- und Haushaltsversicherung: Feuerschäden	Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,10%	Durchschnittsschaden der letzten 10 Jahre	26 000
Feuer- und Haushaltsversicherung: Gasexplosionen	Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,003%	Durchschnittsschaden der letzten 10 Jahre	54 000
Haushaltsversicherung: Einbruchdiebstahl	Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,18%	Durchschnittsschaden der letzten 10 Jahre	2 900
Haushaltsversicherung: Überspannung	Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,14%	Durchschnittsschaden der letzten 10 Jahre	850
Einbruchdiebstahl Firmengeschäft	Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,50%	Durchschnittsschaden der letzten 10 Jahre	16 500
Leitungswasserversicherung: Frostschäden	Expert Judgement	0,90%	Expert Judgement	3 500
Allrisiko-Versicherung: Normalschäden	Frequenz des schlechtesten der letzten 10 Jahre	Manuelle Eingabe	Durchschnittsschaden der letzten 10 Jahre	60 000
Allrisiko-Versicherung: Großschäden	Expert Judgement	Manuelle Eingabe	Expert Judgement	750 000
Allgemeine Haftpflicht: Normalschäden	Expert Judgement	0,08%	Expert Judgement	400 000
Allgemeine Haftpflicht: Großschäden	Expert Judgement	0,03%	Expert Judgement	8 000 000
Rechtsschutzversicherung	Expert Judgement	0,06%	Expert Judgement	14 000
Einkommensausfallversicherung	Expert Judgement	0,04%	Expert Judgement	20 000

Quelle: Eigene Excel-Berechnung

Abbildung 4.1: Annahmen bezüglich Schadenfrequenzen und -höhen

In obiger Tabelle sind jeweils aktuelle Werte einzutragen.

Normalschaden vs. Großschaden

Wie schon in 4.1 zu sehen ist, unterteilen wir einige verwendete Szenarien in Normalschaden- und Großschaden-Szenarien. Dieser Ansatz ist in großschadenlastigen Sparten auch im Zuge der Bewertung gemäß Solvency II üblich, da zumeist keine Verteilung existiert, mit der sich gleichzeitig Normal- und Großschäden angemessen modellieren lassen. Ab welcher Schadenhöhe ein Versicherungsfall als Großschaden deklariert wird, kann je nach Versicherungsgruppe und Rendement unterschiedlich sein[4]. Die Grenze kann technisch (als optimale Grenze, bei der beide Schadenhöhenverteilungen bestmöglich durch zwei Verteilungsfunktionen approximiert werden können) oder auch fachlich festgelegt werden (etwa die Grenze, ab der eine Schadenfallkündigung eingeleitet wird). Auch in der Rückversicherung wird oft eine Unterteilung in Normal- und Großschäden durchgeführt, um explizit nur einen Teil dieser Schäden zu decken.

In dieser Arbeit werden beispielhaft folgende Grenzen für die Klassifikation gewählt:

- Allrisiko-Versicherung: 250.000 EUR
- Allgemeine Haftpflichtversicherung: 1.000.000 EUR

4.4.3 Annahmen zur Rückversicherung

Die Rückversicherungsberechnung folgt in unserem Beispiel vielerlei Annahmen; Eine weitere Generalisierung des Modells bezüglich der Nettoschadensberechnung, um bessere Ergebnisse zu erhalten, wird als Weiterentwicklungsvorschlag im entsprechenden Kapitel genannt.

Dadurch, dass bei den Einzelszenarien ausschließlich Durchschnittsschäden und Schadenhäufigkeiten anzugeben sind, muss für die Berechnung der Rückversicherungsbeteiligung angenommen werden, jeder berücksichtigte Schaden hätte genau die Höhe des Durchschnittsschadens. Dies verzerrt den Rückversicherungsanteil insbesondere bei einzelschadenbasierten Excess of Loss-Verträgen, ist jedoch mit dem explorativen Ziel der Analyse durchaus vereinbar.

Weiters nehmen wir an, dass die klassischen Schadenexzedenten-Vereinbarungen über zwei Layer verfügen. Die Methodik dahinter ist jedoch flexibel für ein beliebiges $n \in \mathbb{N}$ als Anzahl der Layer anwendbar und einfach zu erweitern.

Ein letzter hier zu erwähnender Punkt liegt in der Rangfolge der Rückversicherungskontrakte: Wir nehmen an, dass Zahlungen durch den Summenexzedenten-Vertrag zuerst vom

[4] Vgl. dazu etwa [Ngu08, S. 367ff.]

Bruttoschaden abgezogen werden; Danach folgt der klassische Schadenexzedenten-Vertrag. Zuletzt wird auf den verbleibenden Schaden im Eigenbehalt der Aggregated XL-Vertrag angewandt. Weist eine Versicherungsgruppe andere Rangfolgen in ihrer Rückversicherungsstruktur auf, so kann dies mittels Bilden von Zwischenergebnissen ebenso leicht angepasst werden.

4.4.4 Berechnung des Bruttoschadens

Der Gesamtschaden vor Rückversicherung B setzt sich aus den Bruttoschäden der 17 Einzelszenarien, aufgeteilt auf die 9 Tochterunternehmen zusammen. Notieren wir $\mathcal{S}$ für die Menge der Szenarien, und $\mathcal{T}$ für die Gesamtheit der Firmen, so kann der Gesamtschaden als

$$B = \sum_{i \in \mathcal{S}} \sum_{j \in \mathcal{T}} b_{i,j} \tag{4.1}$$

dargestellt werden, wobei $b_{i,j}$ den Bruttoschaden in Szenario i für Unternehmen j darstellt. In unserem Fall sind diese Zahlen Einträge von 17×9-Matrizen mit Werten in $\mathbb{R}^+$. Bezeichnen

- $r_{i,j}$ die Anzahl an Risiken,
- c_i den Durchschnittsschaden, der in Szenario i für die österreichische Tochter in Euro angegeben wurde,
- f_i die angenommene Frequenz für Szenario i,
- und PPP_j den Faktor, mittels dem der Schaden auf die Kaufkraft des betrachteten Landes von Unternehmen j skaliert wird,

so berechnet sich $b_{i,j}$ folgendermaßen:

$$b_{i,j} = r_{i,j} \cdot f_i \cdot c_i \cdot PPP_j \tag{4.2}$$

Berechnen wir dies beispielhaft für das 14. Szenario "Allgemeine Haftpflicht: Großschäden"[5]: Der Durchschnittsschaden c_{15} ist mit 8.000.000 Euro geschätzt. Die angenommene Frequenz wurde mittels Expert Judgement bestimmt und hat einen Wert von $0,03\%$. Die beispielhaft generierte Anzahl der Risiken in Form des Spaltenvektors $r_{15,j}$ nimmt folgende Werte an:

[5] Diese Berechnung ist beispielhaft und kann von den Ergebnissen im Excel-Tool aufgrund von Rundungsfehlern minimal abweichen.

j	Land	Anzahl $r_{i,j}$ an Haftpflichtrisiken
1	Versicherung AT1	113.429
2	Versicherung CZ1	19.067
3	Versicherung CZ2	51.169
4	Versicherung CZ3	84.854
5	Versicherung PL1	61.524
6	Versicherung HU1	29.738
7	Versicherung HU2	184.301
8	Versicherung SK1	185.505
9	Versicherung RO1	167.270

Quelle: Eigene Berechnung

Tabelle 4.3: Anzahl der Transportversicherungs-Risiken je Tochter

Dazu lauten die Kaufkraftfaktoren PPP_j wie folgt:

j	Bezeichnung Unternehmen	Indexstand	Wert PPP_j (Versicherung AT1=1)
1	Versicherung AT1	114,4	1
2	Versicherung CZ1	72,2	$\approx 0,63$
3	Versicherung CZ2	72,2	$\approx 0,63$
4	Versicherung CZ3	72,2	$\approx 0,63$
5	Versicherung PL1	58,5	$\approx 0,51$
6	Versicherung HU1	60,9	$\approx 0,53$
7	Versicherung HU2	60,9	$\approx 0,53$
8	Versicherung SK1	78,9	$\approx 0,69$
9	Versicherung RO1	52,7	$\approx 0,46$

Quelle: [Ind21b], eigene Berechnung

Tabelle 4.4: Kaufkraftparität 2020 der betroffenen Versicherungsunternehmen

Die kaufkraftangepassten Schäden sehen nun wie folgt aus:

j	Bezeichnung Unternehmen	$c_{15} \cdot PPP_j$
1	Versicherung AT1	8.000.000
2	Versicherung CZ1	5.048.951
3	Versicherung CZ2	5.048.951
4	Versicherung CZ3	5.048.951
5	Versicherung PL1	4.090.909
6	Versicherung HU1	4.258.741
7	Versicherung HU2	4.258.741
8	Versicherung SK1	5.517.483
9	Versicherung RO1	3.685.315

Quelle: [Ind21b], eigene Berechnung

Tabelle 4.5: Durchschnittsschäden kaufkraftangepasst für Szenario $i = 15$

Die Anzahl der Schäden ergibt sich aus dem Produkt der Anzahl der Risiken mit der angenommenen Schadenhäufigkeit[6]. Entsprechend obiger Formeln erhalten wir für den Bruttoschaden:

j	Bezeichnung Unternehmen	Anzahl an Schäden	Ergibt $b_{i,j}$ in EUR (gerundet)
1	Versicherung AT1	$113429 \cdot 0,03\% \approx 34$	272.229.600
2	Versicherung CZ1	$19067 \cdot 0,03\% \approx 6$	28.880.505
3	Versicherung CZ2	$51169 \cdot 0,03\% \approx 15$	77.504.933
4	Versicherung CZ3	$84854 \cdot 0,03\% \approx 25$	128.527.108
5	Versicherung PL1	$61524 \cdot 0,03\% \approx 18$	75.506.727
6	Versicherung HU1	$29738 \cdot 0,03\% \approx 9$	37.993.934
7	Versicherung HU2	$184301 \cdot 0,03\% \approx 55$	235.467.082
8	Versicherung SK1	$185505 \cdot 0,03\% \approx 56$	307.056.178
9	Versicherung RO1	$167270 \cdot 0,03\% \approx 50$	184.932.776

Quelle: Eigene Berechnung

Tabelle 4.6: Bruttoschaden für Einzelszenario $i = 15$

Für das Szenario "Allgemeine Haftpflicht: Großschäden" erhalten wir also insgesamt einen Bruttoschaden von 1.348.098.843 EUR.

4.4.5 Berechnung des Nettoschadens

Entsprechend der Annahmen in 4.4.3 ermitteln wir nun den rückversicherten Anteil des Bruttoschadens je Szenario und Unternehmen. Ausgang dieser Berechnung sind sowohl Durchschnittsschaden, Bruttoschaden sowie die Schadenanzahl aus den obigen Berechnungen. Diese entsprechen den Vorgängen im Tabellenblatt "Hauptberechnung".

[6] Minimale Unterschiede zu den Ergebnissen im Excel-Modell sind zu erwarten, da hier bspw. die Schadenanzahl gerundet wird

Zunächst benötigen wir Daten auf Einzelschadenbasis, also den angepassten Durchschnittsschaden $c_i \cdot PPP_j$. Auf diesen wird die durchschnittliche Abgabequote $s_{i,j}$ des Summenexzedenten-Vertrags angewandt, was zu einem verbleibenden Eigenbehalt pro Schaden von

$$x^1_{i,j} \coloneqq c_i \cdot PPP_j \cdot (1 - s_{i,j}) \tag{4.3}$$

führt.

In der Rangfolge als nächstes folgt der klassische XL-Vertrag, in diesem Fall mit zwei Layern. Trotzdem sei hier der Fall mit n Layern beschrieben, um einer Versicherung die leichte Anpassung ermöglichen zu können:

Nun benötigen wir zur Berechnung als Input die Anzahl der Schäden je Szenario und Unternehmen $r_{i,j} \cdot f_i$ Die Grenzen der Layer bezeichnen wir im Folgenden mit $l^k_{i,j}$ für die untere Grenze (für $k = 1$ den Selbstbehalt) des k-ten Layers respektive $u^k_{i,j}$ für die obere Haftungsgrenze für Unternehmen j in Szenario i; die Anzahl der möglichen Reinstatements sei mit $re^k_{i,j}$ gegeben. Damit berechnet sich der verbleibende (gesamte) Eigenbehalt $x^2_{i,j}$ folgendermaßen:

$$x^2_{i,j} \coloneqq (x^1_{i,j} \cdot r_{i,j} \cdot f_i) - (\sum_{k=1}^{n} \min(u^k_{i,j} - l^k_{i,j}, (x^1_{i,j} - l^k_{i,j})^+) \cdot \min(r_{i,j} \cdot f_i, re^k_{i,j})), \tag{4.4}$$

wobei jeder Summand in der Summe genau den Teil des Schadens im Eigenbehalt darstellt, welcher vom k-ten Layer gedeckt wird. Diese Deckungen sind jedoch gedeckelt mit der maximalen Anzahl an Reinstatements für diesen Layer.

Zuletzt wollen wir die Berücksichtigung des Aggregated XL-Vertrags mathematisch beschreiben. Dieser wirkt auf den Gesamtschaden und besitzt einen Selbstbehalt $l^{\text{agg}}_{i,j}$ sowie eine obere Haftungsgrenze $u^{\text{agg}}_{i,j}$. Der endgültige Nettoschaden $n_{i,j}$ für Versicherungsunternehmen j im Szenario i ergibt sich nun, ähnlich zum klassischen Schadenexzedenten-Vertrag, folgendermaßen:

$$n_{i,j} \coloneqq x^2_{i,j} - \min((x^2_{i,j} - l^{\text{agg}}_{i,j})^+, u^{\text{agg}}_{i,j} - l^{\text{agg}}_{i,j}) \tag{4.5}$$

Betrachten wir dies wieder an einem Beispiel, indem wir für das Szenario "Allgemeine Haftpflicht: Großschäden" aus dem zuvor berechneten Bruttoschaden den Nettoschaden ermitteln:

Die benötigten Inputdaten je Unternehmen für dieses Einzelszenario stehen in den Tabellen 4.5 und 4.6. Der verbleibende Eigenbehalt pro Schaden $x^1_{i,j}$ für $i = 15$ berechnet sich wie

folgt:

j	Bezeichnung Unternehmen	$c_{14} \cdot PPP_j$	$s_{i,j}$	Berechnung $x^1_{i,j}$
1	Versicherung AT1	8.000.000	15%	$8.000.000 \cdot 85\% = 6.800.000$
2	Versicherung CZ1	5.048.951	21%	$5.048.951 \cdot 79\% \approx 3.988.671$
3	Versicherung CZ2	5.048.951	18%	$5.048.951 \cdot 82\% \approx 4.140.140$
4	Versicherung CZ3	5.048.951	27%	$5.048.951 \cdot 73\% \approx 3.685.734$
5	Versicherung PL1	4.090.909	10%	$4.090.909 \cdot 90\% \approx 3.681.818$
6	Versicherung HU1	4.258.741	8%	$4.258.741 \cdot 92\% \approx 3.918.042$
7	Versicherung HU2	4.258.741	13%	$4.258.741 \cdot 87\% \approx 3.705.105$
8	Versicherung SK1	5.517.483	21%	$5.517.483 \cdot 79\% \approx 4.358.811$
9	Versicherung RO1	3.685.315	4%	$3.685.315 \cdot 96\% \approx 3.537.902$

Quelle: Eigene Berechnung

Tabelle 4.7: Berechnung des Summenexzedenten-Anteils in Szenario $i = 15$

Der Bruttoschaden nach Abzug des Schadenexzedenten, in unserem Fall mit $n = 2$ Layern, erfolgt analog zu 4.5. Folgend die Beschreibung der beiden Layer in zwei Tabellen:

j	Bezeichnung Unternehmen	$l^1_{i,j}$	$u^1_{i,j}$	$re^1_{i,j}$
1	Versicherung AT1	2.500.000	3.500.000	25
2	Versicherung CZ1	2.000.000	3.000.000	10
3	Versicherung CZ2	2.000.000	3.000.000	10
4	Versicherung CZ3	2.000.000	3.000.000	10
5	Versicherung PL1	1.000.000	1.500.000	8
6	Versicherung HU1	2.500.000	3.500.000	10
7	Versicherung HU2	2.500.000	3.500.000	10
8	Versicherung SK1	1.000.000	3.000.000	40
9	Versicherung RO1	500.000	2.000.000	35

Quelle: Eigene Berechnung

Tabelle 4.8: Beschreibung des ersten RV-Layers in Szenario $i = 15$

j	Bezeichnung Unternehmen	$l^2_{i,j}$	$u^2_{i,j}$	$re^2_{i,j}$
1	Versicherung AT1	3.500.000	6.000.000	25
2	Versicherung CZ1	-	-	-
3	Versicherung CZ2	-	-	-
4	Versicherung CZ3	-	-	-
5	Versicherung PL1	1.500.000	2.000.000	5
6	Versicherung HU1	2.500.000	3.500.000	6
7	Versicherung HU2	2.500.000	3.500.000	6
8	Versicherung SK1	3.000.000	5.000.000	30
9	Versicherung RO1	2.000.000	4.000.000	35

Quelle: Eigene Berechnung

Tabelle 4.9: Beschreibung des zweiten RV-Layers in Szenario $i = 15$

Die endgültige Berechnung des verbleibenden Schadens im Eigenbehalt $x^2_{i,j}$ ist beispielhaft in der nachstehenden Tabelle dargestellt:

j	Bezeichnung VU	Berechnung $x^2_{i,j}$
1	Versicherung AT1	$231.395.160 - (1.000.000 \cdot 25 + 2.500.000 \cdot 25) = 143.895.160$
2	Versicherung CZ1	$22.815.599 - (1.000.000 \cdot 6) = 16.815.599$
3	Versicherung CZ2	$63.554.045 - (1.000.000 \cdot 15) = 48.554.045$
4	Versicherung CZ3	$93.824.789 - (1.000.000 \cdot 25) = 68.824.789$
5	Versicherung PL1	$67.956.055 - (500.000 \cdot 8 + 500.000 \cdot 5) = 61.456.055$
6	Versicherung HU1	$34.954.420 - (1.000.000 \cdot 9) = 25.954.420$
7	Versicherung HU2	$204.856.361 - (1.000.000 \cdot 10 + 205.105 \cdot 6) = 193.625.731$
8	Versicherung SK1	$242.574.381 - (2.000.000 \cdot 40 + 1.358.811 \cdot 30) = 121.810.051$
9	Versicherung RO1	$177.535.456 - (1.500.000 \cdot 35 + 1.537.902 \cdot 35) = 71.208.895$

Quelle: Eigene Berechnung

Tabelle 4.10: Berechnung der Auswirkungen des klassischen XL in Szenario $i = 15$

Zu guter Letzt werden vom übrigen Gesamtschaden etwaige Aggregate-XL-Deckungen abgezogen, und wir erhalten den Nettoschaden $n_{i,j}$:

j	Bezeichnung VU	$l_{i,j}^{\text{agg}}$	$u_{i,j}^{\text{agg}}$	Ergibt $n_{i,j}$
1	Versicherung AT1	15.000.000	90.000.000	68.895.160
2	Versicherung CZ1	-	-	16.815.599
3	Versicherung CZ2	-	-	48.554.045
4	Versicherung CZ3	15.000.000	90.000.000	15.000.000
5	Versicherung PL1	10.000.000	50.000.000	21.456.055
6	Versicherung HU1	15.000.000	90.000.000	15.000.000
7	Versicherung HU2	30.000.000	150.000.000	73.625.731
8	Versicherung SK1	30.000.000	150.000.000	30.000.000
9	Versicherung RO1	25.000.000	100.000.000	25.000.000

Quelle: Eigene Berechnung

Tabelle 4.11: Berechnung der Auswirkungen des Aggregate-XL-Vertrags in Szenario $i = 15$

Damit erhalten wir einen Gesamt-Nettoschaden für "Allgemeine Haftpflicht: Großschäden" von 314.346.590 EUR. Unter Verwendung des entsprechenden Bruttoschadens ergibt sich ein Rückversicherungsanteil von etwa 77%. Da in der zugrundeliegenden Anwendung die Schadenzahlen nicht gerundet werden, ergibt sich hier ein geringfügig abweichender Nettoschaden von 314.275.790 EUR.

4.4.6 Ergebnisse

Aus dem gesamten Blackout-Szenario ergibt sich ein Bruttoschaden von etwa 1,74 Milliarden Euro, welcher sich nach Abziehen eines durchschnittlichen Rückversicherungsanteils von etwa 64% auf einen Eigenbehaltsschaden von ca. 634 Millionen Euro reduziert. Der Link zum zugrundeliegenden Modell ist im Anhang vorzufinden.

In dieser Arbeit wird von weiteren Analysen und grafischer Aufarbeitung der Ergebnisse abgesehen, da die Input-Zahlen rein fiktiv sind und damit keine Interpretationsbasis bieten.

4.5 Weiterentwicklungsmöglichkeiten

Nach Konzeption eines allgemeinen Frameworks für die deterministische Szenariomodellierung wollen wir nun einige Ideen zur Weiterentwicklung des Modells diskutieren und gegebenenfalls auch im Ansatz realisieren. Diese Möglichkeiten reichen von einfach zu realisierenden Erweiterungen bis hin zu komplett eigenen Bausteinen in der Modellierung, die einer eigenständigen Datenanforderung bedürfen:

4.5.1 Inklusion anderer Deckungen

Eine naheliegende Option besteht in der Inklusion weiterer Einzelszenarien und Versicherungssparten. In 3.3.2 wurden dabei etwa die KFZ-Haftpflicht-, die Geschäftsunterbrechungs- und die Krankenversicherung genannt. Hierzu müssten gesonderte Portfolio-, Schaden- und Deckungsanalysen durchgeführt werden, was jedoch mit einem realistischen Arbeitsaufwand seitens der Versicherungsgruppe und ihrer Tochterunternehmen erledigt werden kann. Besonders das eher selten rückversicherte, großvolumige Kranken- und Lebensversicherungsgeschäft bedarf in diesem Fall genauer Schätzungen und infolgedessen den Dialog mit Personenversicherungs-Aktuariaten innerhalb der Versicherungstöchter.

4.5.2 Verfeinerte Nettoschadensberechnung

Wie in 4.4.3 zu sehen ist, gehen mit der Rückversicherungsberechnung einige Annahmen einher. Eine dieser Einschränkungen beläuft sich auf die Verteilung der Schadenhöhen: Derzeit wird angenommen, dass jede Schadenhöhe genau dem angenommenen Durchschnittsschaden je Szenario entspricht.

In der VIG etwa werden jedes Jahr für die Parametrisierung von internen Risikotools die Schadendaten je Szenario einer Verteilungsschätzung unterzogen. Genau die Ergebnisse dieser Verteilungsschätzungsmethoden, die häufig in *RStudio* implementiert werden, können auch in der Blackout-Modellierung Anwendung finden und somit für wenig Aufwand mehr Tiefe in die Aussagekraft der Analyse bringen.

Entspricht etwa die Verteilung der Schadenhöhe X im Szenario "Allgemeine Haftpflicht: Großschäden" für *Versicherung AT1* einer Lognormalverteilung (also eines klassischen Typs einer Schadenhöhenverteilung)[7] mit Parametern $\mu = 15,834$ sowie $\sigma = 0,349$, so wäre der Erwartungswert dieser Zufallsvariablen annähernd gleich dem erwarteten Durchschnittsschaden mit

$$\mathbb{E}[X] = \exp(\mu + \frac{\sigma^2}{2}) \approx 7.999.587 \tag{4.6}$$

Aus ebendieser Verteilung könnte man nun mittels unterschiedlicher Sampling-Methoden realistische "Variation" in die Höhen der verschiedenen Schäden bringen.

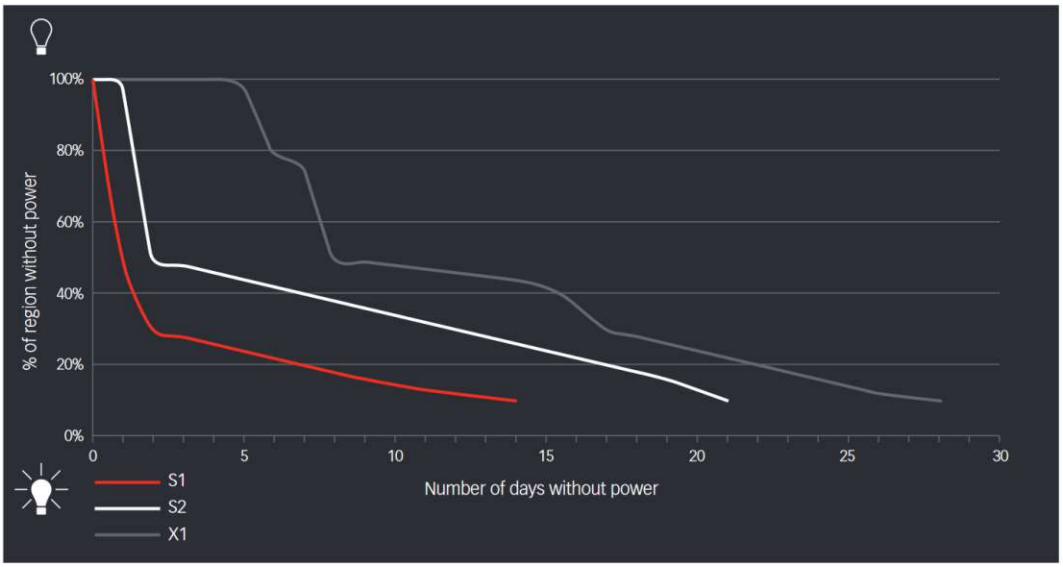
Besonders in der dann möglichen einzelschadenbasierten Rückversicherungsberechnung kann diese Methode aufzeigen, ob die Strategie aus Summen- und Schadenexzedenten für ein solches Blackout-Szenario adäquat gewählt wurde.

[7] Hier wird diese Verteilung nur angeschnitten, für weiterführende Informationen vgl. [Wik21a]

4.5.3 Variation der Blackout-Länge

Weiteres Entwicklungspotential wird auch in der Wahl der Blackout-Intensität und des Erholungsprozesses geortet. Betrachten wir zum Beispiel das in der Arbeit mehrfach erwähnte US-amerikanische Blackout-Szenario der britischen Universität Cambridge[8]: Hier wurden, entsprechend Schritt 4 im vorgestellten Szenariomodellierungsprozess, drei verschiedene Szenariovariationen ausgewertet, welche mit den Namen "S1" und "S2" für die "Standardszenarien" und "X1" für die ausgedachte "Extremvariante" versehen sind. Ebenso wurden hier Recovery-Phasen berücksichtigt, welche insbesondere bei der Berechnung des wirtschaftlichen Schadens entscheidend sind.

Folgend der Plot der einzelnen Szenarien, in welchem der Anteil der Haushalte ohne Strom in Abhängigkeit zur Zeit in Tagen abgebildet wurde:



Quelle: [Cam15, S.15]

Abbildung 4.2: Plot der drei Szenariovarianten

Den Einschätzungen von Herbert Saurugg aus [Sau21] und [Gra21] als auch der "Worst Case"-Betrachtungsweise der VIG entspräche das Szenario "X1". Beispielhaft wollen wir nun diese Variante, die zuvor im Modellierungstool implementiert wurde, auf die Variante eines "S2"-Blackouts skalieren:

Die Zielgröße im obigen Fall, entlang dem der Gesamtschaden skaliert werden kann, ist in

[8] Vgl. [Cam15, S.15]

der besprochenen Arbeit die Anzahl der "Outage-Days", welche dem jeweiligen Flächeninhalt unter den drei Funktionsgraphen entspricht. Dieser ist zu interpretieren als die Menge an fehlender Elektrizität, gemessen am durchschnittlichen Tagesbedarf der betroffenen Region. Das Extremszenario und das Szenario "S2" weisen "Outage-Days"-Werte von $13,83$ respektive $8,08$ auf.[9]

Nun gäbe es für den Aktuar die Möglichkeit, zusammen mit Fach- und Risikomanagement-Experten aufgrund dieses Skalenfaktors von $\frac{8,08}{13,83} \approx 0,584$ und dem Recovery-Profil des Szenarios die bestehenden Schadenhäufigkeiten und -höhen zu skalieren, um mit relativ wenig Arbeitsaufwand andere Szenariovarianten zu implementieren. Dies wurde im Zuge dieser Diplomarbeit beispielhaft implementiert, etwa unter der Annahme, dass die Häufigkeit von Schäden aufgrund sozialer Unruhen sich überproportional zu den "Outage Days" verhält (nicht jedoch die Schadenhöhen), oder etwa dass die kürzere Blackout-Länge in der Einkommensausfallversicherung keinen Einfluss auf die Schadenanzahl, jedoch einen direkt proportionalen Einfluss auf die Schadenhöhe haben könnte. Dies führt zu folgenden Annahmen bezüglich Frequenz und Schadenhöhe:

[9] Vgl. [Cam15, Appendix 2, S.18]

Name Einzelszenario	Frequenz: Schätzung basierend auf AT1	Wert mit 31.12.2020 in EUR	Durchschnittsschaden: Schätzung basierend auf AT1	Wert mit 31.12.2020 in EUR
KFZ-Kasko: Einbruchdiebstahl/Benzindiebstahl	30%*1/2 der regulären Jahresfrequenz im 10-Jahres-Schnitt	0,18%	100%*Durchschnittsschaden der letzten 10 Jahre	700
KFZ-Kasko: Fahrzeugdiebstahl	30%*1/2 der regulären Jahresfrequenz im 10-Jahres-Schnitt	0,02%	100%*Durchschnittsschaden der letzten 10 Jahre	8 000
KFZ-Kasko: Vandalismus	30%*1/2 der regulären Jahresfrequenz im 10-Jahres-Schnitt	0,08%	100%*Durchschnittsschaden der letzten 10 Jahre	1 100
Transportversicherung: Diebstahl	30%*1/3 der regulären Jahresfrequenz im 10-Jahres-Schnitt	1%	100%*Durchschnittsschaden der letzten 10 Jahre	7 500
Transportversicherung: Verderb von Gütern	80%*Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,88%	100%*Durchschnittsschaden der letzten 10 Jahre	3 200
Feuer- und Haushaltsversicherung: Feuerschäden	60%*Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,06%	100%*Durchschnittsschaden der letzten 10 Jahre	26 000
Feuer- und Haushaltsversicherung: Gasexplosionen	20%*Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,001%	100%*Durchschnittsschaden der letzten 10 Jahre	54 000
Haushaltsversicherung: Einbruchdiebstahl	30%*Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,05%	100%*Durchschnittsschaden der letzten 10 Jahre	2 900
Haushaltsversicherung: Überspannung	100%*Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,14%	100%*Durchschnittsschaden der letzten 10 Jahre	850
Einbruchdiebstahl Firmengeschäft	50%*Reguläre Jahresfrequenz im 10-Jahres-Schnitt	0,25%	100%*Durchschnittsschaden der letzten 10 Jahre	16 500
Leitungswasserversicherung: Frostschäden	100%*Expert Judgement	0,90%	70%*Expert Judgement	2 450
Allrisiko-Versicherung: Normalschäden	60%*Frequenz des schlechtesten der letzten 10 Jahre	Manuelle Eingabe	75%*Expert Judgement	45 000
Allrisiko-Versicherung: Großschäden	60%*Expert Judgement	Manuelle Eingabe	60%*Expert Judgement	450 000
Allgemeine Haftpflicht: Normalschäden	80%*Expert Judgement	0,06%	70%*Expert Judgement	280 000
Allgemeine Haftpflicht: Großschäden	70%*Expert Judgement	0,02%	58%*Expert Judgement	4 640 000
Rechtsschutzversicherung	85%*Expert Judgement	0,05%	100%*Expert Judgement	14 000
Einkommensausfallversicherung	100%*Expert Judgement	0,04%	60%*Expert Judgement	12 000

Quelle: Eigene Berechnung

Abbildung 4.3: Schaden-Input des Alternativszenarios "S2"

Die vorgenommenen Abstufungen führen zu einem Bruttoschaden von etwa 757 Millionen Euro (ca. 57% niedriger als im VIG-Standardszenario) und einem Nettoschaden von etwa 345 Millionen Euro (ca. 46% niedriger als im VIG-Standardszenario). Auch dieses modifizierte Szenario ist im Anhang unter einem Link abrufbar.

Mittels Recherche und gemeinsamer Abstimmung mit Risikomanagement-Abteilung, Aktuariat und Fachexperten ist also ein Implementieren verschiedener Szenariovarianten und -intensitäten hinsichtlich der Blackout-Länge durchaus eine Überlegung wert. Sie hat ebenfalls den positiven Nebeneffekt, den explorativen Aspekt der Szenarioanalyse zu intensivieren und verschiedene Blickwinkel auf ein Blackout-Szenario einzunehmen.

4.5.4 Weiterentwicklung hinsichtlich Abdeckungsgrad

Im Zuge der Konzeption dieser Diplomarbeit wurde ebenfalls eine Weiterentwicklung hinsichtlich geografischer Abdeckungsgrade diskutiert. Es könnten hierbei Fragen hinsichtlich der energietechnischen Abhängigkeiten von Staaten im Fall eines Frequenzabfalls erklärt werden, oder etwa die Anfälligkeit eines europäischen Landes für Frequenzabweichungen prinzipiell quantifiziert werden. Die Ergebnisse der diesbezüglichen Recherchen sei folgend angeführt:

Wie in den Ausführungen in 3.2.5 zu entnehmen ist, befindet sich die Energiewirtschaft derzeit in einem fundamentalen Wandel. Der Trend hin zu erneuerbaren Energien, die erhöhte Volatilität im Stromnetz sowie die Liberalisierung des Stromhandels innerhalb der EU führen höchst dynamischen Umfeldern. Auch Herbert Saurugg, Präsident der Österreichischen Gesellschaft für Krisenvorsorge, warnt diesbezüglich vor einer "Komplexitätsüberlastung"[10]. Alleine dies gestaltet eine verlässliche Modellentwicklung zur Quantifizierung einer prinzipiellen Blackout-Abhängigkeit zwischen Staaten als den Rahmen sprengend für diese Diplomarbeit. Weiters bestehen beispielsweise mit *ElectricityMap*[11] zwar Datensätze zum Stromhandel und dem Anteil an erneuerbaren Energien in der Stromerzeugung pro Land zur Verfügung, um daraus jedoch statistische Abhängigkeitsmaße zu generieren, fehlt zum derzeitigen Stand der fachliche Ansprechpartner hinsichtlich der europäischen Netzregelungstechnologien.

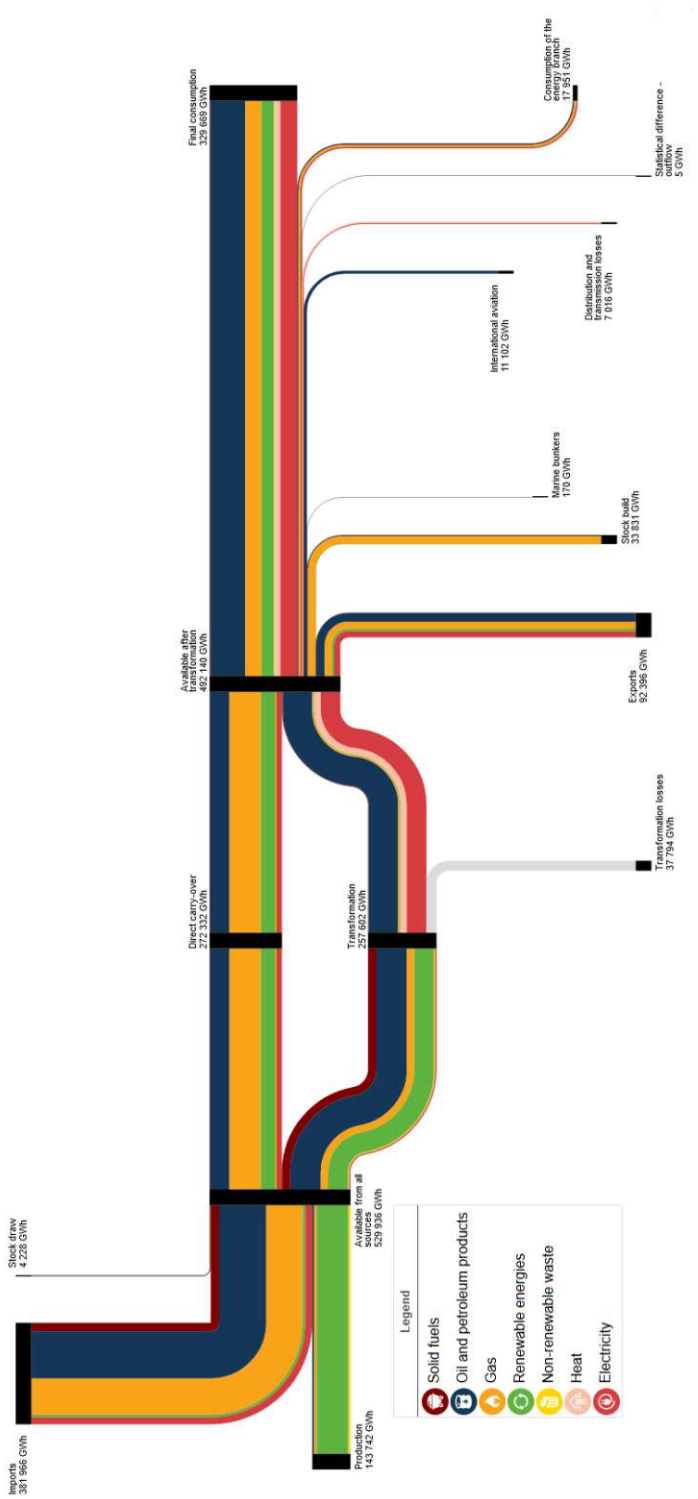
Ansätze und Datenquellen, die zukünftig in Zusammenarbeit mit Experten zu einer Art Risikobewertung von einzelnen Staaten innerhalb der EU führen können, sollen hier aber dennoch erwähnt werden:

Zunächst könnten Analysen auf bereits in dieser Arbeit genannten Kennzahlen aufbauen,

[10] Vgl. [Gra21]
[11] Für weitere Infos siehe `https://app.electricitymap.org/map`

nämlich den "SAIDI"-Werten aus 3.1. Sie geben Auskunft über die Zuverlässigkeit des Stromnetzes der einzelnen Staaten. Inwieweit diese Ausfälle durch Frequenzabweichungen entstehen muss jedoch noch geklärt werden.

Eine weitere Möglichkeit zur Einschätzung der Blackout-Anfälligkeit könnte in den Energie-Handelsbilanzen der europäischen Statistikbehörde *Eurostat* bestehen: Diese sind in sogenannten "Sankey"-Diagrammen für jedes EU-Mitglied verfügbar. Als Beispiel ist folgend die Bilanz für Österreich aus dem Jahr 2019 zu sehen:



Quelle: [San]

Abbildung 4.4: Energie-Handelsbilanz für Österreich 2019

Aus diesen Diagrammen können der Anteil an erneuerbaren Energien, das Verhältnis von Energieimporten zu -exporten sowie viele weitere Kennzahlen abgeleitet werden, welche als Attribute in verschiedenste Modelle eingebaut werden können. Auch hier gilt es jedoch, mit Spezialisten aus der Energiebranche die Aussagekraft ebensolcher Kennzahlen und ihren Einfluss auf die Blackout-Anfälligkeit eines Staates zu besprechen.

Weiters wurden vom österreichischen Übertragungsnetzbetreiber *Austrian Power Grid* diesbezüglich relevante Daten angefordert, wozu es bis dato jedoch keine Rückmeldung gab. Sobald hier entsprechende Daten und fachliches Know-How verfügbar ist, wird der Ansatz einer Risikobewertung je Land außerhalb dieser Diplomarbeit in einer eigenen Arbeit weiterverfolgt.

4.5.5 Berücksichtigung des Gegenparteiausfallrisikos

Die letzte auf diesen Seiten präsentierte Möglichkeit zur Weiterentwicklung stammt aus dem Vergleich des Blackout-Szenarios mit der Ermittlung der Solvenzkapitalanforderung gemäß Solvency II. Ein wichtiger Punkt in letzterer Berechnung besteht in der Ermittlung des *Gegenparteiausfallrisikos*[12], also des Verlustrisikos, welches mit unvorhergesehenen Ausfällen von bspw. Rückversicherern einhergeht. Genau dieses Risiko sollte auch für das Blackout-Szenario quantifiziert werden da das Szenario schließlich nicht nur ein Versicherungsunternehmen, sondern die komplette europäische Versicherungs- und Rückversicherungsbranche betrifft. Zahlungsausfälle in Rückversicherungskonstrukten können in diesem Fall ob des internationalen Ausmaßes nicht ausgeschlossen werden.

Der Zugang hierzu kann analog zur Berechnung des Gegenparteiausfallsrisikos in der SCR-Ermittlung erfolgen. Hierzu ist zusätzlich die Diskussion der Eintrittswahrscheinlichkeit eines (hackerinduzierten) Blackouts vonnöten, um die zu verwendenden Formeln von der "1-in-200-Jahren"-Sichtweise auf die gegebene Frequenz anpassen zu können. Näheres zum Vorgehen nach der Solvency II-Standardformel ist [Lag] zu entnehmen.

[12] Vgl. [Lag]

5 Conclusio

In dieser Arbeit wurden affirmative als auch "Silent" Cyber-Risiken definiert, erforscht und ihre Auswirkungen auf Versicherer erarbeitet. Die wichtigsten Schlüsse daraus sollen nun als Empfehlungen an die Wiener Städtische Versicherung, die Vienna Insurance Group als auch an allgemeine Versicherer, welche bei sich noch Optimierungspotential bezüglich Cyber-Risiken orten, dienen.

5.1 Schlüsse hinsichtlich klassischen Cyber-Risiken

Schenkt man den Prognosen der großen Beratungs- und Rückversicherungshäuser Glauben, so hat der Cyber-Versicherungsmarkt noch ein großes Wachstum vor sich, besonders in Europa. Um diesen Trend nicht zu verpassen, sollten sich Versicherer so früh als möglich mit entsprechenden Produkten im Zivil- und Firmen-/Gewerbegeschäft am Markt positionieren. Hierbei können Risiken, die vom Versicherer aufgrund geringer Erfahrung oder kleinen Beständen unerwünscht sind, durch Mittel wie bspw eine umfangreiche Rückversicherungsstrategie mitigiert werden.

Ein besonders wichtiges Merkmal bei Cyber-Risiken sind die allgemein fehlende Schadenhistorie, sowie der hohe Vernetzungsgrad unter den einzelnen Risiken. Bezüglich Ersterem kann man sich durch Data Sharing-Methoden teils Abhilfe verschaffen. Die aus Letzterem resultierende hohe Kumulanfälligkeit gehört jedoch genau beobachtet und kontrolliert. Dazu wurden verschiedene Methoden vorgestellt wie z.B. die Risikoselektion im Zuge des Underwriting-Prozesses oder die Kumulquantifizierung durch deterministische und stochastische Szenarien.

Die Wiener Städtische ist hier derzeit großteils von den Einschätzungen seitens externer Spezialisten abhängig, welche sich hauptberuflich mit der Cyber-Szenarienmodellierung beschäftigen und hierzu durch ihre Vielzahl an Kunden weltweit Daten sammeln. Soll ein eigener Szenarioansatz, wie beispielhaft durch verschiedene Narrative vorgestellt, durchgeführt werden, so muss für eine entsprechende Modellgüte eine Vielzahl an Informationen hinsichtlich der versicherten Risiken erhoben und dokumentiert werden. Die damit zu erzeugende Datenbasis ist ebenso skizziert worden.

Bei der Abschätzung des zukünftigen Bestandswachstums wurde anstatt des bisher verwendeten linearen Ansatzes eine Bestandsprognose entlang logistischer Wachstumskurven implementiert. Dieser wurde betriebswirtschaftlich argumentiert und führt zu einem weitaus höheren Kumulpotential als bisher angenommen.

5.2 Resümee hinsichtlich Silent Cyber-Risiken

Wir fassen die Ergebnisse der Aufarbeitung von nicht-affirmativen Cyber-Risiken ebenfalls kurz zusammen:

Mit dem Aufkommen der klassischen Cyber-Versicherungen sollten sich Versicherer in Europa auch mit dem Cyber-Exposure ihres klassischen Bestands beschäftigen. Laut einer Umfrage, welche die EIOPA bei ausgewählten Versicherungsgruppen durchgeführt hat, haben sich 41% noch nicht mit Cyber-Risiken im eigenen Bestand auseinandergesetzt. Diesen steht eine Vielzahl an Maßnahmen zur Verfügung, um die auftretenden Risiken zu messen, zu mitigieren und zu kontrollieren. Aber auch Maßnahmen im eigenen Bestand, etwa durch Awareness-Kampagnen in der Gesellschaft, zählen zu solch risikomindernden Maßnahmen.

Darauffolgend wurde untersucht, wie es eigentlich zu hackerinduzierten Blackouts kommen kann. Im Vergleich zu den restlichen Staaten, in denen die VIG operativ tätig ist, sieht hier die Risikolage Österreichs vergleichsweise gut aus. Die Entwicklungen bei der Umstellung auf erneuerbare Energien, der Etablierung von Smart Grids und dem fehlenden Ausbau von Primärregelleistung sollten jedoch von Versicherern und Energieregulatoren genau beobachtet werden.

Danach wurden die Folgen eines Blackouts nach österreichischen und britischen Expertenmeinungen analysiert. Verglichen mit den Auswirkungen der texanischen Energiekrise im Februar 2021 wirken sämtliche Annahmen durchaus plausibel. Dies unterstreicht die Notwendigkeit der Auseinandersetzung mit Blackout-Szenarien, auch und besonders bei Versicherungen aufgrund des hohen Kumulpotentials.

Nach Beleuchtung des Ablaufs einer generellen Szenarioanalyse wurden die Ambitionen der VIG hinsichtlich Szenariomodellierungen beleuchtet, sowie ein an das Modell des Enterprise Risk Managements angelehntes, allgemeines Tool zur explorativen Analyse des Kumulschadenpotentials im Blackout-Fall mathematisch beschrieben. Die Anwendung dieses Modells in Microsoft Excel ist frei verfügbar im Anhang dieser Arbeit verlinkt, und jedem Versicherungsunternehmen ans Herz zu legen, das sich noch nicht mit dem Thema "Silent Cyber" auseinandergesetzt hat. Die Methodik, Annahmen und Datenanforderungen dazu sind dieser Arbeit zu entnehmen.

Unter den zuletzt vorgestellten möglichen Weiterentwicklungen für das Blackout-Szenario finden sich mit der Inklusion anderer Deckungen oder der Variation des Recovery-Prozesses des Blackouts Optionen, die außerhalb dieser Diplomarbeit in das auf die VIG zugeschneiderte Szenariomodell eingearbeitet einen großen Mehrwert liefern können und werden. Auch die weitere Auseinandersetzung mit den einhergehenden Annahmen und logischen Strukturen (etwa in der Rückversicherungsberechnung) kann die Modellgüte noch weiter verbessern.

Zusammenfassend bietet diese Diplomarbeit mit dem Thema "Maßnahmen zur Kontrolle von Cyber-Kumulrisiken in der Versicherungswirtschaft" Versicherern erste Anhaltspunkte und Ideen zur Entwicklung eines Risikokontrollprozesses und damit die Möglichkeit, sich im Cyber-Versicherungsmarkt entsprechend zu positionieren. Die tiefergehende Auseinandersetzung sowie die Beleuchtung der unternehmenseigenen Kumulkontroll-Maßnahmen decken im Speziellen bei der Wiener Städtischen Versicherung und der Vienna Insurance Group Potentiale zur Optimierung und Weiterentwicklung in dieser Hinsicht auf und leisten somit einen Mehrwert; Einen Mehrwert dafür, dieses dynamische, vergleichsweise junge Risiko in einem immer komplexer werdenden Umfeld besser verstehen, abschätzen und managen zu können.

6 Abkürzungsverzeichnis

Abkürzung	Langform
5G	5. Generation des Mobilfunknetzes
bspw.	beispielsweise
bzw.	beziehungsweise
ca.	circa
CEE	Central and Eastern Europe, zu deutsch: Zentral- und Osteuropa
DACH-Raum	Deutschland, Österreich, Schweiz
DDoS	Distributed Denial of Service
EDV	Elektronische Datenverarbeitung
EIOPA	European Insurance and Occupational Pensions Authority
etc.	et cetera
EUR	Euro
Gbps	Gigabit pro Sekunde, Messgröße für Datenverkehr
ggf.	gegebenenfalls
KMU	Kleine und mittlere Unternehmen
kV	Kilovolt
Mio.	Millionen
PC	Personal Computer
RV	Rückversicherung
sog.	sogenannt/e/er/es
SQL	Structured Query Language
u.A.	unter Anderem
UCTE	Union for the Co-ordination of Transmission of Electricity
VIG	Vienna Insurance Group
VU	Versicherungsunternehmen
VVO	Verband der Versicherungsunternehmen Österreichs
WSTV	Wiener Städtische Versicherung AG
z.B.	zum Beispiel

7 Literaturverzeichnis

[APG21] Grafik: Austrian Transmission Grid. https://www.apg.at/api/sitecore/projectmedia/download?id=27e04cae-d929-4e56-b9af-992e25a1dea4, 2021. Abgerufen am 04.10.2021.

[Aue21] M. Auer. Die Presse: Wie Wien zur CO2-neutralen Stadt werden will. https://www.diepresse.com/6047335/wie-wien-zur-co2-neutralen-stadt-werden-will, 2021. Abgerufen am 17.10.2021.

[AVo21] Aktuarvereinigung Österreichs: Säule I. https://avoe.at/bibliothek/solvency-ii-risikomanagement/saeule-i/, 2021. Abgerufen am 29.10.2021.

[Bö21] U. Böse. Brauche ich einen Verkehrsrechtsschutz im VW Skandal? https://www.db-anwaelte.de/aktuelles/abgasskandal/welche-rechtsschutzversicherung-brauche-ich-im-abgasskandal, 2021. Abgerufen am 25.08.2021.

[BLR18] R. Böhme, S. Laube, and M. Riek. A Fundamental Approach To Cyber Risk Analysis. *The Variance Journal*, 11(2):453–510, 2018. Abgerufen am 16.12.2020.

[Bra14] 'Bolware' virus targets Brazil transactions. https://www.nafcu.org/newsroom/bolware-virus-targets-brazil-transactions, 2014. Abgerufen am 30.08.2021.

[BSG15] M. Bachmann, M. Shahd, and F. Grimm. Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz im digitalen Zeitalter. https://www.bitkom.org/sites/default/files/file/import/150709-Studienbericht-Wirtschaftsschutz.pdf, 2015. Abgerufen am 05.05.2021.

[Bun21] Sicher. Und morgen? - Sicherheitspolitische Jahresvorschau 2021. https://www.bundesheer.at/pdf_pool/publikationen/sihpoljahresvorschau2021.pdf, 2021. Abgerufen am 25.10.2021.

[Cam15] Cambridge CSR: Business Blackout. The insurance implications of a cyber attack on the US power grid. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf, 2015. Abgerufen am 09.09.2021.

[Cam16] Cambridge CSR: Managing Cyber Insurance Accumulation Risk. https://www.jbs.cam.ac.uk/wp.content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf, 2016. Abgerufen am 30.08.2021.

[CGGP20] S. Cartagena, V. Gosrani, J. Grewal, and J. Pikinska. Silent Cyber Assessment Framework. *British Actuarial Journal*, 25:1–19, 2020.

[Cor21] Schwarzstart: Stromausfall – Die Sekunden nach dem Blackout. https://correntlly.de/post/schwarzstart-stromausfall-die-sekunden-nach-dem-blackout/, 2021. Abgerufen am 26.10.2021.

[EIO18] EIOPA. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies, 2018.

[EIO19] Cyber Risk For Insurers - Challenges And Opportunities. https://www.eiopa.europa.eu/sites/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf, 2019. Abgerufen am 09.09.2021.

[EIO21] EIOPA: Insurance stress test. https://www.eiopa.europa.eu/insurance-stress-test_en, 2021. Abgerufen am 29.10.2021.

[Fro19] S. Frost. "Wir werden die Cyberversicherung als einen Standard sehen" - Interview mit Onnen Siems. https://www.gdv.de/de/themen/news/-wir-werden-die-cyberversicherung-als-einen-standard-sehen--44082, 2019. Abgerufen am 23.08.2021.

[Ger18] Klaus Gerathewohl. *Rückversicherung - Grundlagen und Praxis. Bd. 1.* VVW, 2018.

[Gla18] H. Glaab. Dealing with cyber accumulation risk. https://www.munichre.com/topics-online/en/digitalisation/cyber/dealing-with-cyber-accumulation-risk.html, 2018. Abgerufen am 28.08.2021.

[Gra21] A. Grass. Wiener Zeitung: Blackout - Was passiert, wenn nichts geht. https://www.wienerzeitung.at/nachrichten/wissen/technologie/2090245-Was-passiert-wenn-nichts-mehr-geht.html, 2021. Abgerufen am 26.10.2021.

[Her92] M. Herbrich. *Kumulkontrolle*. Gabler, 1992.

[Hon21] Wikipedia: Honeypot. https://de.wikipedia.org/wiki/Honeypot, 2021. Abgerufen am 16.02.2021.

[Ind21a] Baukostenindex, 2021.

[Ind21b] Eurostat: Purchasing power parities (PPPs), price level indices and real expenditures for ESA 2010 aggregates, 2021.

[Ind21c] Kraftfahrzeughaftpflicht-Versicherungsleistungspreisindex - KVLPI, 2021.

[Ind21d] Verbraucherpreisindex (VPI/HVPI, 2021.

[Jud20] Cambrige CSR: Developing Scenarios for Disaster Risk Reduction. https://lighthillrisknetwork.org/wp-content/uploads/DRR-DevelopingScenarios.pdf, 2020. Abgerufen am 09.09.2021.

[Koh21] Meyerthole Siems Kohlruss. Datenpools. https://aktuare.de/index.php/de/leistungen/datenpools.html, 2021. Abgerufen am 11.06.2021.

[KPM21] KPMG. Cyber-Versicherung. Versicherungssparte der Zukunft. https://home.kpmg/de/de/home/dienstleistungen/branchen-und-maerkte/financial-services/cyber-versicherung, 2021. Abgerufen am 23.08.2021.

[Kur21] Kurier: Beinahe-Blackout verursachte beim Flughafen Wien hohen Schaden. https://kurier.at/wirtschaft/beinahe-blackout-verursachte-beim-flughafen-wien-hohen-schaden/401163408, 2021. Abgerufen am 17.10.2021.

[Lag] Hilke Lagemann. Ermittlung des Gegenparteiausfallrisikos.

[Lam21] R. Lamprecht. Cyber Security in Österreich. https://publikationen.kpmg.at/cyber-security-2021/4458aa22b2ea8637773699413babfe27/cyber-security-in-oesterreich-2021.pdf, 2021. Abgerufen am 30.04.2021.

[Moe21] E. Moechel. Wie ein Blackout in Österreich abgewendet wird. https://fm4.orf.at/stories/3018234, 2021. Abgerufen am 02.10.2021.

[Net21] Was ist die Netzfrequenz? https://www.next-kraftwerke.de/wissen/netzfrequenz, 2021. Abgerufen am 13.10.2021.

[Ngu08] Tristan Nguyen. *Handbuch Der Wert- Und Risikoorientierten Steuerung Von Versicherungsunternehmen*. VVW, 2008.

[Pet11] Thomas et al. Petermann. *Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls*. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bd. 33. Nomos Verlag, Berlin, 2011.

[Pre18] Die Presse: Bericht: Europaweiter Stromausfall nach Hackerangriff möglich. https://www.diepresse.com/5485391/bericht-europaweiter-stromausfall-nach-hackerangriff-m\protect\unhbox\voidb@x\bgroup\U@D1ex{\setbox\z@\hbox{\char127}\dimen@-.45ex\advance\dimen@\ht\z@}\accent127\fontdimen5\font\U@Do\egroupglich, 2018. Abgerufen am 11.11.2021.

[RK20] J. Reinhart and M. Kreuzer. Cyber Insurance: Risks and Trends 2020. https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2020.html, 2020. Abgerufen am 05.05.2021.

[RSS13] J. Reichl, F. Schneider, and M. Schmidthaler. Power Outage Cost Evaluation: Reasoning, Methods and an Application. *Journal of Scientific Research and Reports*, 2013. Abgerufen am 23.10.2021.

[San] Eurostat: Energy balance flow for Austria 2019.

[Sau21] H. Saurugg. Auswirkungen eines Blackouts. https://www.saurugg.net/blackout/auswirkungen-eines-blackouts, 2021. Abgerufen am 27.10.2021.

[Ser21] Redaktion ServusTV. Blackout – Kein Plan für den Notfall. https://www.servustv.com/aktuelles/v/aa-27eq5wp4w1w11/, 2021. Abgerufen am 26.10.2021.

[Sig21] Wikipedia: Sigmoidfunktion. https://de.wikipedia.org/wiki/Sigmoidfunktion, 2021. Abgerufen am 09.08.2021.

[Sok08] M. Sokele. Growth Models for the Forecasting of New Product Market Adoption. https://www.researchgate.net/publication/242636096_Growth_

Models_for_the_Forecasting_of_New_Product_Market_Adoption, 2008. Abgerufen am 09.08.2021.

[Swi21] Netzebenen. https://www.swissgrid.ch/de/home/operation/power-grid/grid-levels.html, 2021. Abgerufen am 02.10.2021.

[Ver21] Wie funktioniert das Stromnetz? https://www.verbund.com/de-at/privatkunden/themenwelten/strom-aus-wasserkraft/stromnetz, 2021. Abgerufen am 02.10.2021.

[VIG21] VIG Konzernbericht 2020. https://www.vig.com/fileadmin/web/Investor_Relations/Geschaeftsberichte/Konzernabschluss/210415_-_VIG_Konzernbericht_2020_INTERNET.pdf, 2021. Abgerufen am 13.05.2021.

[VVO21] VVO: Jahresbericht 2020. https://www.vvo.at/vvo/vvo.nsf/sysPages/Jahresbericht_2020.html/$file/VVO_Jahresbericht2020_Gesamt.pdf, 2021. Abgerufen am 13.05.2021.

[Whi21] White-Hat-Hacker: gut, böse oder beides? https://www.kaspersky.de/resource-center/definitions/white-hat-hackers, 2021. Abgerufen am 05.05.2021.

[WHSJ17] J. Wälder, M. Heyen, C. Sagawe, and H. Jahn. KPMG: Neues Denken, Neues Handeln: Insurance Thinking Ahead - Versicherungen im Zeitalter von Digitalisierung und Cyber. Studienteil B: Cyber, 2017.

[Wik21a] Logarithmische Normalverteilung. https://de.wikipedia.org/wiki/Logarithmische_Normalverteilung, 2021. Abgerufen am 26.11.2021.

[Wik21b] Netzebene (Stromversorgung). https://de.wikipedia.org/wiki/Netzebene_(Stromversorgung), 2021. Abgerufen am 02.10.2021.

[Wik21c] Wikipedia: 2021 Texas power crisis. https://en.wikipedia.org/wiki/2021_Texas_power_crisis, 2021. Abgerufen am 29.10.2021.

[Wik21d] Wikipedia: Regelleistung (Stromnetz). https://de.wikipedia.org/wiki/Regelleistung_(Stromnetz), 2021. Abgerufen am 17.10.2021.

[Wik21e] Wikipedia: System Average Interruption Duration Index. https://de.wikipedia.org/wiki/System_Average_Interruption_Duration_Index, 2021. Abgerufen am 26.10.2021.

[WST17] Klauseltext Pay Protect, 2017.

[WST19] Besondere Bedingungen für die Haushaltsversicherung: Deckungsvariante Haushalt Extra, 2019.

[WST20a] Allgemeine Bedingungen für die Cyber-Protect-Versicherung, 2020.

[WST20b] Flugblatt Cyber Protect Basic. https://www.wienerstaedtische.at/fileadmin/user_upload/Dokumentenpool/Business/Flugblatt_CyberProtectBasic.pdf, 2020. Abgerufen am 26.07.2021.

[WST20c] Klauseltext 2013K: Internet Schutz-Hilfe, 2020.

[WST20d] Klauseltext Internet-Rechtsschutz, 2020.

[WTW] The problem of silent cyber risk accumulation.

[WTW21] Wtw: Data sharing models in the insurance industry. https://www.willistowerswatson.com/en-GB/Insights/2021/02/data-sharing-models-in-the-insurance-industry, 2021. Abgerufen am 11.06.2021.

8 Anhang

8.1 Fragebogen zu Cyber Protect

Folgend der gesamte Fragebogen der Wiener Städtischen, welcher im Zuge des Underwritings für das Produkt "Cyber Protect" verwendet wird:

Betrieb & Absichern | Cyber Protect

Cyber-Fragebogen zur Risikobeurteilung

Cyber-Center-Hilfe 24 Stunden, 7 Tage unter 050 350 355

Dieser Fragebogen ist weder ein Angebot noch ein bindender Versicherungsvertrag (Deckung). Das Ausfüllen dieses Fragebogens verpflichtet den Versicherer nicht, eine Deckung anzubieten.

Name und Anschrift aller AntragstellerInnen inklusive aller Tochterunternehmen

In welcher Branche sind Sie tätig?

Jahresumsatz

Österreich	EUR	USA	EUR	weltweit exkl. USA (exkl. Österreich)	EUR

davon Jahresumsatz durch Onlineaktivitäten (z. B. durch E-Commerce)

Österreich	EUR	USA	EUR	weltweit exkl. USA (exkl. Österreich)	EUR

Welche Art von sensiblen Kundendaten wird im Unternehmen verarbeitet und gespeichert?

personenbezogene Daten	Bezahlkarteninformationen	persönliche Gesundheitsinformationen
geistiges Eigentum	Usernamen und Passwörter	

Verarbeiten/Speichern Sie personenbezogene Daten von BürgerInnen der USA, oder verarbeiten/speichern Sie die personenbezogenen Daten in Datenzentren, die sich in den USA befinden? ja nein

Bitte geben Sie den (erwarteten) Umfang (Anzahl an eindeutigen Datensätzen) sensibler Daten an, die Ihr Unternehmen verarbeitet/speichert:

Versicherungssumme und Selbstbehalt

Versicherungssumme	EUR 100.000,–	EUR 250.000,–	EUR 500.000,–	EUR 1.000.000,–
Selbstbehalt	EUR 1.000,–	EUR 2.500,–	EUR 5.000,–	

Betrieb & Absichern | Cyber Protect

Welche optionalen Deckungen sind gewünscht?

Betriebsunterbrechung	pauschaler Deckungsbeitrag pro Tag EUR	ja nein
Cybererpressung		ja nein
Medienhaftpflicht		ja nein
Krisenmanagement		ja nein
Cyberbetrug und Cyberdiebstahl (Sublimit: 20 % der kombinierten Versicherungssumme)		ja nein
Haben Sie Teile Ihres Netzwerks, Ihres Computersystems oder Ihrer Informationssicherheitsmaßnahmen an externe Dienstleister (Outsourcing) vergeben?		ja nein

Outsourcing-Dienstleister
(Name, Adresse)

Management des gesamten IT-Systems | Datenverarbeitungsdienstleister | Anwendungsdienstleister

externe Speicher und Back-up-Dienstleistungen | sonstige Cloud-Dienstleistungen

Risikofragen

Wenn Unternehmensumsätze **bis EUR 10.000.000,–,** dann müssen die Risikofragen 1 bis 5 beantwortet werden.
Wenn Unternehmensumsätze **über EUR 10.000.000,–,** dann sind zusätzlich die Risikofragen 6 bis 10 zu beantworten.
Wenn Unternehmen ein **Cyber-Trust-Austria-Label** (Basis oder Gold) vorweisen können, dann bitte um Beantwortung der Risikofragen 1, 2, 3 sowie 9. Eine Kopie der aktuellen Zertifizierung (Cyber-Trust-Austria-Label oder Cyber-Trust-Austria-Label Gold) ist diesem Fragebogen beizufügen.

1.	Verwenden Sie einen laufend aktualisierten Schutz vor Schadsoftware für alle Server und Endgeräte?	ja nein
2.	Installieren Sie – zumindest innerhalb eines Monats nach Veröffentlichung – Aktualisierungen für kritische IT-Systeme und Anwendungen („Sicherheits-Patching")?	ja nein
3.	Führen Sie mindestens wöchentlich Datensicherungen (physisch getrennt, Zugriff nur mit administrativen Rechten) aller geschäftskritischen Daten durch?	ja nein
4.	Vermeiden Sie lokale Administratorrechte und beschränken Sie die Zugriffsrechte von MitarbeiterInnen und externen NutzerInnen auf Basis betrieblicher Notwendigkeit (insbesondere administrative Berechtigungen und Zugriff auf vertrauliche, z. B. persönliche, Daten)?	ja nein
5.	Sind vertrauliche Informationen, die auf mobilen Geräten (z. B. Smartphones und Laptops) gespeichert sind, verschlüsselt?	ja nein
6.	Bieten Sie mindestens jährlich eine Weiterbildung an, um das Sicherheitsbewusstsein Ihrer BenutzerInnen (MitarbeiterInnen und AuftragnehmerInnen) zu erhöhen und sie darauf vorzubereiten, widerstandsfähiger und wachsamer gegen Phishing zu sein?	ja nein
7.	Haben Sie einen Plan zur Reaktion auf Informationssicherheitsvorfälle (Incident Response Plan)?	ja nein
8.	Haben Sie eine Kennwortrichtlinie implementiert, die die Verwendung langer und komplexer Kennwörter in Ihrer Organisation erzwingt?	ja nein
9.	Sind alle Internetzugangspunkte durch entsprechend konfigurierte Firewalls abgesichert?	ja nein
10.	Überprüfen Sie regelmäßig kritische Systeme (inkl. Penetrationstests oder Schwachstellenanalysen) – entweder selbst oder von Dritten unterstützt –, insbesondere bei jeder Einführung neuer Systeme und nach Änderungen?	ja nein

Betrieb & Absichern | Cyber Protect

Sicherheitsereignisse und Schadenshistorie, Verlustbegrenzung und Unterschrift

Kam es in den letzten drei Jahren zu einer Verletzung der IT-Sicherheit, zu Netzwerkschäden, Systemkorruption oder Datenverlust?		ja	nein
Wenn ja, wie hoch war der diesbezügliche finanzielle Schaden für Ihr Unternehmen?	EUR		
Stimmen Sie zu, dass im Fall eines Schadens (externen) SchadensbearbeiterInnen und/oder IT-ExpertInnen Zugang zu Ihrem IT-System und Netzwerk gewährt wird?		ja	nein

Hiermit – durch Unterzeichnen dieses Dokuments (durch ein Vorstandsmitglied, eine/n EigentümerIn oder ManagerIn) – bestätige ich, dass ich ein/e bevollmächtigte/r VertreterIn des Unternehmens mit ausreichender technischer Fähigkeit bezüglich der IT-Sicherheit bin und – nach bestem Wissen – genaue und umfassende Antworten zu den Fragen dieses Fragebogens im Namen des Unternehmens getätigt habe. Der ausgefüllte Fragebogen und optionale Anhänge sind Basis für die Deckung und werden folglich ein Teil des Versicherungsvertrags. Alle oben erwähnten Angaben gelten für die/den AntragstellerIn sowie für die genannten Tochterunternehmen.

Name

Position

E-Mail

Datum

Unterschrift

Das könnte Sie auch interessieren:

Business Class
Unser Sicherheitsplan für Ihren Betrieb

Kfz-Versicherung für Klein- und Mittelbetriebe
Die Versicherungslösung für Ihre Firmenfahrzeuge

Wir sind für Sie da.

Für weitere Informationen wenden Sie sich einfach an Ihre/n BeraterIn der Wiener Städtischen, oder nutzen Sie diese Kontaktmöglichkeiten:

Serviceline 050 350 350
kundenservice@wienerstaedtische.at
wienerstaedtische.at mit ServiceBot | Videoberatung | Live Chat

Hinweis: Zweck dieses Folders ist eine kurze und geraffte Information über unsere Produkte. Er ist kein Angebot im rechtlichen Sinn. Der Folder wurde sorgfältig erarbeitet, doch kann die verkürzte Darstellung zu missverständlichen oder unvollständigen Eindrücken führen. Für verbindliche Informationen verweisen wir auf die vollständigen Antragsunterlagen, die Polizzen und die diesen zugrunde liegenden Versicherungsbedingungen.

Aus Gründen der besseren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung bei zusammengesetzten Wörtern und Produktnamen verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichstellung selbstverständlich für alle Geschlechter.

Medieninhaber und Hersteller:
Wiener Städtische Versicherung AG Vienna Insurance Group
Verlags- und Herstellungsort: Wien
Bildnachweis: Shutterstock
(21.04 – J20218724)

Ihre Sorgen möchten wir haben.

WIENER STÄDTISCHE
VIENNA INSURANCE GROUP

8.2 R-Code zur Bestandsprognose

Der folgende Code wurde mit *RStudio* in der Version *3.5.2-"Eggshell Igloo"* in einer 64 Bit-Umgebung ausgeführt. Er hat die Plots aus 2.1.4 als Output:

```
#Projektion des Haushalts- und Rechtsschutz-Cyberbestandes der WSTV
#Autor: Andreas Schmid
#Stand/Last Edit: 23.09.2021

#x/y - Daten: Aus "Cyber Kumul - Entwicklung und Abschaetzung_ab 2021"
#entnommen und auf ersten verfuegbaren Wert normiert
x_HH<-c(1:9)
y_HH<-c(100,469,5753,15490,29288,46457,65369,86231,107055)

x_RS<-c(1:11)
y_RS<-c(100,108,120,127,133,145,149,214,284,371,450)

#G: Aus Gesamtzahl der Vertraege im Bestand mit Normierung (lfd.
#Auswertung durch Gernot Steiner)
#durchdringung: Aus SQL-Query "Cyber-Durchdringung", Zeitraum
#01.01.2021-13.08.2021
G_HH<-578000
durchdringung_HH<-0.927

G_RS<-3729
durchdringung_RS<-0.82

alph_HH<-1000  #Gewicht des Strafterms
alph_RS<-100   #Gewicht des Strafterms

index<-c(1:30) #Plotbereich

#Startwerte der Optimierungen: Durch Ausprobieren und Plotten von
#verschiedenen Varianten

##################################################################
#Version ohne Bestrafung, ohne Trend
##################################################################
#Haushalt Extra - Basic
G<-G_HH * durchdringung_HH
modelfct<- y_HH ~ G / (1 + exp(-k * (x_HH-c)))
coefs<-as.numeric(coef(nls(modelfct, start=list(k=0.5,c=12))))

plot(y_HH ~ x_HH, main = "Haushalt_Extra", xlim=c(1,max(index)),
     ylim=c(0,G*1.05))
```

```
lines(index, G / (1 + exp(-coefs[1] * (index-coefs[2]))))
abline(h=G, col='red')

#RS Gesamt - Basic
G<-G_RS * durchdringung_RS
modelfct<- y_RS ~ G / (1 + exp(-k * (x_RS-c)))
coefs<-as.numeric(coef(nls(modelfct, start=list(k=0.2,c=23))))

plot(y_RS ~ x_RS, main = "RS Gesamt", xlim=c(1,max(index)),
     ylim=c(0,G*1.05))
lines(index, G / (1 + exp(-coefs[1] * (index-coefs[2]))))
abline(h=G, col='red')




######################################################################
#Version mit Bestrafungsterm, ohne Trend
######################################################################
#Haushalt Extra mit Bestrafungsterm
G<-G_HH * durchdringung_HH
modelfct<- y_HH ~ (G / (1 + exp(-k * (x_HH-c))) + alph_HH*
                   ((G/(1+exp(-k*(x_HH[length(x_HH)]-c))))-
                   y_HH[length(y_HH)]))
coefs<-as.numeric(coef(nls(modelfct, start=list(k=0.43,c=12))))

plot(y_HH ~ x_HH, main = "Haushalt /w Constraints", xlim=c(1,max(index)),
     ylim=c(0,G*1.05))
lines(index, G / (1 + exp(-coefs[1] * (index-coefs[2]))))
abline(h=G,col='red')


#RS Gesamt mit Bestrafungsterm
G<-G_RS * durchdringung_RS
modelfct<- y_RS ~ (G / (1 + exp(-k * (x_RS-c)))) + alph_RS*
                   ((G/(1+exp(-k*(x_RS[length(x_RS)]-c))))-
                   y_RS[length(y_RS)])
coefs<-as.numeric(coef(nls(modelfct, start=list(k=0.2,c=23))))

plot(y_RS ~ x_RS, main = "RS Gesamt /w Constraints", xlim=c(1,max(index)),
     ylim=c(0,G*1.05))
lines(index, G / (1 + exp(-coefs[1] * (index-coefs[2]))))
abline(h=G, col='red')
```

8.3 Links und Gesamtübersicht Blackout-Szenario

Die Modellierungsdatei, welche für beliebige europäische Versicherungsgruppen konzipiert ist, ist unter folgendem Link frei verfügbar: *Google Docs*.

Hier auch das auf das Szenario "S2" skalierte Modell, welches im Zuge von 4.5.3 erstellt wurde. Es ist ebenfalls frei verfügbar: *Google Docs*.

Folgend ein Auszug aus dem Tabellenblatt "Hauptberechnung" des Standard-Blackout-Modells, welches eine Gesamtübersicht über die exakten Berechnungen mit gerundeten, beispielhaften Input-Daten bietet. Die abgebildeten Daten sind daher, wie im gesamten entsprechenden Kapitel dieser Arbeit, rein fiktiv, bewegen sich jedoch in einer plausiblen Größenordnung:

Name Einzelszenario	Durchschnittsschaden ATI in EUR	Angenommene Frequenz	Bruttoschaden (gewichtet)	RV-Anteil	Nettoschaden	Anzahl an Schäden	Anzahl an Risiken in der Sparte
KFZ-Kasko: Einbruchdiebstahl/Benzindiebstahl	700	0,60%	4 482 074	0%	4 482 074	8 942	1 490 345
KFZ-Kasko: Fahrzeugdiebstahl	8 000	0,07%	5 549 234	0%	5 549 234	969	1 490 345
KFZ-Kasko: Vandalismus	1 100	0,28%	3 286 854	0%	3 286 854	4 173	1 490 345
Transportversicherung: Diebstahl	7 500	4,00%	5 646 276	0%	5 646 276	1 012	25 290
Transportversicherung: Verderb von Gütern	3 200	1,10%	662 496	0%	662 496	278	25 290
Feuer- und Haushaltsversicherung: Feuerschäden	26 000	0,10%	65 048 598	0%	65 048 598	4 183	4 183 120
Feuer- und Haushaltsversicherung: Gasexplosionen	54 000	0,00%	4 053 028	0%	4 053 028	125	4 183 120
Haushaltsversicherung: Einbruchdiebstahl	2 900	0,18%	9 173 772	0%	9 173 772	5 135	2 852 595
Haushaltsversicherung: Überspannung	850	0,14%	2 091 339	0%	2 091 339	3 994	2 852 595
Einbruchdiebstahl Firmengeschäft	16 500	0,50%	24 807 040	0%	24 807 040	2 342	468 477
Leitungswasserversicherung: Frostschäden	3 500	0,90%	24 959 815	0%	24 959 815	12 706	1 411 749
Allrisiko-Versicherung Normalschäden	60 000	Manuelle Eingabe	7 328 129	48%	3 846 810	168	-
Allrisiko-Versicherung: Großschäden	750 000	Manuelle Eingabe	41 891 171	56%	18 378 706	78	-
Allgemeine Haftpflicht: Normalschäden	400 000	0,08%	179 746 512	26%	133 732 898	717	896 857
Allgemeine Haftpflicht: Großschäden	8 000 000	0,03%	1 348 098 843	77%	314 275 790	269	896 857
Rechtsschutzversicherung	14 000	0,06%	4 091 461	0%	4 091 461	442	735 910
Einkommensausfallversicherung	20 000	0,04%	9 840 080	0%	9 840 080	774	1 936 234
SUMME:			**1 740 756 724**	**64%**	**633 926 272**	**46 307**	**24 939 129**

Abbildung 8.1: Gesamtübersicht des Blackout-Szenarios