



ASSICONSULT

---

INTERNATIONAL INSURANCE BROKER

**CYBER RISK**

**IHR SCHUTZ IM DIGITALEN ZEITALTER**

# WER SOLLTE EINE CYBER RISK-VERSICHERUNG IN BETRACHT ZIEHEN?

Cyber-Risiken kennen keine Ausnahmen – Schutz ist für alle unverzichtbar

Wenn es um Cyberkriminalität geht, lassen sich die Nutzer von IT-Systemen in zwei Kategorien einteilen:

- **diejenigen, die bereits Opfer eines Angriffs geworden sind**
- **und diejenigen, die noch angegriffen werden**

In einer Zeit, in der Cyberangriffe immer ausgefeilter werden, ist sie für **Unternehmen jeder Größe ein wichtiger Baustein im Risikomanagement.**



# WOZU EINE CYBER RISK-VERSICHERUNG/DECKUNG?

Eine Cyber Risk Versicherung ist kein Ersatz für IT-Sicherheitsmaßnahmen, sondern eine Ergänzung, die finanzielle und organisatorische Risiken abdeckt

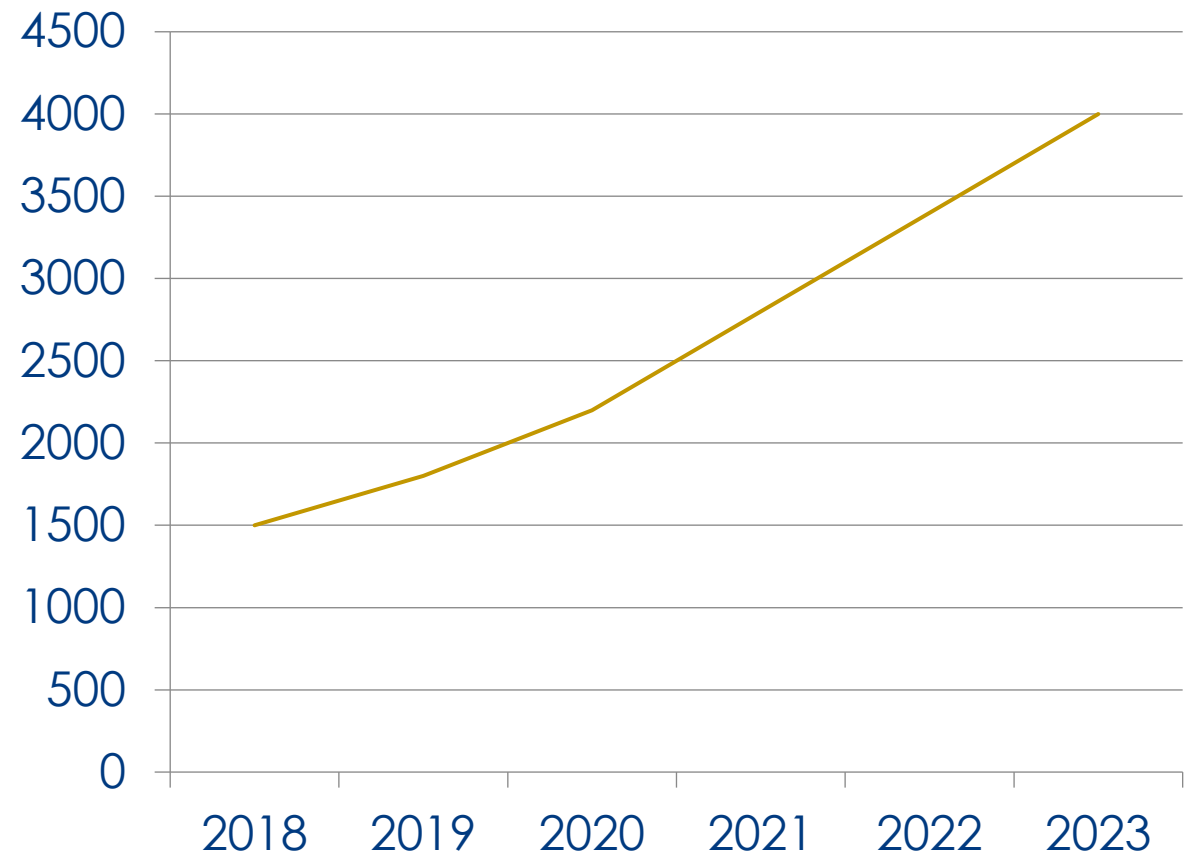
Cyberangriffe sind das **größte Geschäftsrisiko** weltweit laut Allianz Risk Barometer 2024

**9 von 10 Unternehmen** in Deutschland waren von Cyberangriffen betroffen, mit Schäden von über 220 Milliarden Euro pro Jahr (Quelle: Bitkom Digitalverband)

**4,78 Millionen €** kostet ein Cyberangriff deutsche Unternehmen im Durchschnitt (Quelle: Diligent)

**Eine Cyber Risk-Versicherung ist kein Ersatz für IT-Sicherheitsmaßnahmen, sondern eine Ergänzung, die finanzielle und organisatorische Risiken abdeckt.**

**Cyberattacken in Italien (2018-2023)**



# KONSEQUENZEN OHNE CYBER RISK-VERSICHERUNG

Cyber-Risiken sind unvermeidbar, aber die finanziellen und existenziellen Schäden können abgesichert werden

- **Finanzielle Verluste:** Hohe Kosten für Datenwiederherstellung, Umsatzeinbußen durch Betriebsunterbrechung, mögliche Lösegeldzahlungen ohne Garantie sowie Bußgelder bei Datenschutzverstößen können Unternehmen ohne Cyber Risk-Versicherung schwer belasten.
- **Haftungsrisiken:** Schadenersatzforderungen und hohe Rechtskosten belasten Unternehmen erheblich bei Datendiebstahl.



# NIS2 – WAS SIE WISSEN SOLLTEN

NIS2 (EU 2022/2555) ist die neue europäische Cybersicherheits-Richtlinie. Sie verpflichtet Unternehmen zu konkreten Sicherheitsmaßnahmen und Meldepflichten bei IT-Vorfällen

## Wen betrifft NIS2?

- **Unternehmensgröße:**
  - mind. **50 Mitarbeitende** oder
  - **10 Mio. € Umsatz**

## Wie verschärft NIS2 die Vorgaben der bisherigen NIS1-Richtlinie?

- Risikomanagement & IT-Sicherheitsmaßnahmen (inkl. Backup, Zugangskontrollen, Patchmanagement)
- Verpflichtende Meldung schwerwiegender IT-Vorfälle innerhalb 24 Stunden
- Verantwortung der Geschäftsleitung: Haftung bei Pflichtverstößen



**Schutz kritischer und wirtschaftsrelevanter  
Infrastrukturen vor Cyber-Bedrohungen**

# WAS HEIßT DAS FÜR IHR UNTERNEHMEN?

NIS2 & Cyber-Risiken betreffen nicht nur die IT – sondern das ganze Unternehmen.

## Warum wird der Abschluss einer Cyber Polizze stark empfohlen?

- **Deckt viele dieser Risiken finanziell ab** – und unterstützt bei **Incident Response & Wiederherstellung**
- **Sichert Betriebsunterbrechungsschäden ab**, die durch Ausfall von IT-Systemen entstehen
- **Support-Hotline – eine konkrete Hilfe im Notfall** und ein Zeichen von Verantwortung gegenüber Kunden und Partnern.
- hilft nicht nur im Ernstfall – sie zeigt auch, dass Sie **Ihrer Verantwortung aktiv nachkommen**

## Fazit:

- Cyber-Risiken sind nicht nur technisches Problem, sondern auch ein **Compliance-Risiko**
- **Management-Haftung:** Geschäftsführer und Vorstände können **persönlich belangt** werden (siehe nächste Slide)

**Die Frage ist nicht mehr, ob man versichert sein sollte, sondern ob man es sich leisten kann, es nicht zu sein.**

# D&O ALS ERGÄNZUNG ZUR CYBER-POLIZZE

Mit NIS2 und DSGVO steigen die Sorgfaltspflichten für die Geschäftsführung – und damit das Risiko, persönlich belangt zu werden

- **NIS2 verpflichtet die Geschäftsleitung** für angemessene Cybersicherheitsmaßnahmen zu sorgen (Art. 20 & 21)
- **Verstöße können zur persönlichen Haftung** von Geschäftsführern, Vorständen oder IT-Verantwortlichen führen
- **Zusätzlicher Druck durch den „Codice della crisi e dell'insolvenza“:** Er verschärft die Pflichten der Verwaltungsräte und Manager, indem er die Einführung angemessener Organisationsstrukturen und Frühwarnsysteme zur rechtzeitigen Erkennung von Krisensignalen vorschreibt.  
Die unterlassene Umsetzung solcher Maßnahmen – auch im Zusammenhang mit Cyberrisiken, die die Unternehmensfortführung gefährden können – kann als Verletzung der Sorgfalts- und Leitungspflichten gewertet werden und damit das Risiko von Haftungsklagen gegen die Verwaltungsräte erhöhen.
- **Bei Pflichtverletzungen drohen** Bußgelder bis 10 Mio. € oder 2 % vom Jahresumsatz; Regressforderungen durch Gesellschafter oder Aufsichtsräte, **Schäden am Privatvermögen bei fehlender D&O-Versicherung**

**Wer Verantwortung trägt, muss sich schützen –  
Cyber- & D&O-Versicherung sind heute unverzichtbar**

Sie ergänzen sich ideal:



**Die Cyber-Polizze hilft, die finanziellen Folgen  
eines IT-Sicherheitsvorfalls abzufedern**



**Die D&O-Versicherung schützt die verantwortlichen  
Personen vor persönlichen Haftungsrisiken – auch über  
Cyber hinaus**

# WAS DECKT DIE CYBER RISK-VERSICHERUNG AB?

Von finanziellen Verlusten bis hin zu Haftungsansprüchen: Die Cyber Risk-Versicherung schützt Sie umfassend vor den Folgen von Cyberangriffen



## Eigene Schäden:

- Entfernung von Schadsoftware und Sicherung der Systeme.
- Wiederherstellung von Backups und IT-Systemen nach Angriffen.
- Erstattung von Einnahmeausfällen und zusätzlichen Betriebskosten.
- Maßnahmen, um Arbeitsprozesse und den Geschäftsbetrieb schnellstmöglich wieder aufzunehmen.
- Abdeckung von Forderungen, die zur Beendigung eines Erpressungsfalls gezahlt wurden.



## Haftpflichtschäden (Drittschäden):

- Verletzung der Privatsphäre und der Netzwerksicherheit
  - Verstoß gegen personenbezogene Daten
  - Verletzung von geschäftlichen Informationen Dritter
  - Unbeabsichtigter Verstoß gegen Datenschutzbestimmungen
  - Durchführung eines Cyberangriffs auf Dritte
- Haftung im Zusammenhang mit Medien
  - Verleumdung, Beleidigung, Plagiat
  - Verletzung von Urheberrechten im Zusammenhang mit Online-Multimedia-Inhalten

# WEITERE VORTEILE DER CYBER RISK-VERSICHERUNG

## Mehr als nur ein Schutzinstrument

- **Unterstützung beim Krisenmanagement:** professionelle Hilfe bei der Analyse und Bewältigung eines Cyberangriffs.
- **Präventionsmaßnahmen:** Bewertung von Schwachstellen, Schulung der Mitarbeitenden und Phishing-Simulationen zur Stärkung der IT-Sicherheit.
- **Reputationsschaden:** Schutz des Vertrauens von Kunden und Partnern nach einem Cybervorfall.
- **Erfüllung von Kundenerwartungen und gesetzlichen Anforderungen:** Antwort auf wachsende Anforderungen von Kunden, Partnern und Regulierungsbehörden.
- **Zusätzliche Leistungen:** Incident Response, individuelle Schulungen und Sensibilisierungskampagnen.
- **Eingeschlossene Erweiterungen ohne Mehrprämie:** Betrügerische Überweisung von Geldmitteln, Social-Engineering-Betrug, Manipulation von Rechnungen oder Zahlungsanweisungen  
*(gültig nur, wenn die Schulungen zu Cyberbetrugsrisiken innerhalb von 30 Tagen nach Versicherungsbeginn abgeschlossen werden)*



# MAßGESCHNEIDERTE CYBER-DECKUNG FÜR IHRE BEDÜRFNISSE

Welche Informationen werden für einen Vertragsabschluss benötigt?

- **Erforderliche Informationen:**

- Umsatzsteuer-Identifikationsnummer und persönliche Daten des Versicherungsnehmers
- Angabe der gewünschten Erweiterungen
- Hinweis, ob eine Prämienaufteilung gewünscht wird

- **Optional wählbare, nicht standardmäßig enthaltene Erweiterungen:**

- Betriebsunterbrechungsschäden durch einen nicht-IT-Schlüsselzulieferer
- Kosten für Reparatur oder Ersatz beschädigter Hardware
- Hackerangriffe auf Telefonleitungen
- Cryptojacking (Kryptowährungs-Mining)



# UNSERE ERFAHRUNG UND EXPERTISE FÜR IHRE SICHERHEIT

Vertrauen Sie auf unseren professionellen Service

## Was uns auszeichnet:

- Versicherungsbegeisterte Mitarbeiter, die wir kontinuierlich weiterbilden
- Erarbeitung maßgeschneiderter Versicherungslösungen
- Zugang zu internationalen Versicherungsmärkten

## Ihre Vorteile:

- Versicherungsprofis die ausschließlich in Ihrem Interesse handeln
- Persönliche Beratung und individuelle Betreuung
- Erfahrene Schadensreferenten, die Sie vertreten, wenn es darauf ankommt





**ASSICONSULT**  
INTERNATIONAL INSURANCE BROKER

**GENAU DIE SICHERHEIT, DIE SIE IM  
DIGITALEN ZEITALTER BRAUCHEN!**

 +39 0471 069900  
 [info@assiconsult.com](mailto:info@assiconsult.com)  
 [www.assiconsult.com](http://www.assiconsult.com)

# DISCLAIMER

Dies ist ein Offenlegungsdokument und spiegelt die Meinung von Assiconsult GmbH zum Zeitpunkt der Erstellung und auf der Grundlage der verfügbaren Informationen wider. Die hierin enthaltenen Informationen, Analysen und Meinungen wurden aus einer Vielzahl von Quellen zusammengestellt, die als zuverlässig und seriös eingestuft wurden; Assiconsult GmbH übernimmt jedoch keine Garantie für die Richtigkeit oder Vollständigkeit der in dieser Präsentation enthaltenen Daten. Die Informationen, Analysen und Meinungen werden nur zu Informationszwecken bereitgestellt. Assiconsult GmbH veröffentlicht diese Präsentation nach bestem Wissen und Gewissen und auf der Grundlage von wirtschaftlich angemessenen Bemühungen. Assiconsult GmbH haftet daher nicht für (direkte oder indirekte) Schäden oder Verluste jeglicher Art, die dem Leser durch die Nutzung und das Verständnis der Informationen, Analysen und Meinungen entstehen. Die Präsentation enthält Analysen und Meinungen, die ausschließliches Eigentum von Assiconsult GmbH sind; der Leser ist berechtigt, sie zu konsultieren oder für den internen Gebrauch zu vervielfältigen, vorausgesetzt, dass sie deutlich mit dem Vermerk "Assiconsult - Vervielfältigung vorbehalten" versehen sind, dass dieser Absatz wiedergegeben wird und dass die Daten nicht verändert oder modifiziert werden. Jegliche Nutzung, Entnahme, Weitergabe, Vervielfältigung für öffentliche oder kommerzielle Zwecke ohne vorherige Zustimmung von Assiconsult GmbH ist verboten.