# MCC-Industrie-Risiken 2024

## Marktüberblick und aktuelle Situation in der Cyber-Versicherung

Dr. Sven Erichsen
Finlex GmbH

Köln den 10.04.2024

# Ähnlichkeiten mit der Feuer-Versicherung

„Cyber-Versicherung - ist ~~bald~~ schon so selbstverständlich wie eine Feuer-Versicherung?“



# Agenda

- Allgemeine Schadensituation
  - Statistiken zu Cyber-Schadenfälle
  - Aktuelle Schäden und Schadenbearbeitung
  - Treiben kriegerische Handlungen die Schadenentwicklung?
  - Datenschutzvorfälle
- Risikobewertung und -Standards - was setzt sich durch?
  - NIS 2 / DORA – Regulatorik nimmt Fahrt auf
  - Auswirkungen auf Anforderungen der Versicherer
  - Kumulrisiken – gibt es Sie?
- Markentwicklungen
  - Underwriting / Zeichnungsverhalten (Kapazitäten, Prämien, Risikoerfassung)
  - Neue Player – schon etabliert?

# Übersicht über Schadenursachen

## Externer Angriff/ Ransomware

- Angreifer verschaffen sich über Phishing/ Schwachstelle Zugriff auf IT-Systeme

## Externer Angriff/ DDoS

- Netz-Provider wird mit großer Anzahl von E-mails bombardiert

## Externer Betrug

- Ein gefälschtes E-Mail veranlasst eine Fehlüberweisung

# Übersicht über Schadenursachen

– die man nicht kennt

## Sabotage

- Verärgerter IT-Mitarbeiter klaut Daten
- Sabotage der IT-Landschaft durch Mitarbeiter

## Bedienfehler

- IT-Administrator konfiguriert ein Update falsch entgegen der Anweisung- Systemabsturz

## Software-Fehler

- Software-Fehler führt zu Fehlberechnungen

# Aktuelle Bedrohungslage

## Schäden einheitlich

- Erstaunliche Tatsache

## Schadenfrequenz steigt wieder

- Schadenfrequenz zwischen März 2022 und Ende 2022 gesunken – jetzt wieder am steigen

## Schäden verhinderbar

- Investition in Cyber-Sicherheit lohnt sich und sollte von VR besser honoriert werden

# Cyber-Claims

## Statistiken aus der Finlex Claims-Datenbank

### Schadenhöhe

- 70 % unter 100.000 €
- 25 % 100.000 € – 1 Mio. €
- 5 % über 1 Mio. €
- Durch frühe Hilfe bleiben Kosten gering.
- Wenige Großschäden treiben Schadenkosten dennoch in die Höhe.

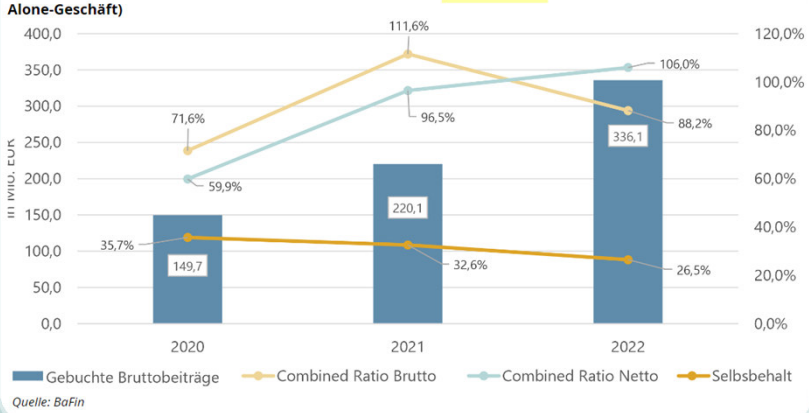
### Schließungsgründe

- 40 % Regulierung
- 25 % Hotlinehilfe
- 10 % unterhalb Selbstbehalts
- 20 % nicht versichert
- 5 % sonstige
- Hohe Regulierungsquote. ¼ der Cyber-Claims können mit Hilfe der Hotline gelöst werden.

# Cyber-Claims

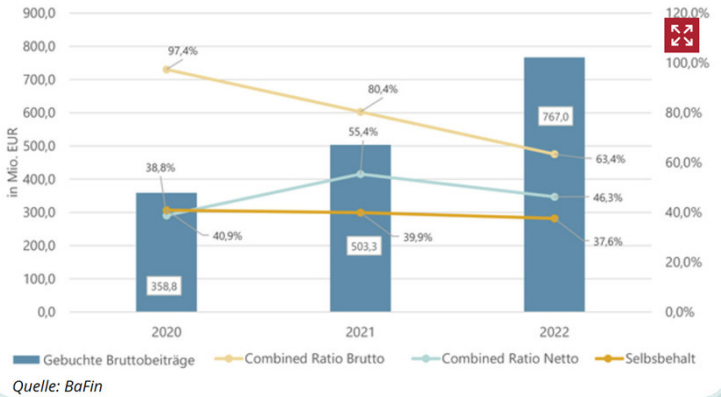
## BaFin – deutsches Geschäft defizitär

**Grafik 3: Entwicklung von Combined Ratio und Selbstbehalt in Deutschland (selbst abgeschlossenes Stand-Alone-Geschäft)**




*Quelle: BaFin*

**Grafik 4: Entwicklung von Combined Ratio und Selbstbehalt weltweit (selbst abgeschlossenes Stand-Alone- und Endorsement-Geschäft)**

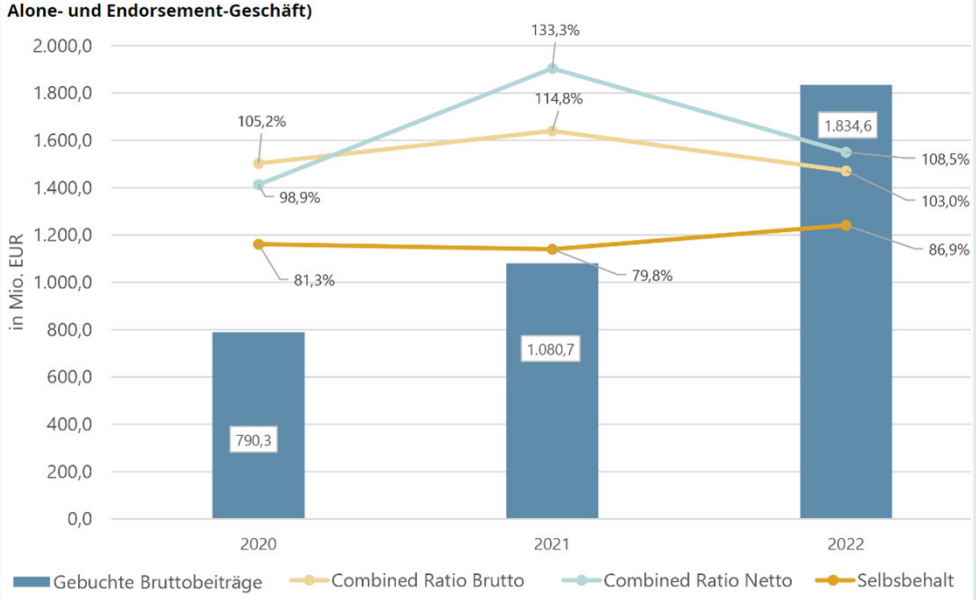



*Quelle: BaFin*

# Cyber-Claims

## BaFin – Rückversicherung verläuft schlechter

**Grafik 5: Entwicklung von Combined Ratio und Selbstbehalt weltweit (in Rückdeckung übernommenes Stand-Alone- und Endorsement-Geschäft)**




*Quelle: BaFin*

# NIS 2 | DORA

## Regulatorik nimmt (langsam) Fahrt auf

### NIS 2 (Network & Information Security Directive)

- Europ. Rechtsvorschrift, die Mindeststandards für die Cybersicherheit in Unternehmen in der EU festlegt.
- Ersetzt NIS-Richtline von 2016 (Fokus: KRITIS Unternehmen); erweiterter Anwendungsbereich und erweiterte Anforderungen zur Informationssicherheit unter NIS-2.
- Die NIS2-Richtlinie ist am 16.01.2023 in Kraft getreten und sollte bis September 2024 in nationales Recht überführt werden.
  Die Umsetzung in deutsches Recht (mittel NIS2-Umsetzungsgesetz) wird sich voraussichtlich verzögern und nicht mehr in 2024 erfolgen (Stand 03/2024) – ähnliches gilt für Dänemark und die Niederlande.

### DORA (Digital Operational Resilience Act)

- EU-Verordnung, die einheitliche Vorgaben für den Umgang mit Cyberrisiken und der Sicherheit von Informations- und Kommunikationstechnologie (IKT) im Finanzsektor vorgibt.
- Die EU-Verordnung ist am 17.01.2023 in Kraft getreten, die Institute und Unternehmen müssen den Anforderungen von DORA ab 17. Januar 2025 nachkommen

# NIS 2 | DORA

## Regulatorik nimmt (langsam) Fahrt auf

### NIS 2 (Network & Information Security Directive)

#### Anwendungsbereich:

| Sektoren mit hoher Kritikalität | Sonstige krtische Sektoren |
|---|---|
| Sektor Energie | Sektor Logistik: Post- und Kurierdienste |
| Sektor Transport und Verkehr | Sektor Abfallbewirtschaftung |
| Sektor Bankwesen | Sektor Chemie: Produktion, Herstellung und Handel mit chemischen Stoffen |
| Sektor Finanzmarktinfrastrukturen | Sektor Ernährung: Produktion, Verarbeitung und Vertrieb von Lebensmitteln |
| Sektor Gesundheitswesen | Sektor Verarbeitendes Gewerbe/Herstellung von Waren |
| Sektor Trinkwasser | Sektor Anbieter digitaler Dienste |
| Sektor Abwasser | Sektor Forschung |
| Sektor Digitale Infrastruktur | |
| Sektor Verwaltung von IKT-Diensten (B2B) | |
| Sektor öffentliche Verwaltung | |
| Sektor Weltraum | |

### DORA (Digital Operational Resilience Act)

#### Anwendungsbereich:

- So gut wie alle beaufsichtigten Institute und Unternehmen des europäischen Finanzsektors
- Auch IKT-Drittdienstleister, die den Finanzmarkt bedienen rücken in den Fokus.
  Verpflichtungen hinsichtlich Risikoüberwachung und Exit-Strategien für kritische/wichtige ausgelagerte Funktionen.

#### Impact:

- > 3.600 betroffene Unternehmen des Finanzsektors in Deutschland (> 20.000 in Europa)
- Indirekt unzählige Drittdienstleister die für diesen Sektor tätig sind

# NIS 2 | DORA

## Regulatorik nimmt (langsam) Fahrt auf

### NIS 2 (Network & Information Security Directive)

Inhalt:

- Angemessene Maßnahmen in den Bereichen Cyber-Risikomanagement, Lieferkettensicherheit, Business-Continuity-Management, Penetrationstests, Incident Response, Wiederherstellung
- Erhöhte Haftung der Geschäftsleitung der betroffenen Organisationen für die Einhaltung der Informationssicherheitsanforderungen
- Hohe Geldstrafen für Verstöße gegen die Cybersicherheitsvorschriften, die bis zu 10% des weltweiten Jahresumsatzes oder 20 Millionen Euro betragen können.
- Strenge Meldepflichten für Cyber-Vorfälle

### DORA (Digital Operational Resilience Act)

Inhalt:

- Sechs wesentliche Kernbereiche: IKT-Risikomanagement; Behandlung, Klassifizierung du Berichterstattung IKT-bezogener Vorfälle; Testen der digitalen operationellen Resilienz inkl. Threat-led Penetration Testing; Management des IKT-Drittparteienrisikos; Überwachungsrahmen für kritische IKT-Drittdienstleister; Vereinbarungen über den Austausch von Informationen sowie Cyberrisiken- und Notfallübungen
- Unternehmensleitung verantwortlich für das Management der IKT-Risiken, sowie für das Festlegen einer Strategie für digitale operationelle Resilienz, inkl. angemessenem Budget

# NIS 2 | DORA

## Regulatorik nimmt (langsam) Fahrt auf

- Mögliche Auswirkungen auf die Cyber-Versicherung
  - Konkrete Auswirkungen noch unklar – Detailgrad der Anforderungen und Überprüfung der Umsetzung.
  - Wünschenswert wäre: Erleichterte Erfassung von Risikoinformationen für von den Regulierungen betroffenen Unternehmen, da bereits in geeigneter Form im Unternehmen aufbereitet?
  - Einheitlicherer Blick auf die wichtigsten IT-Sicherheitsvorkehrung?
  - Höhere Management-Attention = höhere Nachfrage nach Cyberversicherung?

# Wesentliche Schlussfolgerungen der VR

## Anforderungen an die Cyber-Security

**Vorbemerkung**

Im Folgenden werden die technisch-organisatorischen Anforderungen zur Cyber-Security aufgeführt, wie wir sie von unseren Kunden erwarten. Sie können je nach Risiko bzw. Schutzbedarf im Einzelfall in unterschiedlichem Maße Anwendung finden. Es gilt dabei der Grundsatz der Angemessenheit. In jedem Fall sind gesetzliche Anforderungen (z. B. aus dem Datenschutzgesetz, dem Telemediengesetz oder dem IT-Sicherheitsgesetz) sowie behördliche Auflagen zu berücksichtigen. Verbindlich für den Versicherungsnehmer sind stets ausschließlich die Regelungen im Versicherungsschein und den Versicherungsbedingungen (z. B. Auflagen und Vorbehalte).

Die einzelnen Anforderungen können in einer Art **Präventionskette** eingeordnet werden:

| Nr. | Was? | Stichworte (nicht abschließend) |
|---|---|---|
| 1 | Schwachstellen von außen erkennen | Schwachstellen-/Port-Scan |
| 2 | Mensch / User | Awareness |
| 3 | Software-Schwachstellen | Asset-Management - Patchmanagement - kritische Patche - eol-Systeme |
| 4 | Lateral Movement | Segmentierung |
| 5 | Berechtigungen | Berechtigungsmanagement - Privilegierte Accounts – Fernzugriffe - MFA - MDM |
| 6 | Detektion und Reaktion | AV/EDR - NAC - IDS/IPS - Logfiles - SIEM/SOC |
| 7 | Backups | Backupkonzept - Schutz vor Manipulation (möglichst offline) - Restore-Tests |
| 8 | Vorbereitet sein | Notfallplan - Desaster Recovery - Übungen |
| 9 | Ständige Verbesserung | ISMS - Risikomanagement - BCM - Pen-Testing |

**1. Basis-Anforderungen für alle Unternehmensarten und -größen**

**1.1 Awareness-Maßnahmen**

Der Versicherungsnehmer führt für seine Mitarbeiter regelmäßig (mind. jährliche) Maßnahmen zur Aufrechterhaltung und Verbesserung des Bewusstseins (Awareness) zum sicheren Umgang mit Internet, IT und Daten durch, z. B. über Info-Mails, Schulungen und/oder Phishing-Simulationen.

# Cyber-Risiken

## Schutzmaßnahmen = Mindestanforderungen

Technische Komponenten:

- (Offline-) Back-up, Back-up, Back-up
- Regelmäßige und systematische Updates/Patches
- Multi-Faktor Authentifizierung
- Keine (nicht isolierten) Alt-Systeme
- Segmentierung
- Schutz Admin-Accounts
- Sicherheitskonzept
- ...

Organisatorische Komponenten :

- Verantwortungen etablieren
- Mitarbeiter schulen/Awareness-Maßnahmen
- Kunden- und Mitarbeiterdaten separat speichern.
- Notfallplanung

# Kumulrisiken (aus Sicht eines Rückversicherers)

## Überblick über die gängigsten Cyber Kumulszenarien

### Ausfall kritischer Infrastruktur :

- V.a. Internet, Telekommunikation, Stromversorgung
- Nicht versicherbar – heute Standard-Ausschluss in Cyberpolicen

### Wide-spread Virus:

- Nicht zielgerichteter bösartiger Angriff trifft Vielzahl von Unternehmen (bspw. aufgrund ungepatchter Systeme)
- Risikoselektion
- Internes Monitoring und Limit-Management seitens der Versicherer auf Basis hauseigener oder am Markt verfügbarer Risikomodelle

### Cloud Ausfall / Ausfall externer Dienstleister:

- Ausfall bedeutender externer Dienstleister mit Auswirkungen auf viele Versicherte
- Limitierte Deckungen (1st Tier only), Limit-Management, zukünftig ggf. erhöhte Informationsanforderungen

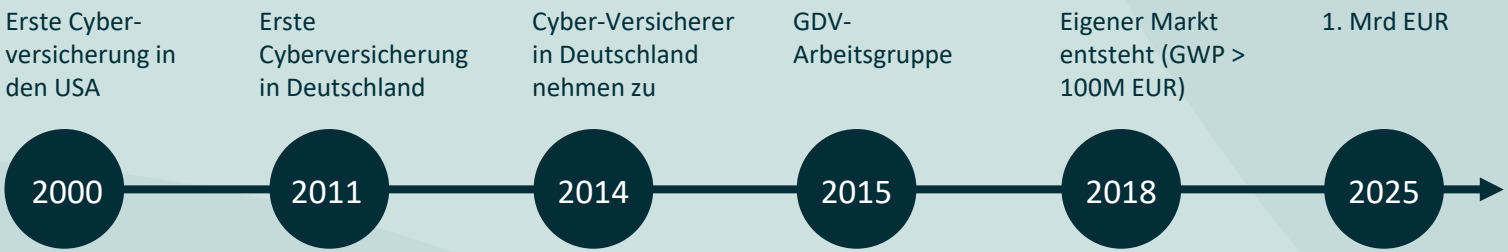
### Data Breach:

- Koordinierter Hackerangriff auf mehrere Versicherte (bspw. einer Branche) durch Ausnutzung gemeinsamer Schwachstelle(n)
- Vertrauliche/sensible Daten werden im großen Umfang gestohlen/veröffentlicht
- Internes Monitoring und Limit-Management

# Prämien der Cyberversicherung wachsen exponentiell

## Exponentielles Prämienwachstum

### Entwicklung der Cyber Versicherung 2000 – 2025




Quelle: Swiss Re Institute

- Unterschiedliche Bedingungswerke, Rahmenverträge, Antragsmodelle, eigene Abteilungen bei VR
- >40 Versicherer am dt. Markt, aber sehr unterschiedliche Ausrichtung
- Prämienvolumen in Deutschland 2024 > 500M EUR GWP (USA > 3,5Mrd USD)
- Am schnellsten wachsender Markt in der Versicherungsbranche

# Cyber-Risiken zum wiederholten Mal zum Top-Unternehmensrisiko gewählt

1 → **34%**
*2022: 1 (44%)*

**Cyber Vorfälle**

*(z. B. Internetkriminalität, Malware/ Ransomware, die Systemausfälle verursacht, Datenschutzverletzungen, Geldbußen und Strafen)*

2 → **34%**
*2022: 2 (42%)*

**Betriebsunterbrechung**

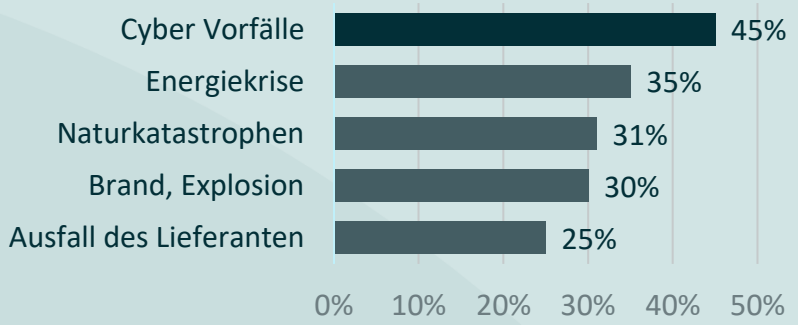
*(einschließlich Unterbrechung der Lieferkette)*

## Deutschland

**1. Betriebsunterbrechung** → 2. Cyber → 3. Energiekrise ↑

*Betriebsunterbrechungen sind nach wie vor das größte Risiko, während die Unternehmen auch über die Energiekrise besorgt sind*

**Welche Ursachen von Betriebsunterbrechungen fürchtet Ihr Unternehmen am meisten?**




*Quelle: Allianz Risk Barometer 2023 Total number of respondents: 917. Respondents could select more than one risk*



Quelle: Allianz Risk Barometer Report 2023

# Zoom-In: Deutscher Cyber-Versicherungsmarkt

**~400-500 Mio. €**
Prämien-volumen

Deutscher Cyber-Markt

**71**
Versicherer mit Cyber-Angeboten

**+ 18%**
in den letzten 2 Jahren

**20 - 113%**
Schadenquote

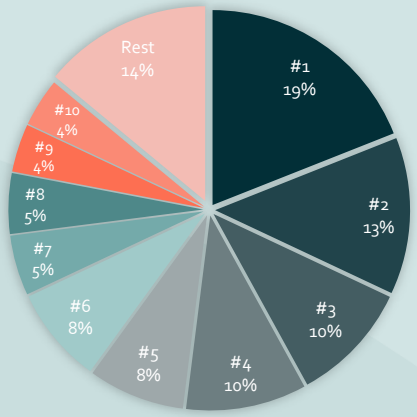
Extreme Volatilität unter den Top 10 Anbietern

**58 Mio. €**
Prämie

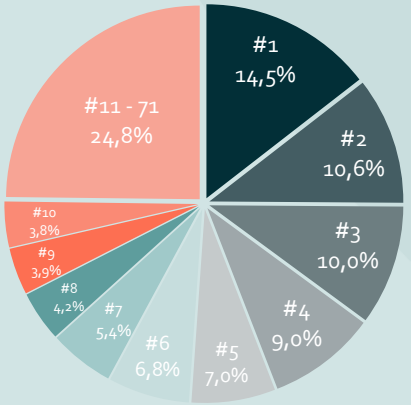
Prämienein-nahme des größten Cyber-VR in Deutschland

## Fokus Cyberpolice: Marktkonzentration gegenüber 2020 geringer

Marktanteile Dtl. 2020




Marktanteile Dtl. 2022




Quelle: Bundesamt für Finanzdienstleistungen



Quelle: BAFIN

# Die Grundstruktur der Cyber-Versicherung

## Haftpflicht

- Schadenersatzansprüche Dritter:
  - → Rechtschutzfunktion/ Anspruchsabwehr
  - → Befriedigung Berechtigter

## Eigenschäden

- Kosten für Information betroffener Dateninhaber nach Datenschutzvorfall
- Kosten IT Forensik
- Kosten Rechtsberatung
- Kosten PR-Berater

## Kostenpositionen

- Wiederherstellungskosten Daten/ Netzwerke
- Ertragsausfall durch Umsatzverluste
- Mehrkosten zur provisorischen Aufrechterhaltung oder beschleunigten Betriebswiederherstellung
- Erpressungsgelder und Vertragsstrafen
- Bedienfehler

Optional

- → Technische Probleme
- → Vertragsstrafen/ Pönalen
- → Betriebsunterbrechung infolge Cloud-Ausfall
- → Cyber-Diebstahl (Außentäter)

# Im Schadenfall fallen Kosten an für:

## Kostenpositionen:

- Kosten für Information betroffener Dateninhaber nach Datenschutzvorfall
- Kosten IT Forensik
- Kosten Rechtsberatung
- Kosten PR-Berater

## Eigenschäden:

- Wiederherstellungskosten Daten und Netzwerke
- Ertragsausfall durch Umsatzverluste
- Mehrkosten zur provisorischen Aufrechterhaltung oder beschleunigten Wiederherstellung des Betriebs
- Erpressungsgelder
- Vertragsstrafen
- Vermögensverluste
- Bußgelder

## Drittschäden:

- Schadenersatzansprüche Dritter:
  - Rechtschutzfunktion/ Anspruchsabwehr
  - Befriedigung berechtigten

# Bedingungswerke decken das Risiko schon gut ab

Enthaltene Komponenten schützen vor:

- Versicherungsschutz für zielgerichtete und nicht zielgerichtete Cyber-Angriffe
- Versicherungsschutz für Angriffe durch Außentäter (Hacker & Co) und Innentäter (Saboteure)
- Versicherungsschutz auch für Datenrechtsverletzungen außerhalb des Cyber-Raumes, z.B. durch das Abhandenkommen von Papierakten
- Inhaltliche und zeitliche Ausdehnung des versicherungstechnischen „Endes eines Betriebsunterbrechungsschadens" bis zum Wiedererreichen der regulären Einnahmen – erweiterte Haftzeiten möglich

- ABER: Bedingungswerke werden restriktiver (Kriegsklauseln, Mitversicherung IT-Dienstleister, Ransomware-Klausel

# Große Unterschiede im Wording

Technische Probleme

div. Vertragsstrafen

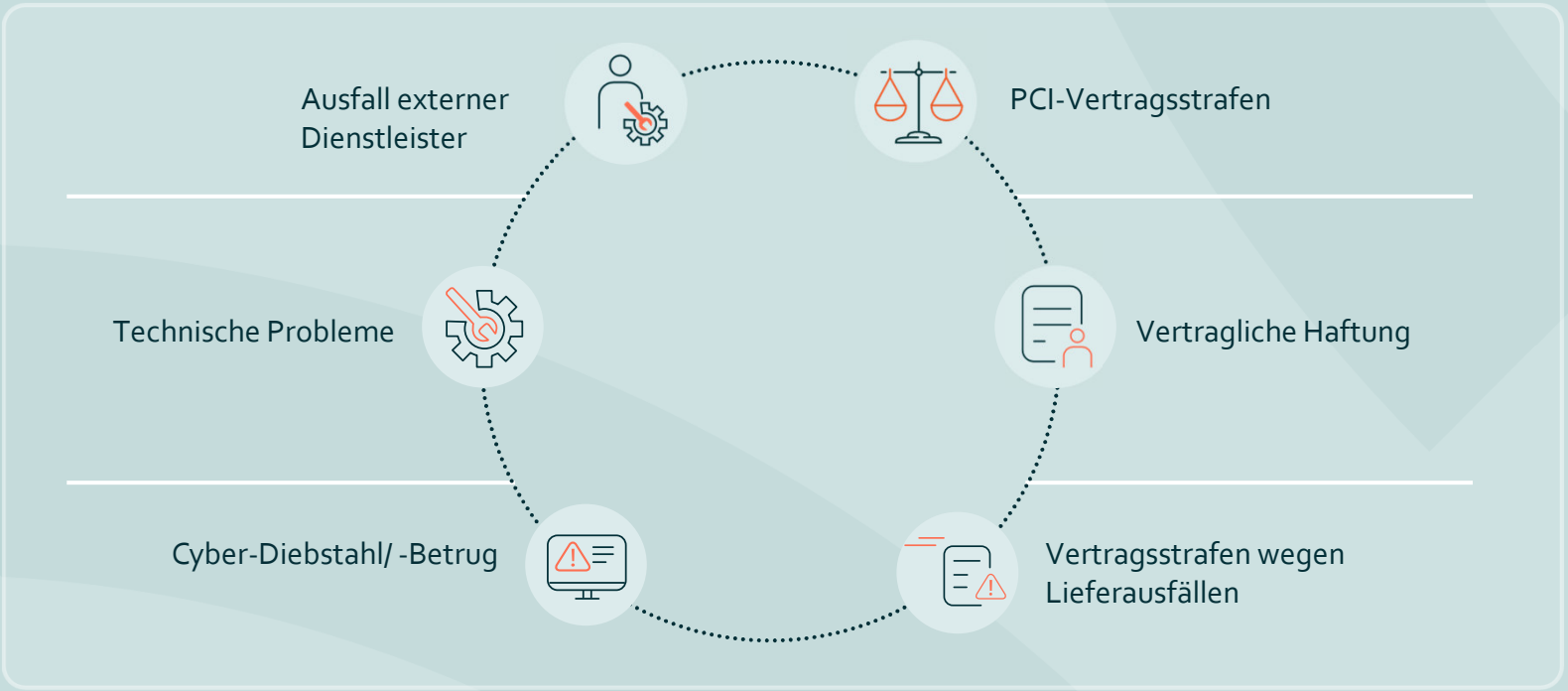
Assistance-Leistungn

BU infolge Ausfall externer IT-Dienstleister

Cyber Diebstahl*

* Kombination Cyber/VSV in einer Police jetzt möglich

# Zusatz-Deckungsbausteine






Achtung: Unterschiedliche Ausprägungen bei den einzelnen Versicherern


Vielen Dank für Ihre
Aufmerksamkeit!