Aktueller Stand Cybermarkt

März 2024

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)

3 → 25%
2022: 10 (11%)

Makroökonomische Entwicklungen

(z. B. Inflation, Deflation, Geldpolitik, Sparprogramme)

5 → 19%
2022: 5 (19%)

Änderungen von Gesetzen und Vorschriften

(z. B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Zerfall der Eurozone)

6 ↓ 19%
2022: 3 (25%)

Naturkatastrophen

(z. B. Sturm, Überschwemmung, Erdbeben, Waldbrand, extreme Wetterereignisse)

2 → 34%
2022: 2 (42%)

Betriebsunterbrechung

(einschließlich Unterbrechung der Lieferkette)

4 ↑22%
Neu

Energiekrise

(z. B. Versorgungsengpässe, Preisschwankungen)

7 → 17%
2022: 6 (17%)

Klimawandel

(z. B. physische, operative und finanzielle Risiken infolge der globalen Erwärmung)

8 ↑ 14%
2022: 9 (13%)

Arbeitskräftemangel

9 ↓ 14%
2022: 7 (17%)

Brand, Explosion

10 ↑ 13%
2022: 13 (9%)

Politische Risiken und Gewalt

(z. B. politische Instabilität, Krieg, Terrorismus, innere Unruhen, Streiks, Aufruhr)

Quelle: Allianz Risk Barometer Report 2023

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

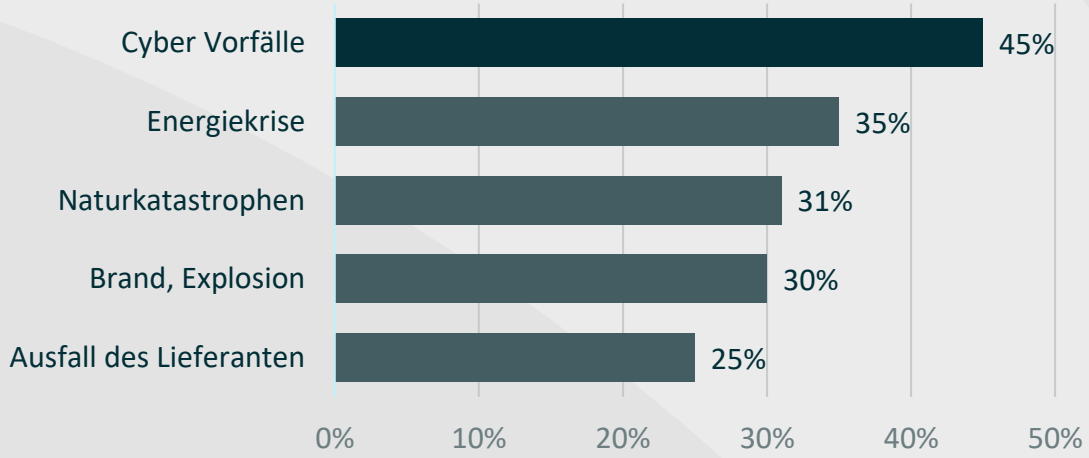
(einschließlich Unterbrechung der Lieferkette)

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

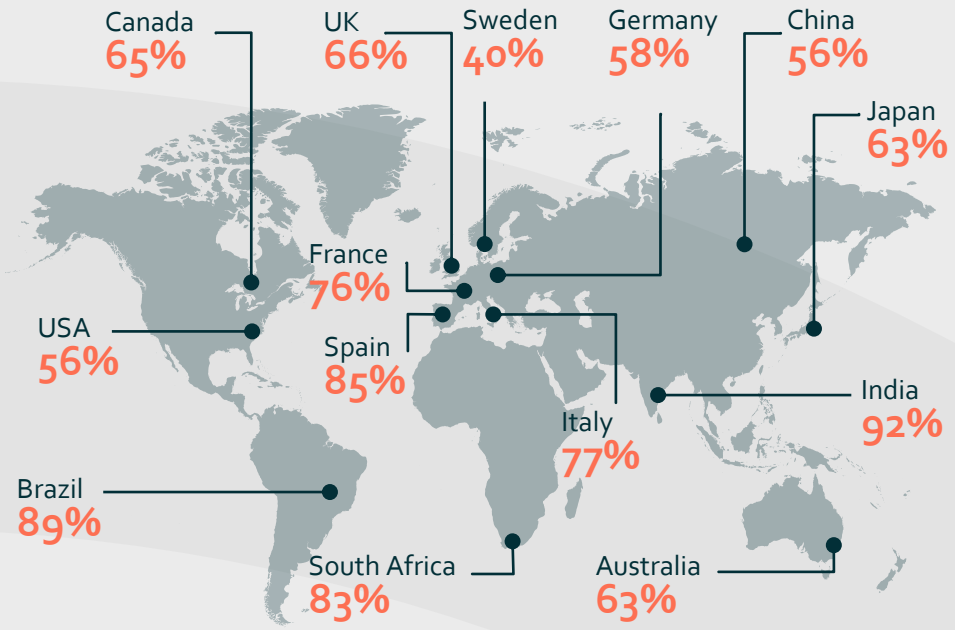
Quelle: Allianz Risk Barometer Report 2023

Cyber-Bedrohungslage

Die Auswirkung auf Unternehmen

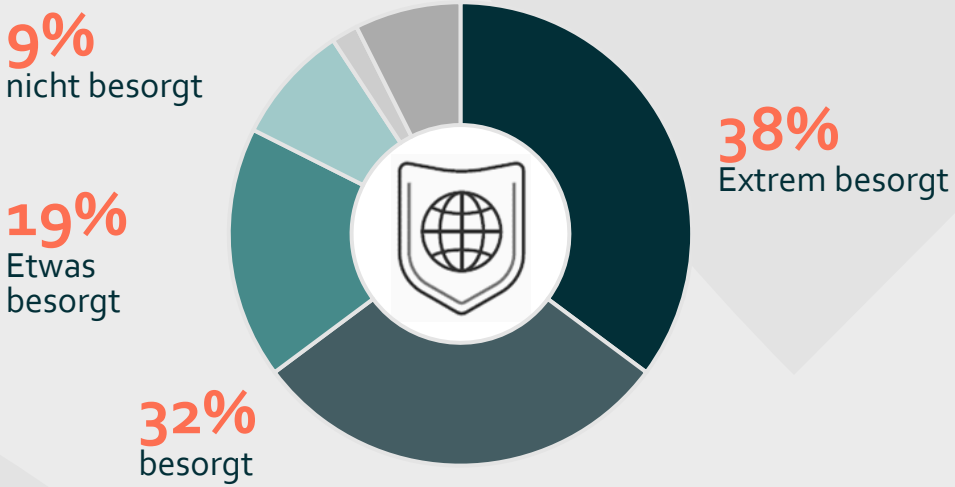
Nach Ländern:

Wie besorgt sind Sie hinsichtlich eines möglichen Angriffs auf Ihr Unternehmen?



Fokus auf KMUs (weltweit)

Wie besorgt sind Sie hinsichtlich eines möglichen Angriffs auf Ihr Unternehmen?



Die Anzahl der Teilnehmer auf C-Level Ebene, die "äußerst besorgt" sind, ist von 30 auf 38 % gestiegen.

Cyber Bedrohungslage

Zahlen & Fakten

Cyberkriminalität

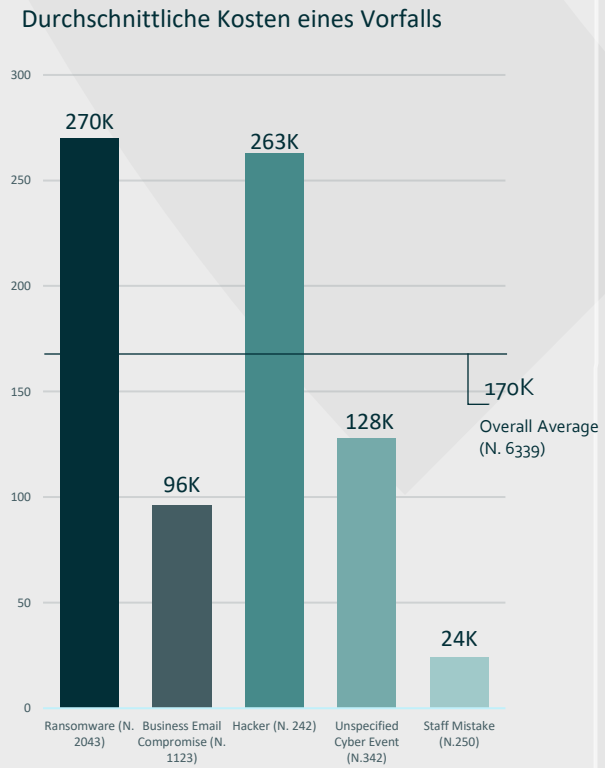
Beträchtlicher Anstieg der wirtschafltichen Kosten der Cyberkriminalität in den nächsten 5 Jahren erwartet – von **$8.44 Billionen** in 2022 auf **$11 Billionen** in 2023, bis hin zu **$23.84 Billionen** bis 2027.

www.statista.com

Top 5 Schadenursachen für KMUs

Ransomware sowohl Hauptschadenursache, als auch Auslöser für die höchsten Durchschnittskosten.

NETDILIGENCE® Cyber claims study 2022 report



Cyberkriminalität als **führende Schadenursache** verantwortlich für **76.8%** aller Fälle in 2022.
Cyber Spionage mit **10.4%** an zweiter Stelle – untermauert die Auswirkungen des Kriegs in der Ukraine.

Hackmageddon 2022 Cyber Attack Statistics

Dauer eines Cyber Vorfalls

Im Schnitt dauert es etwa **9 Monate** einen Cyber Vorfall zu erkennen und einzudämmen.

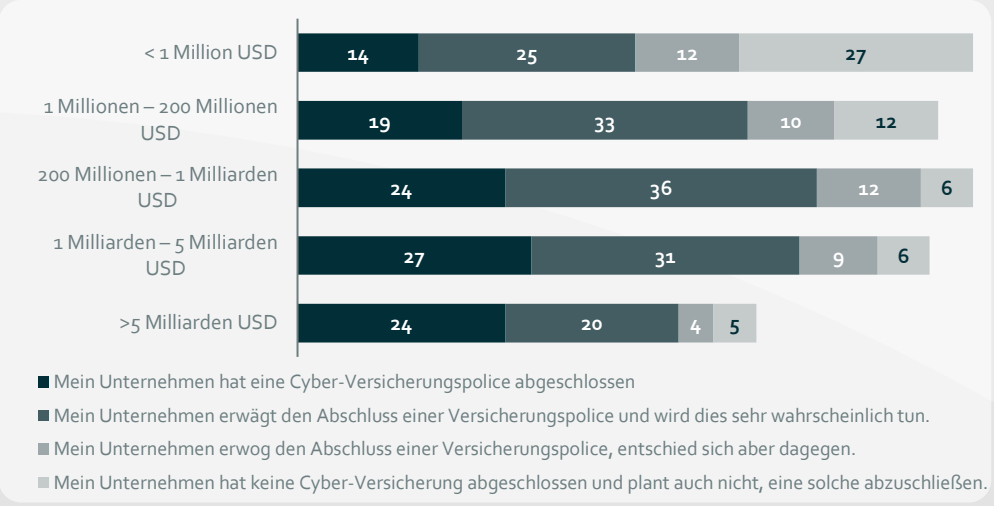
IBM Cost of a Data Breach Report 2022

Cyber Bedrohungslage

Nachfrage nach Cyber Versicherungen

Nachfrage nach Cyber Versicherung

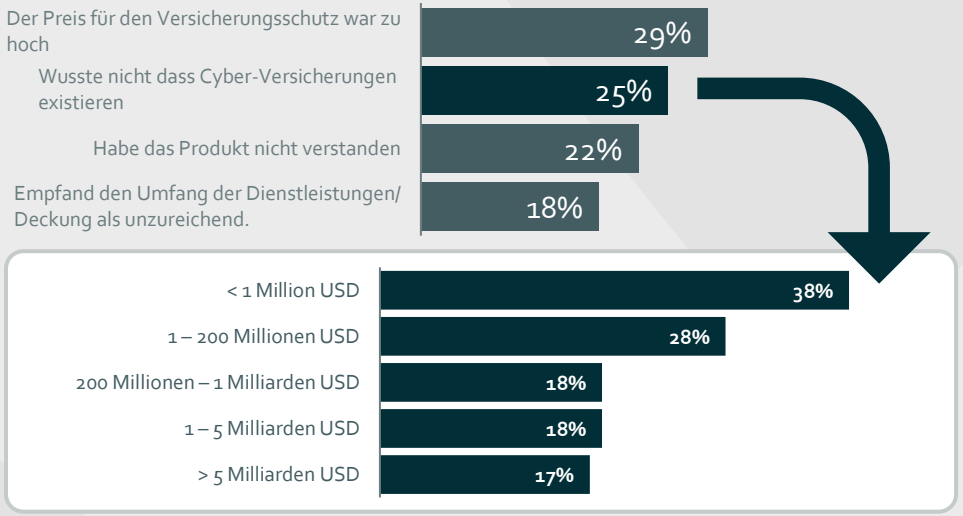
Unternehmen, die von Internetkriminalität betroffen sind
Würden Sie eine Cyber-Versicherung für Ihr Unternehmen abschließen?



Anteil an **Erstkäufern** wird vermutlich in allen Segmenten zunehmen.

Hindernisse für den Abschluss

Warum hat Ihr Unternehmen keine Cyberversicherung abgeschlossen? Global (C-Level)

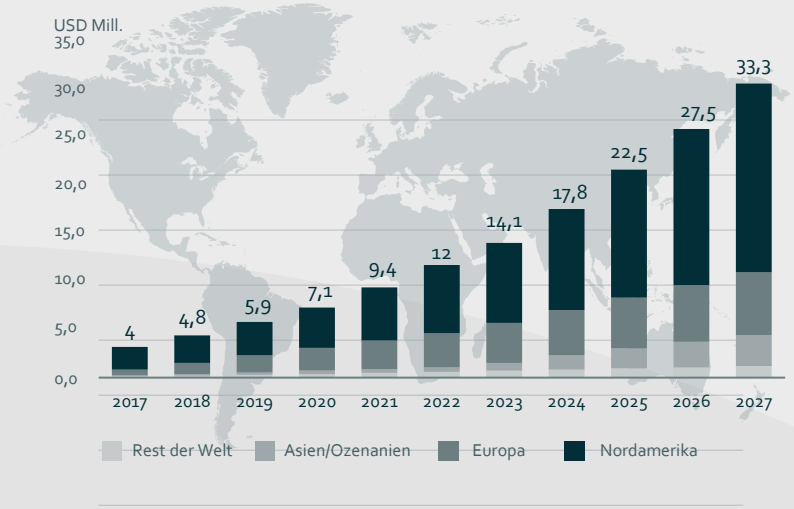


Vor allem bei **kleineren Unternehmen** (< $ 200 Mio. Umsatz p.a.) bedarf es weiterhin **erhöhten Beratungsaufwand** hinsichtlich des Produktangebotes.

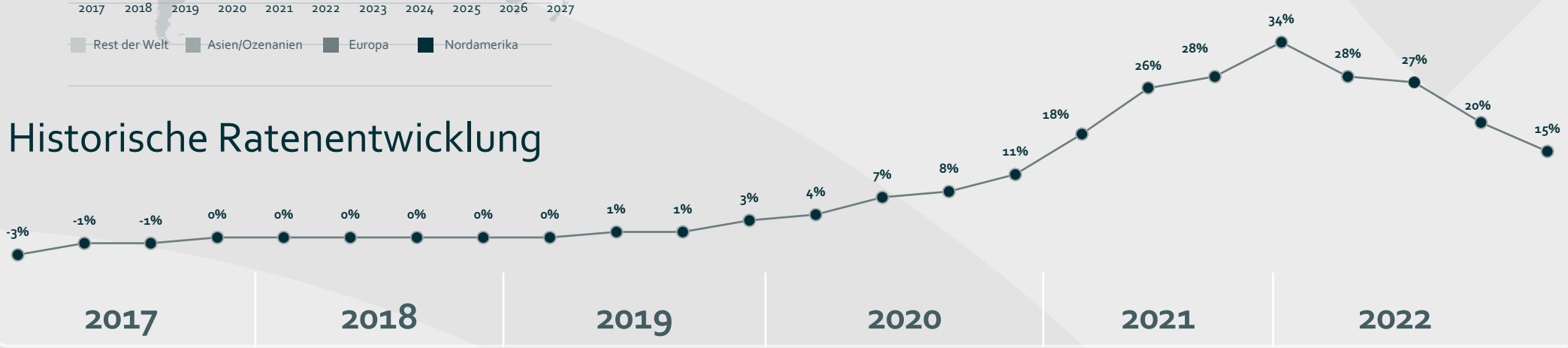
Quelle: Munich Re Global Cyber Risk and Insurance Survey 2022

Wo steht der Cyber-Versicherungsmarkt aktuell?

Entwicklung der weltweiten Cyber Prämie



Historische Ratenentwicklung



Quelle: The Council of Insurance Agents & Brokers - Commercial Property & Casualty Market Index Q4/2022

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

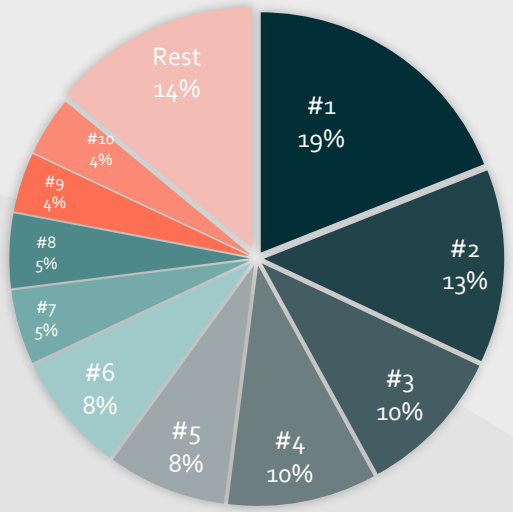
Extreme Volatilität unter den Top 10 Anbietern

58 Mio. €
Prämie

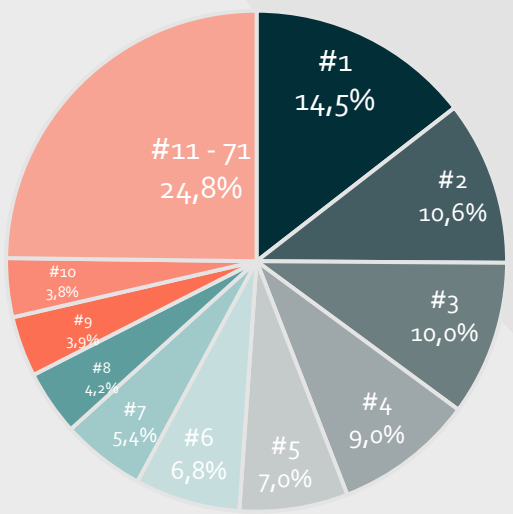
Prämienein-nahme des größten Cyber-VR in Deutschland

Fokus Cyberpolice: Marktkonzentration gegenüber 2020 geringer

Marktanteile Dtl. 2020



Marktanteile Dtl. 2022



Quelle: Bundesamt für Finanzdienstleistungen

Quelle: BAFIN

Cyber Versicherung – nur für große und mittelständische Unternehmen relevant?

Großer Irrglaube!

Zahl der Cyberattacken auf kleine- und mittelständische Unternehmen steigt kontinuierlich an

Kleine Unternehmen aufgrund unzureichender IT-Sicherheit als „low hanging fruit“ für Angreifer

Fehlende Inhouse-Ressourcen & fehlendes Expertennetzwerk, um schnell und effizient auf Angriff zu reagieren

Angriff auf kleine Unternehmen als Einfallstor für größere Kooperationspartner

Auswirkungen eine Cyberangriffs für kleine Unternehmen oft viel verheerender als für große Unternehmen

Cyber-Versicherung und ihre Hürden

Schlechte IT-Infrastruktur

Beispielhaft:

- Altsysteme
- Schlechte Datensicherung
- Schlechtes Backup-Konzept
- Fehlendes Patch-Management

Fehlendes Verständnis

- Neue Bedrohungsszenarien
- Unterschätztes Risikobewusstsein des eigenen Unternehmens

Exponiertes Risiko

- Branche mit hohem Schadenpotenzial
- Viele personenbezogene Daten
- Hoher E-Commerce Umsatz
- Komplexe Unternehmensstruktur

Cyber-Markt Trends – was ist zu erwarten?

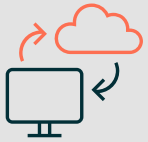
Trotz des jüngsten Marktwachstums ist die Versicherungslücke weiterhin groß, was weiteres Wachstum erwarten lässt.

Prämienstagnation, Preissteigerungen deutlich verlangsamt.
Erneuter Anstieg der Kapazität; Rückkehr zu Vor-Hartmarkt Limiten scheint möglich

Risikoqualität weiterhin im Fokus der Versicherer, kein "Softmarkt" hinsichtlich technischer Voraussetzungen und Kontrollen.

Systemische Risiken bleiben eine Herausforderung für die Nachhaltigkeit des Produktes; mehr Klarheit bzgl. Sprache, risikobasiertem Underwriting und Risikoquantifizierung.

Weiterhin starker Fokus auf passenden Cyber-Kriegsausschlüssen.



Verstärkter Fokus auf Lieferkettenrisiko, v.a. für Großkunden.

Relevanz der verbesserten Datenerfassung für (Rück-) Versicherer, um Pricing- und Kumulmodelle stetig weiterzuentwickeln.

Ransomware weiterhin führende Schadenursache. Angriffe auf Lieferketten und Komprimittierung von Geschäfts-Emails stellen weitere Risiken dar.

Auswirkung neuer Richtlinien (z.B. NIS-2) noch abzuwarten.

Quelle: Munich Re Global Cyber Risk and Insurance Survey 2022