

# Bericht der AG Cyber und Beispiele aus der Praxis

Dr. Clemens Frey, Roland Berger  
Dr. Hendrik Kläver, Gen Re  
Jonas Becker, Munich Re



DAV

DEUTSCHE  
AKTUARVEREINIGUNG e.V.



DGVFM

DEUTSCHE GESELLSCHAFT  
FÜR VERSICHERUNGS- UND  
FINANZMATHEMATIK e.V.

Bericht der AG Cyber – Fachgruppe ASTIN



# Agenda

1. AG Cyber – Überblick
2. Besonderheiten und Einfluss auf das Risikomanagement
3. Modellierung von Cyberrisiken – Use Case
4. Beispiel: Management von Cyber-Kumulativen bei der Munich Re

# AG Cyber – Überblick und Ergebnisse

Vorstand Deutsche Aktuarvereinigung e.V.

Ausschuss Schadenversicherung

"AG Cyber" - Arbeitsgruppe  
Daten und Methoden zur  
Bewertung von  
Cyberrisiken

- Januar 2019 – Gründung
- Juli 2020 – *Daten und Methoden zur Bewertung von Cyberrisiken*
- Juni 2022 – *Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement von Versicherungsunternehmen*
- November 2022 – *Use Case zur Modellierung (Beispielportfeuille, Modellansätze inkl. Programmierung)*
- Webinare und Vorträge (auch international)
- Veröffentlichungen

# Mitglieder der AG Cyber

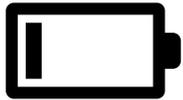
- Dr. Clemens Frey (Roland Berger)
- Jonas Becker (Munich Re)
- Dr. Vinzenz Erhardt (Allianz)
- Christine Fonger (Gothaer)
- Jan Gompers (Allianz)
- Claudia Görtzen (HDI)
- Dr. Hendrik Kläver (Gen Re)
- Florian Liebe (EY)
- Dr. Carsten Liese (HDI)
- Nina Kilian (BaFin)
- Dr. Mathias Raschke (Ecclesia Re)
- Dr. Leonie Ruderer (R+V Re)
- Frank Sagerer (Allianz)
- Maximilian Stosch (Munich Re)
- Dr. Franziska Taruttis-Glagoleff (HUK)
- Roland Voggenauer (Humn)
- Dr. Nikolai Vogl (Munich Re)



# Agenda

1. AG Cyber – Überblick
2. Besonderheiten und Einfluss auf das Risikomanagement
3. Modellierung von Cyberrisiken – Use Case
4. Beispiel: Management von Cyber-Kumulativen bei der Munich Re

# Aktuelle Marktentwicklungen im Bereich Cyberversicherung



Begrenzte  
Kapazität  
am Markt



Hohe Nachfrage,  
starker Anstieg  
der Preise



Ukraine Krieg,  
Ransomware,  
Covid 19

## USA

- Cyber pricing increased 79%, compared to 110% in the prior quarter and 133% in December 2021.
  - Insurers have begun to calibrate underwriting and pricing strategies on an account-by-account basis rather than on a portfolio basis.
  - Several insurers recently entered the cyber market, increasing competition.
  - Insureds with strong cybersecurity controls may experience a stabilizing of pricing if they have previously experienced significant rate adjustments.
  - Insureds lacking basic cyber hygiene can expect to see continued significant premium and retention increases, coverage restrictions, and/or overall insurability challenges.

## Europa

- Cyber insurance pricing increased by 50%, compared to 80% in the prior quarter.
- Concerns around systemic exposures and accumulation risk continued to grow, with the war in Ukraine a particular concern.

# Cyberisiken sind eine spezifische Herausforderung



Kumulgefahr  
Gesamtbilanz



Systemisches Risiko /  
Veränderungsdynamik



Datenverfügbarkeit und  
Modellierung



Risikosteuerung  
und -transfer

Gesamte Wertschöpfungskette ist betroffen,  
besondere Herausforderungen für das Cyber-Risikomanagement



# Agenda

1. AG Cyber – Überblick
2. Besonderheiten und Einfluss auf das Risikomanagement
3. Modellierung von Cyberrisiken – Use Case
4. Beispiel: Management von Cyber-Kumulativen bei der Munich Re

# Einordnung

- In der AG Cyber hat sich die UAG „Use Case zur Modellierung von Cyberrisiken“ gebildet.
- Dieser Vortrag gibt einen Überblick über den **Ergebnisbericht der UAG Use Case**, der in Kürze veröffentlicht wird. Die im Ergebnisbericht beschriebenen Modellansätze wurden ergänzend in einem **R Skript** umgesetzt.

# Use Case: Zielsetzung

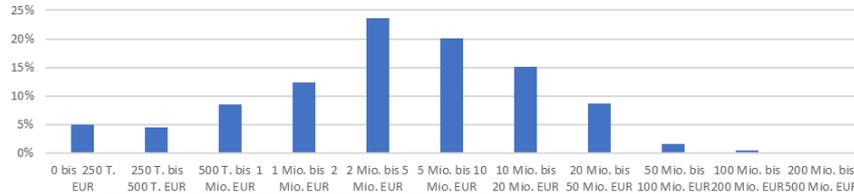
- Fallstudie: Perspektive von aktuariellen ModelliererInnen **in der Erstversicherung**
  - Neu eingeführtes Cyberprodukt für KMU
  - Ermittlung von **Schadenerwartungswert** und **Kumulrisiko**
- Ziel:
  - **methodischer Rahmen**
  - als Ganzes oder in Teilen verwendbar
  - „zweite Meinung“ zu einem bestehenden Modell
- Fragestellungen:
  - **Risikofaktoren?**
  - **Daten?**
  - **Abhängigkeiten?**

# Use Case: Vorgehen

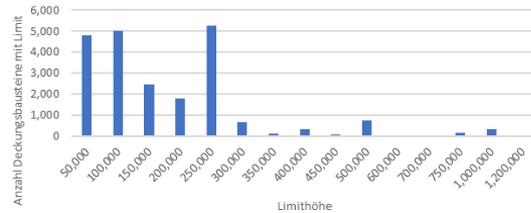
- Modularer Ansatz: Erstellung von Modulen pro Schadenart
  - Ransomware-Angriffe im Fokus
  - Modellierung für andere Schadenarten erfolgt grundsätzlich analog
- Modellkalibrierung
  - Frei verfügbare Datenquellen
  - Expertenschätzungen im weiteren Sinn
- Ergebnisanalyse
  - Kalkulation des Schadenbedarfs
  - Grenzen des Modells

# Portfolio-Zusammensetzung

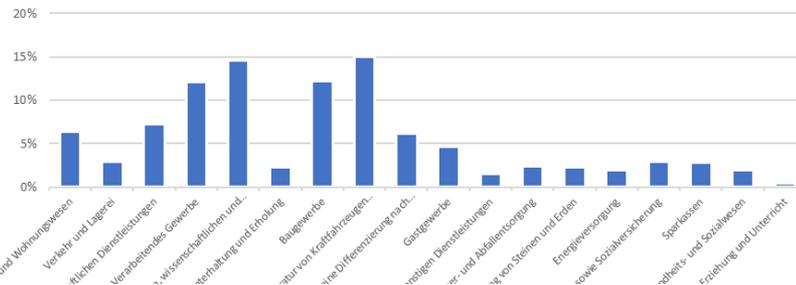
Bestandsmix nach Umsatz-Größenklassen



Verteilung Limite im Portfolio



Bestands-Mix nach Wirtschaftszweigen



- Muster-Portfolio bestehend aus 5000 Risiken
- Risikofaktoren im Modell
  - Wirtschaftszweig
  - Umsatz
  - Anzahl der Beschäftigten
- Deckungsbausteine: BU, Drittschaden, Eigenschaden etc.
- Limit und Selbstbehalt je Police
- Keine weitere Spezifikation wie z.B. Level der IT-Sicherheit, technologische Fähigkeiten etc.

# Frequency-Severity-Ansatz mit Kumulpotential

- Ansatz basiert auf (Zeller & Scherer, 2021)
- Unterscheidung zwischen Cyber-Vorfällen
  - Idiosynkratisch
    - zielgerichtet gegen ein bestimmtes Unternehmen
    - Unabhängigkeit zwischen Risiken
  - Systemisch
    - richtet sich gegen mehrere Unternehmen gleichzeitig
    - Abhängigkeit zwischen Risiken und folglich Kumulpotential
- Jeweils Annahme einer lognormalverteilten Schadenhöhe. Anspruchsvoller ist jeweils die Modellierung der Frequenz.

# Frequenzverteilung im Frequency-Severity-Ansatz mit Kumulpotential (1)

- Idiosynkratische Ereignisse für Risiko  $B_i$ 
  - Poisson-Prozess mit kumulativer Rate  $\lambda(T; B_i) := \int_0^T \exp(f(B_i) + g(t)) dt$
  - $f$  = Relativitäten in Abhängigkeit der Risikofaktoren
  - $g$  = zeitabhängige, marktweite Frequenz
  - Mit der Annahme von zeitlicher Unabhängigkeit, also konstantem  $g \equiv \ln(\lambda)$ , vereinfacht sich die kumulative Rate (bei gegebener Periodenlänge) zu  $\lambda \times p_1^{i_1} \times p_2^{i_2} \times p_3^{i_3}$
  - Schätzung der Parameter:
    - Marktweite Frequenz aus GDV-Statistik und Risikobericht (Dreißigacker & von Skarczynski & Wollinger, 2020).
    - Relativitäten aus Risikobericht

## Frequenzverteilung im Frequency-Severity-Ansatz mit Kumulpotential (2)

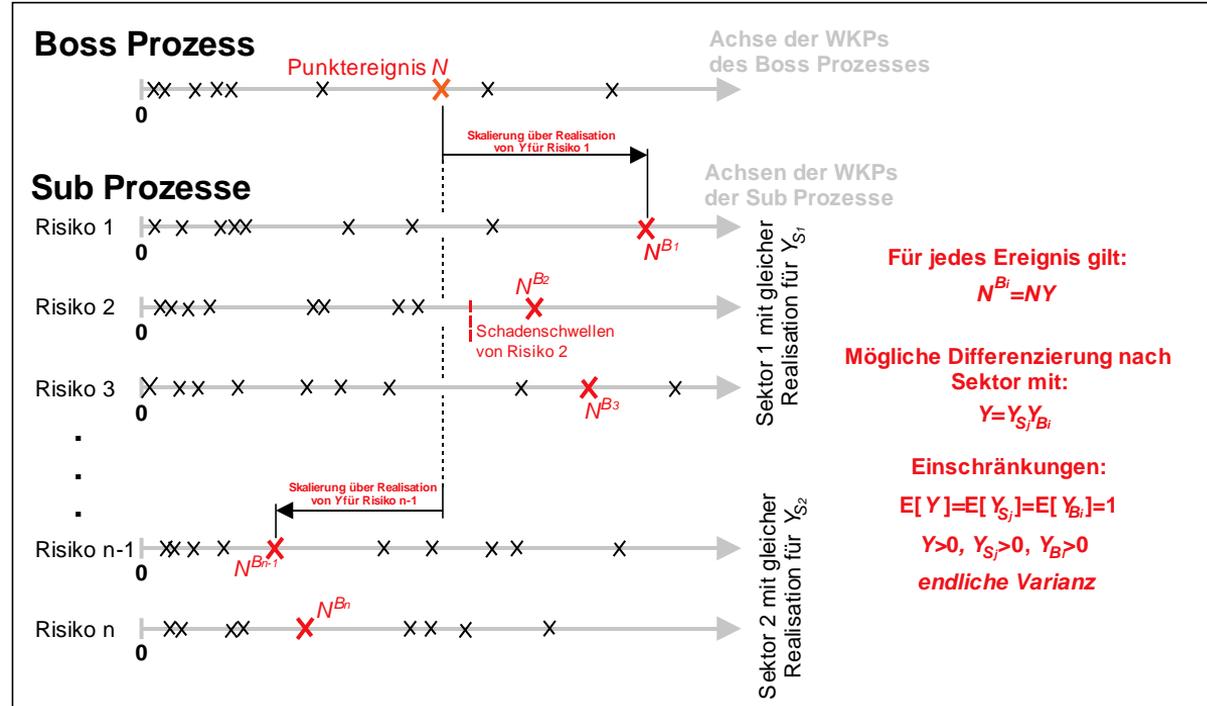
- Systemische Ereignisse
  - Modellierung als Punktprozess mit Poisson-verteilter kumulativer Rate für den Markt
  - Frequenz pro Wirtschaftszweig und Frequenz für Szenarien, die alle Wirtschaftszweige treffen
  - Bestimmung der gleichzeitig tangierten Risiken durch binomialverteilte Simulation
  - Parametrisierung wie bei idiosynkratischen Ereignissen

# Extremwertstatistischer Hintergrund

- Poisson-Punktprozesse mit Intensität (Punktdichte)  $\lambda(x) = x^{-2}$
- Implizit verlinkte Punktprozesse  $x_2 = yx_1$  mit Zufallsvariable  $Y$  ( $E[Y] = 1$ ,  $Var[Y]$  ist endlich).  $Y$  bestimmt die Verlinkung zwischen  $x_1$  und  $x_2$
- Max-stabiler Link:  $Max\{x_1\}$  und  $Max\{x_2\}$  über Extremwert-Copula verbunden (gleiche Copula für ein- oder hundertjähriges Maximum; Tail Dependence)
- Erwartete Frequenz an Punkten  $x$  über einem Schwellenwert  $x_T$  ist  $\Lambda(x_T) = x_T^{-1}$
- Die Wiederkehrperiode (WKP) ist das Reziproke der Frequenz  $\Rightarrow x$  ist eine Wiederkehrperiode

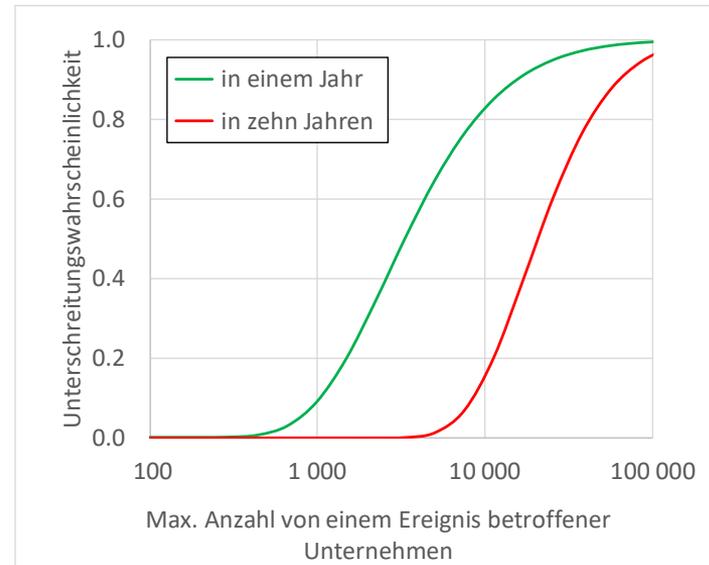
# Extremwertstatistik – Modell für Cyber Kumul

- Simulation verlinkter WKPs
- Differenzierung von  $Y$  möglich
- Einfache Simulation nach Schlather (2002)
- WKP → Schaden über Empfindlichkeitsfunktion
- Weitere Subprozesse (Schadenart) möglich
- Andere Anwendungsfelder, z.B. Natcat (Raschke, 2022)



# Extremwertstatistik – grobe Kalibrierung

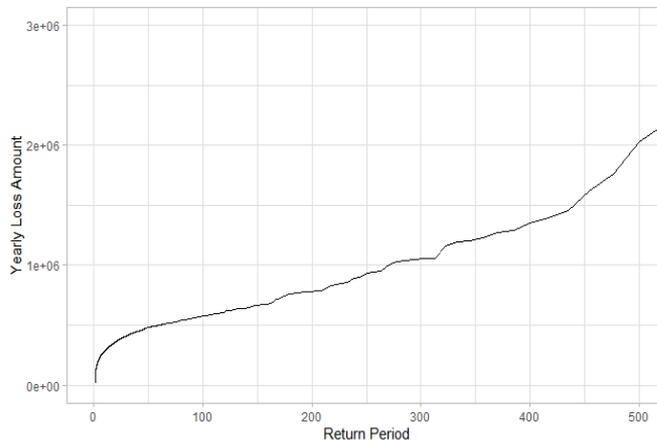
- Projektion der Modellannahmen auf versicherbares Marktportfolio: 370.000 Unternehmen in Deutschland
- Annahme: Cyber-Schaden ca. alle 5 Jahre pro Unternehmen (nach Dreißigacker et al, 2020)
- Verteilung der maximalen Anzahl an geschädigten Unternehmen pro Cyberereignis erscheint konservativ
- Zufallsvariable  $Y$  ist lognormalverteilt mit  $\sigma=3$ , 20% systemische Ereignisse



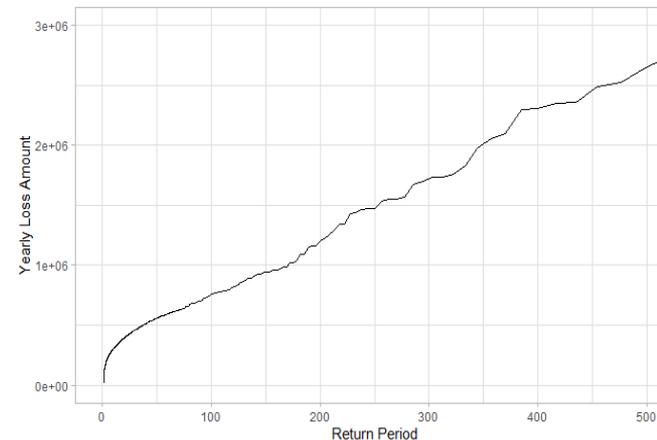
# Kumul des Portfoliobeispiels

- Simulation des Jahresgesamtschadens
- Vorsicht: Wegen unterschiedlicher Parametrisierung können Kurven nicht direkt verglichen werden.

Ansatz nach Scherer, M. & Zeller, G. (2021)



Ansatz nach Raschke (2022)



## Ausblick

- Die vorgestellten Ansätze stellen einen Ausgangspunkt zur (Weiter-) Entwicklung der **eigenen Modellierung** und zur **Plausibilisierung** der Ergebnisse aus kommerziellen Modellen dar.
- Gleichwohl besteht Entwicklungspotential bei verschiedenen Aspekten:
  - Abhängigkeit zwischen den Risiken bei systemischen Ereignissen
  - Verfeinerung der Kalibrierung, vor allem der systemischen Ereignisse
  - Berücksichtigung weiterer Risikofaktoren
  - Weiterentwicklung der Schadenhöhenverteilung
    - Modellierung des Tails
    - Bayessches Modell

## Fazit

- Modellkonzeption erfordert seitens der Aktuarinnen und Aktuare ein **breit gefächertes Methodenwissen** und eine kontinuierliche Erweiterung des eigenen Know-How.
- Die **Kalibrierung** der freien Parameter ist komplex. Neben den selbst erfassten Schäden sind Expertenschätzungen sowie die Kenntnisse der einschlägigen Literatur notwendig.
- Besondere Anforderungen an die Erstellung einer **geeigneten Datenhistorie**: Lange Datenhistorie auf aggregierter Ebene vs. Erfassung auf detaillierter Ebene
- Aufgrund der hohen Dynamik der Gefahr Cyber besteht erhöhte Anforderungen an die **Prozessorganisation** des Unternehmens und die **Modellgovernance**, schnell auf Änderungen zu reagieren.

# Literatur (Auszug)

- Aldasoro, I., Gambarcorta, L., Giudici, P., & Leach, T. (2020). BIS Working Papers No 865: *The drivers of cyber risk*.
- Coles, S. (2001). *An introduction to Statistical Modelling of Extreme Values*. Springer.
- Dreißigacker, A., von Skarczynski, B., & Wollinger, G. (2020). *Cyberangriffe gegen Unternehmen in Deutschland*. Im folgenden Risikobericht genannt.
- GDV. (April 2017). *Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung*.
- Raschke, M. (31. Januar 2022). *About the return period of a catastrophe*. Von Natural Hazards and Earth System Sciences: <https://nhess.copernicus.org/articles/22/245/2022/> abgerufen
- Scherer, M., & Zeller, G. (2021). *A Comprehensive Model for Cyber Risk Based on Marked Point Processes and Its Application to Insurance*. *European Actuarial Journal*.
- *Use Case der DAV AG Daten und Methoden zur Bewertung von Cyberrisiken (2022)*. Ergebnisbericht. Noch nicht veröffentlicht



# Agenda

1. AG Cyber – Überblick
2. Besonderheiten und Einfluss auf das Risikomanagement
3. Modellierung von Cyberrisiken – Use Case
4. Beispiel: Management von Cyber-Kumulen bei der Munich Re

# Munich Re: Cyber Kumul-Management

Jonas Becker  
DAV-Herbsttagung - Mainz, 14. November 2022



# Cyber als neue „man-made“ Gefahr

- Cyber hat sich erst in den vergangenen Jahren als **neue Gefahr** etabliert
- Einige **“prominente” Vorfälle** in den vergangenen Jahren
- Ereignisse stark durch **menschliches Verhalten** beeinflusst
- Angriffsmuster verändern und verbessern sich ständig, auch als Reaktion auf verbesserte IT-Sicherheit
- Digitalisierung sorgt für sich ständig **erhöhende Schadenpotentiale**
- Finanzielle Auswirkungen werden durch Änderungen in **rechtlichen** und **regulatorischen Bedingungen** beeinflusst

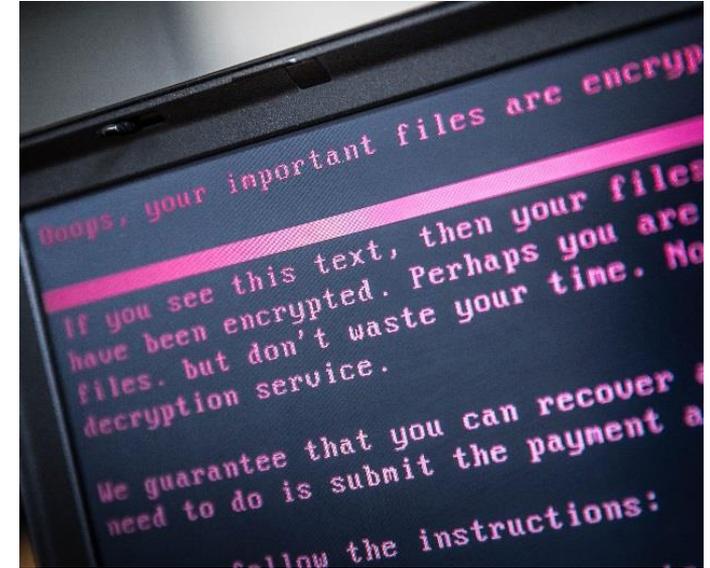


Dyn DDoS Attacke

## Beobachtete Kumul-Pfade

- Gemeinsame Software-Schwachstelle (Wannacry, NotPetya)
- Gemeinsame Hardware-Schwachstelle (Meltdown, Spectre)
- Ausfall eines IT-Dienstleisters (Amazon S3 Outage)
- Angriffe auf kritische Infrastruktur und/oder industrielle Kontrollsysteme

Ransomware-Wurm: NotPetya



▶ Signifikantes Kumul-Potential ergibt sich aus gemeinsamen Schwachstellen und der Störung oder dem Ausfall zentraler IT-Dienstleistungen und externen Netzwerken

## Kontrollierbares Risiko

Für die Teile des Cyber-Risikos, die als **beherrschbar** und damit **versicherbar** gehalten werden, wird die gesamte Exponierung der MR in einem **“Worst-Case“-Szenario** (1 in 1000 Jahre Ereignis) gemessen und mit dem vordefinierten Risikoappetit verglichen.

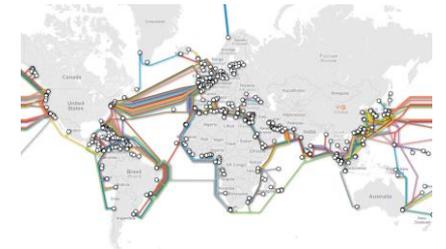
## Nicht kontrollierbares Risiko

- Andere Teile des Cyber-Risikos, insbesondere der **Infrastrukturausfall**, liegt **außerhalb des Risikoappetits**.
- **Cyber “Krieg”** oder eine massive Cyber-Eskalation eines Konflikts zwischen staatsnahen Akteuren schätzen wir als **nicht versicherbar** ein.

IoT DDoS Botnet



Internet & telecommunications infrastructure



Source: <https://www.submarinecablemap.com/>



## Anforderungen

- „Threat Intelligence“ (Akteure, Vektoren)
- System für die Bildung und Bewertung von Szenarien
- Wkt. für Cyber-Attacke und erfolgreicher Verteidigung
- Expertenmeinungen sowie Daten historischer Ereignisse
- Identifikation der „Single Points of Failure“ (SPOFs)
- Festlegung der Unternehmen, die von SPOFs abhängen
- Relevante Risikomerkmale der Unternehmen (Exposure, Schutzniveau)
- Kosten Komponenten aus Cyber-Schadendaten
- Erfassung der VN-Daten (Risiko-Eigenschaften, V-Bedingungen)
- Integration mit UW-Systemen

# Prozess zur Identifikation von Szenarien



- Die **Bewertung** und **Modellierung** von **Cyber-Kumulrisiken** ist in der gesamten Versicherungsindustrie in der **Anfangsphase**.
- Innerhalb der MR wurde die „Cyber Accumulation Expert Group“ (CAEG) gegründet. Diese besteht aus Experten für Cyber-Sicherheit, -Underwriting, -Schaden sowie Risikomanagern und Aktuaren.



- Zweck der „**Cyber Accumulation Landscape**“: strukturierter und wiederholbarer Prozess zur **Identifikation, Ordnung** und **Wahl** möglicher **Cyber Kumul-Szenarien**
- Dieser Prozess ermöglicht die Identifikation von Lücken in der Menge der aktuell modellierten Szenarien sowie die Priorisierung von Weiterentwicklungen.
- Die CAEG durchläuft den Prozess jährlich inkl. monatlicher Abstimmungen, in denen aktuelle Weiterentwicklungen diskutiert und die Aktualität der Szenarien sicherstellt.

# Cyber Kumul-Management

Cyber ist in definierten Grenzen versicherbar

Das Cyber-Risiko aus diesen Szenarien halten wir für modellierbar und damit versicherbar.

## IT Virus / Malware

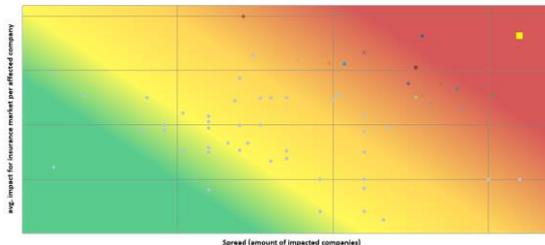
Globaler Ausbruch einer Schadsoftware, die sich selbst reproduziert und sich nicht zielgerichtet weiterverbreitet

## Cloud Outage

Service Provider Ausfall (bspw. Cloud), der zu weitreichenden Auswirkungen auf die Geschäftstätigkeit von Unternehmen führt

## Data Breach

Data Breach Attacke, die in großem Ausmaß mehrere Versicherte gleichzeitig trifft



Dieser Teil des Cyber-Risikos ist außerhalb des Risikoappetits.

## Infrastructure Failure

Ausfall physischer oder digitaler Infrastruktur wie Energieversorgung, Telekommunikation & Internet

### IT Virus / Malware

---

- **Vielfalt eingesetzter Software** (bspw. verschiedene Betriebssysteme, Versionen und unterschiedlicher Patch-Status).
- **Effektivität bestimmter Sicherheitskontrollen** (Anti-virus, Firewall, IT-Sicherheitstraining für Mitarbeiter, Netzwerk-trennung) verringert die Anzahl der von einer Schadsoftware betroffenen Unternehmen

### Cloud Outage

---

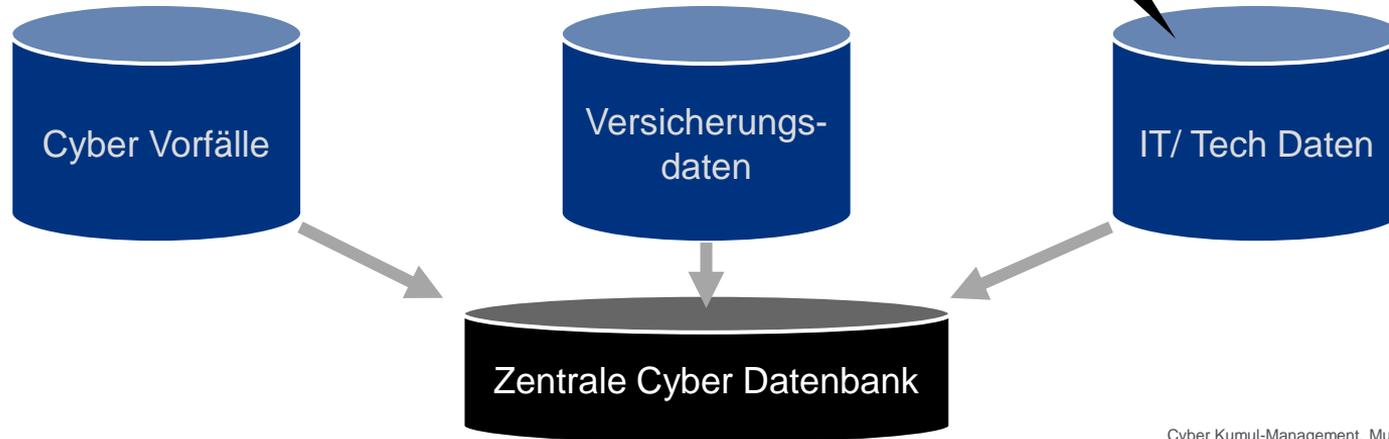
- **Nicht alle Unternehmen sind bei der Umsatz-Erzeugung stark abhängig von Cloud-Dienstleistern.**
- Es sind **unterschiedliche Cloud-Dienstleister** im Einsatz.
- Auf individueller Unternehmensebene kann es **risikomindernde Maßnahmen** geben, bspw. Offline-Arbeit oder Ausweichung auf alternativen Dienstleister

### Data Breach

---

- Grundsätzlich haben die Hacker die Möglichkeit, viele Unternehmen gleichzeitig zu penetrieren
- Wir gehen jedoch von **begrenzten Ressourcen** seitens der Hacker aus. Diese müssen priorisieren, bei welchen Unternehmen durch **individuellen Einsatz** versucht wird, sensible Daten abziehen

# Externe Cyber Datenquellen unabdingbar für das Verständnis der Exponierung



Vielen Dank!

