MCC Fachkonferenz Cyber Risks

Düsseldorf, 25./26. April 2024

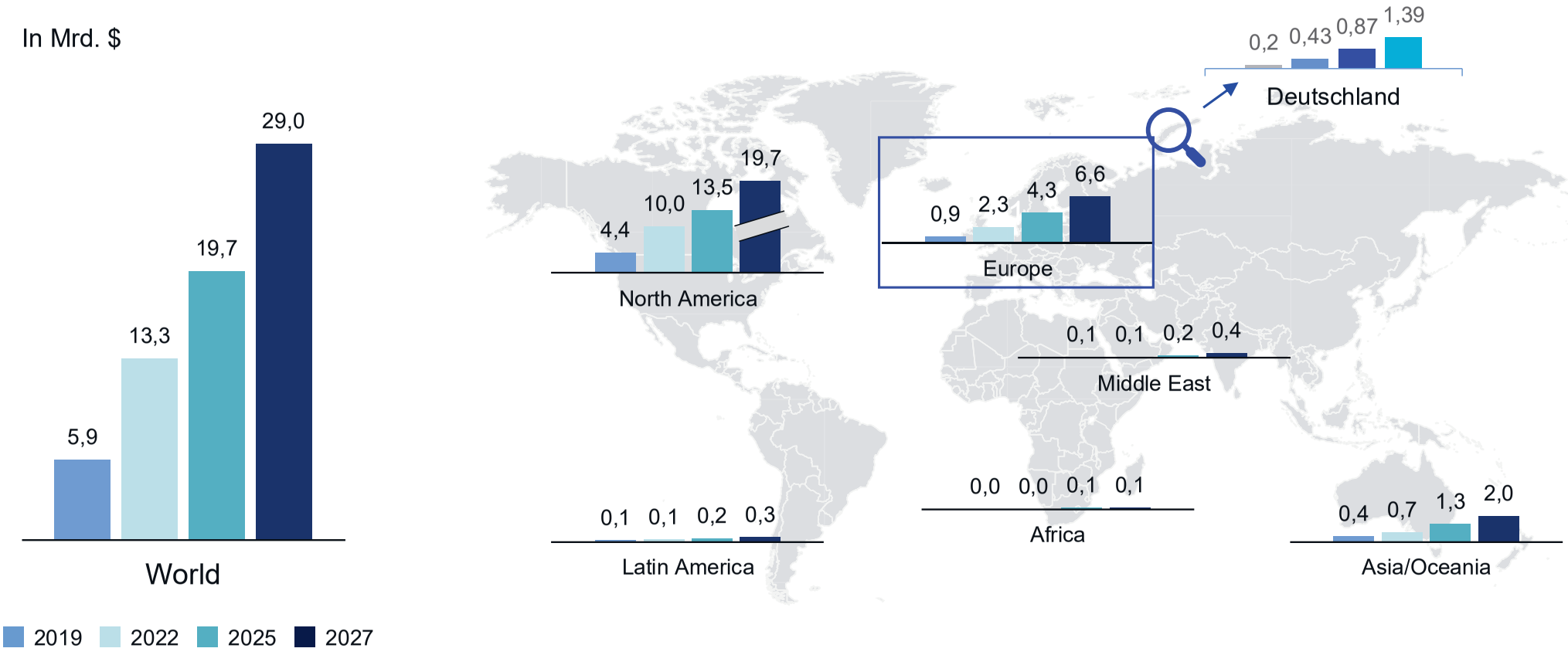
Munich RE

Quelle: blackdovfx / Getty Images

Ausblick auf die Cyber-Versicherung

Munich RE

Weltweite Cyber-Prämien steigen von ~$13 Mrd. USD (2022) auf gut $29 Mrd. USD (2027)

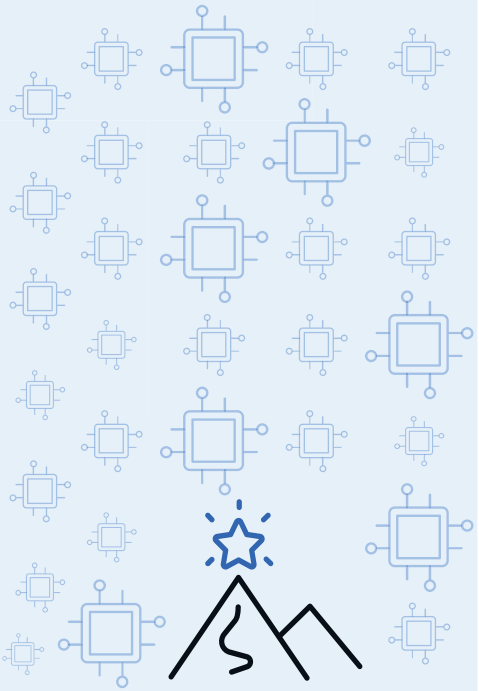


Quelle: Schätzungen von Munich Re, in USD

Aktuelle “Hot Topics” die wir als Munich Re aktiv adressieren

Munich RE

Allgemeine Herausforderungen des Cyber Markts



Nachhaltigkeit des Cyber Markts
(z.B. Services, Austausch mit Politik, Schadenmanagement)

Durchdringung am Markt
Anteil nicht versicherter Cyber-Risiken ist immer noch deutlich zu hoch → Lücke ökonomischer Schaden vs. versicherter Schaden

Trends in der Deckung und im Wording
(z.B. Systemversagen, Bedingte Betriebsunterbrechung)

Akkumulation und systemisches Risiko
(z.B. Modelle, Versicherbarkeit, Versicherungsausschluss)

Cyber-Krieg
(z.B. LMA Cyber Working Group, Pool-Lösungen)

Technologie und Versicherung
(z.B. Underwriting Tools, Data Analytics)

Cyber Resilienz/Sicherheit
In unserer aktuellen globalen Cyber-Umfrage geben 87 % der befragten Manager an, dass ihr Unternehmen nicht ausreichend gegen Cyber-Risiken geschützt ist. In Deutschland sogar 95%

Spezifische Herausforderungen von Erstversicherern

Risikoappetit und **Ambition** des Managements

Risikobewusstsein der Endkunden

Training & Selbstvertrauen der Vertriebsorganisationen

Zugang zu relevanten **Informationen** (am POS)

Unterstützung durch **Fachexperten**

Sorge vor **Falschberatung**

Rückblick

Die wichtigsten Verlusttreiber des Jahres 2023

Munich RE

01

Ransomware - Häufigkeit nimmt trotz einiger Erfolge der Strafverfolgungsbehörden weiter zu

- In H1/2023 **Anstieg der** veröffentlichten Ransomware-Angriffe **um 49%** im Vergleich zu H1/2022. In H2/2023 **Verdopplung zu H2/**2022.
- nur **1 von 5 Angriffen** weltweit wurde gemeldet.
- Datenexfiltration dominiert als Hebel für Erpressung mit 91 % (Blackfog)
- Big Game Hunting
- LOCKBIT, ALPHV und CL0P waren für über 42 % der Ransomware-Angriffe im Jahr 2023 verantwortlich. 32 neue Ransomware-Gruppen aufgetaucht (Cyble)

02

Business Email Compromise (BEC)

- Zwischen 2021 und 2023 waren 22.000 Opfer weltweit bei **Schäden von ca. 3 Mrd. USD** (Symantec)
- **Nigeria** als bedeutendster Absender: **46%** (Symantec)

03

Angriffe auf die Lieferkette - deutlicher Anstieg im Jahr 2023 mit einer starken Zunahme von Schadcode-Paketen

- **52 %** der Unternehmen weltweit in 2023 von Ransomware in Lieferketten betroffen (Trendmicro Threat Predictions 2024).
- MOVEit durch CL0P

04

Datenschutzverletzungen blieben auf einem hohen Niveau, wobei DarkBeam (3,8 Mrd. Datensätze) und der “Indian Council of Medical Research” (815 Mio. Kunden) die Statistiken anführten

Überall KI

Munich RE

- Angriffe werden zunehmend automatisiert, personalisiert und in großem Umfang verteilt, mit Tools, die Angreifern in allen Phasen eines Angriffs helfen.
- Die Entwicklung neuer bösartiger großer Sprachmodelle (LLMs) wie WormGPT wird auch weniger erfahrenen Akteuren helfen
- Bedrohungsakteure werden versuchen, LLMs zu "hacken", um Zugang zu sensiblen Informationen wie Trainingsdaten, Modellkonfigurationen, internen Algorithmen usw. zu erhalten.
- Auch Verteidiger werden KI nutzen (Erkennung, Reaktion und Zuordnung von Angreifern)
- Die weltweiten Ausgaben für KI-Lösungen werden bis 2027 auf über 500 Milliarden Dollar ansteigen (IDC)
- Fokus:
  Kundenbetrieb, Marketing und Vertrieb, Softwareentwicklung und F&E.

Auswirkungen auf die Cyberversicherung

- Bedrohungsakteure und Verteidiger werden zunehmend mit KI-Fähigkeiten ausgestattet sein
- Anstieg der Schadenhäufigkeit, aber bisher keine Änderung in unserer Kumulmodellierung
- Zunehmende Nutzung von KI in der Versicherungsbranche

Geopolitik & Nationalstaaten

Munich RE

> **Wiper werden zu einer Standardfähigkeit in allen Cyber-Arsenalen der Nationalstaaten"** (Google Cloud Cybersecurity Forecast 2024)

- Handlungen zur Beeinflussung wichtiger Wahlen. Hauptziel: USA, sowie die 40 wichtigen Wahlen im Jahr 2024, z. B. in der EU, Indien, Südkorea, Indonesien oder Mexiko
- Nationalstaaten werden zunehmend ihre eigenen großen Sprachmodelle (LLMs) entwickeln, einschließlich Modelle speziell für Malware

Cyberspionage, Intensivierung der Zero-Day-Forschung, zerstörerische Angriffe für militärische oder politische Ziele.

Anhaltende Konzentration UKR, Sammeln von Information und verstärkte Desinformationskampagnen.
Die Abwanderung von Fachkräften wird durch den Diebstahl geistigen Eigentums ausgeglichen.

Weiterhin finanzielle Motive (Kryptowährungs- und NFTs).
Neue Strategie mit Schwerpunkt auf Supply Chain-Angriffen.

Geopolitische Ambitionen, insbes. Rivalität mit Israel/Saudi-Arabien/USA.

Auswirkungen auf die Cyberversicherung

- Hohe Auswirkungen aufgrund der Komplexität der Akteure
- Wettlauf um Zero-Day-Schwachstellen
- Zusammenarbeit von Staaten mit kommerziellen Bedrohungsakteuren/APT-Gruppen zu Cyber Crime & Spionage
- Cyber-Wettrüsten beeinflusst Risiken in der Lieferkette

Ransomware-Trends

Munich RE

- Stärkere Ransomware-Gruppen, kürzere Verweildauer und „Prompt“-Injection-Taktiken. **AI Ransomware-as-a-Service** (RaaS)-Modelle werden auf dem Markt wettbewerbsfähiger sein
- Hohes Maß an **Automatisierung** und **Individualisierung** mit einem Anstieg der "kreativen E-Mail-Erpressung" in allen Sprachen
- Diversifizierung wird Komplexität erhöhen
- Verlagerung von Daten für Erpressungen zu **verwertbaren Daten für den Verkauf** (z. B. Schwachstellen oder identifizierbare Informationen), insbesondere wenn Verhandlungen erfolglos sind
- Ransomware wird seine Opfer bis 2031 jährlich ca. **265 Mrd. USD** kosten
  (Cybersecurity Ventures)

Auswirkungen auf die Cyberversicherung

- Ransomware wird weiterhin der der größte Risiko- und Schadentreiber sein
- Technische Fortschritte und Taktiken deuten auf eine komplexere und schädlichere Ransomware-Landschaft hin
- Der derzeitige Trend der zunehmenden Ransomware-Verluste wird sich 2024 wahrscheinlich fortsetzen

Kompromittierung von Geschäfts-E-Mails (BEC) und Kompromittierung von Geschäftskommunikation (BCC)

Munich RE

- Weiterentwicklung durch KI- und Deepfake-Technologien
- Überzeugende Fake-Anrufe, die aktiv mit den Empfängern interagieren, und gefälschte Fotos und Videos werden auf breiter Basis verfügbar sein

  Somit: Unterscheidung zwischen rechtmäßigen und betrügerischen Anfragen wird schwieriger

Sowohl hohe **finanzielle Verluste** als auch
Erosion von **Vertrauen** und Ansehen

Auswirkungen auf die Cyberversicherung

- Hohe Schadenserwartung im Bereich der BEC/BCC-Angriffe mit hohen Dunkelziffern
- Akteure mit bisher geringem Entwicklungsstand könnten sich in Zukunft leichter weiterentwickeln

Gestiegene Bedrohungslage bei Supply Chain & OT

Munich RE

Supply Chain

- Angriffe auf die Lieferkette als Dienstleistung: Akteure kaufen sich Zugang zu Lieferketten und zielen auf kleinere Unternehmen, um in große Firmen einzudringen
- Anstieg der Schäden durch Angriffe auf die Software-Lieferkette entstehen: 138 Milliarden USD bis 2031, gegenüber 60 Milliarden USD im Jahr 2025 und 46 Milliarden USD im Jahr 2023 (Cybersecurity Ventures)

OT/ IoT

- Bis 2025 wird es 41,6 Milliarden angeschlossene IoT-Geräte geben, die 79,4 Zettabyte (ZB) an Daten erzeugen (IDC, "Internet of Things Ecosystem and Trends").
- Trend zu *Edge*-Geräten
- Muster:
  Mehr Geräte + mehr Kritikalität = höhere Exponierung

Auswirkungen auf die Cyberversicherung

- Mehrere Schadensszenarien möglich: BI, CBI, Datenschutzverletzungen
- Digitale Flaschenhälse und systemische Risiken werden zunehmen - z. B. Cloud-Dienste
- Schwierige Bewertung des Risikos von Drittparteien

Regulierung von Daten, Datenschutz und Cybersicherheit

Munich RE

- Nur wenige (10%) Unternehmen haben den Datenschutz bisher erfolgreich als Wettbewerbsvorteil genutzt (Gartner)
- 5G als treibende Kraft: bis 2028 wird der Anteil von 5G am mobilen Datenverkehr auf 66% ansteigen; Videodatenverkehr mit weiter steigender Dominanz von derzeit 71% auf 80% des mobilen Datenverkehrs im 2028 (Ericom).
- Gesetzgebungsaktivitäten werden von KI-Governance und -regulierung dominiert. Es wird Normen für KI geben, diese verfolgen aber ein schwer greifbares und sich veränderndes Ziel.

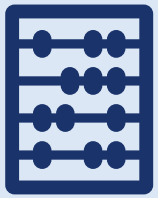
Auswirkungen auf die Cyberversicherung

- Steigende Haftung für die Datenverantwortlichen
- Mehr Regulierung, Vorschriften und Anforderungen an die Berichterstattung & Offenlegung von Verstößen - z. B. NIS2, SEC, DORA.
- Elemente von Drittanbietern werden weiterhin gefragt sein und ein wichtiger Schadentreiber

Munich Re Cyber Kumul-Management

Cyber ist in definierten Grenzen versicherbar

Munich RE



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

- IT Virus / Malware
- Cloud-Ausfall
- Data Breach

Dieser Teil des Cyber-Risikos ist außerhalb des Risikoappetits.

- Infrastruktur-Ausfall
- **Cyber Krieg**

PML aus den Szenarien sowie weitere Exposure KPIs maßgeblich für angebotene Jahreskapazitäten

Ausschluss von Szenarien notwendig

Cyber ist versicherbar, aber die Grenzen sind identifiziert - es gibt nicht-versicherbare Akkumulationsszenarien

Munich RE

Versicherbar

Virus/Malware

Globale Ausbreitung von weit verbreiteter, nicht zielgerichteter, sich selbst reproduzierender Malware

Datenschutz-verletzung

Mehrere Versicherte sind von einem groß angelegten Angriff auf ihre Daten betroffen

Das Computersystem des Versicherten

Interne Computersysteme, die vom Versicherten betrieben oder direkt kontrolliert werden

Kann als IT-Outsourcing-Anbieter gedeckt werden

IT Service Provider Ausfall

Großflächige Ausfälle von Diensten wie der Cloud, die weitreichende Auswirkungen auf das Geschäft haben

Cloud Computing
(SaaS, PaaS, IaaS)

- E-Mail-Dienstleister
- Webhosting-Anbieter
- Cloud-Anbieter

Nicht versicherbar

Ausfall von (kritischer) Infrastruktur

- Elektrische Energieversorgung
- Telekommunikation und Internet
  - Infrastruktur
  - Software-Ausfall

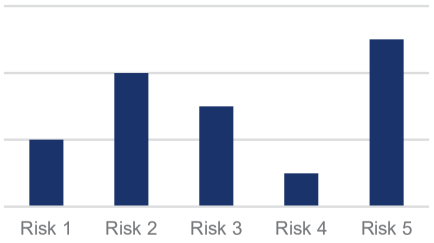
Internet-Dienste

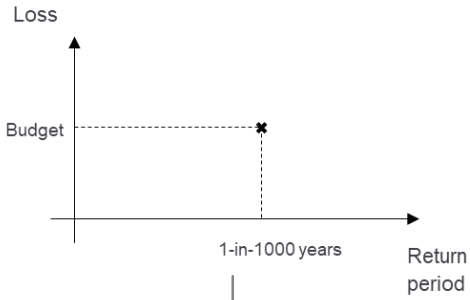
- Internet-Service Provider (ISPs)
- DNS[1]-Dienstleister
- Internet-Knoten-Anbieter

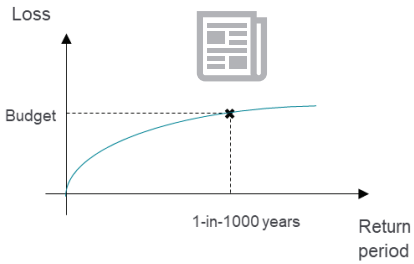
1) DNS = Domain Name System

Cyber Accumulation Quantification Timeline

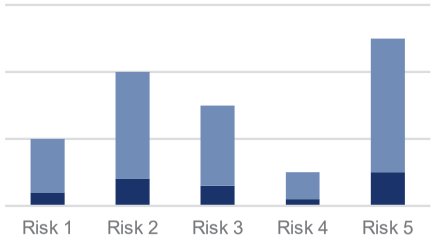
Munich RE

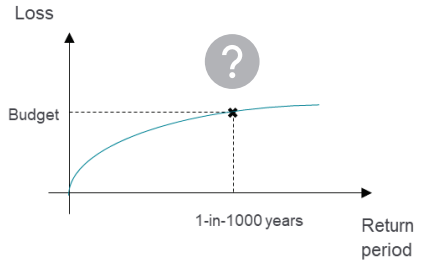






Full limit	Deterministic (percentage)	Deterministic (one event)	Probabilistic (simulation)	Probabilistic (event set)





Cyber Kumul-Szenarien

Limitierende Faktoren

Munich RE

IT Virus / Malware

- Vielfalt eingesetzter Software (bspw. verschiedene Betriebssysteme, Versionen und unterschiedlicher Patch-Status).
- Effektivität bestimmter Sicherheitskontrollen (Anti-virus, Firewall, IT-Sicherheitstraining für Mitarbeiter, Netwerktrennung) 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 anzugreifen.
- Wir gehen jedoch von begrenzten Ressourcen seitens der Hacker aus. Diese müssen priorisieren, bei welchen Unternehmen durch individuellen Einsatz versucht wird, sensible Daten abzuziehen

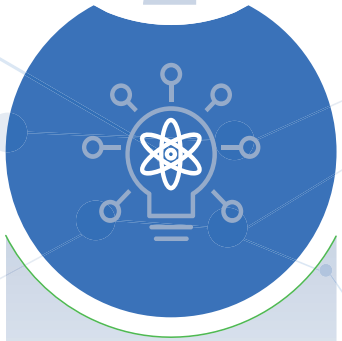
Zusammengefasst

Munich RE

1

Großes Wachstums-potenzial von Cyberversicher-ungen

2



Versicherbarkeit der meisten Cyber-Risiken gegeben

3

Immense Bedeutung von IT-Schutz-maßnahmen

4

Versicherung als Kombination aus Risikotransfer und Services

Vielen Dank!

Munich RE

2017 2018

2019 2020

2021 2022

2023

Munich RE

Cyber-Rückversicherer des Jahres

Vielen Dank!

Munich RE

Quelle: blackdovfx / Getty Images