HISCOX

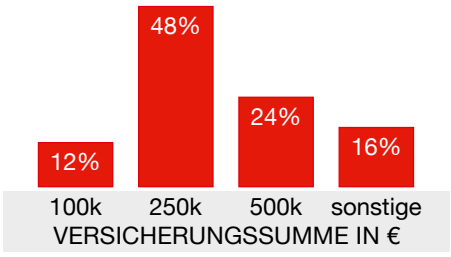
CYBERCLEAR BY HISCOX

PRAXISTIPPS ZUR BESTIMMUNG DER VERSICHERUNGSSUMME

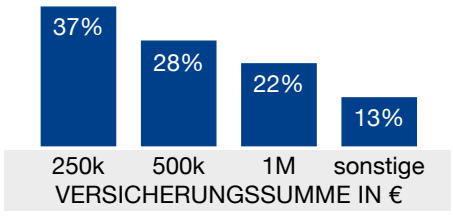
Die Auswahl der richtigen Versicherungssumme für die Absicherung des individuellen Cyber-Risikos kann Kunden und Berater vor Herausforderungen stellen. Eine sich ständig verändernde Risikolandschaft, Weiterentwicklung von Angriffsmustern und komplexer werdende IT-Systeme sorgen dafür, dass sich Risiko und Auswirkungen einer Cyber-Attacke verändern. Mit CyberClear by Hiscox bieten wir als Branchenpionier ein Versicherungsprodukt, dass sich erfolgreich dieser Herausforderung stellt und Unternehmen seit über 13 Jahren verlässlichen und passgenauen Versicherungsschutz bietet. Auch bei der Ermittlung der individuellen Versicherungssummen stehen wir an Ihrer Seite und geben Ihnen hilfreiche Tipps an die Hand.

Dank unserer langjährigen Cyber-Erfahrung haben wir Einblick in tausende Cyber-Risiken. Um Ihnen konkrete Praxiseinsicht zu geben, stellt nachfolgende Übersicht dar, welche Versicherungssummen Unternehmen spezifischer Umsatzgrößen auswählen:

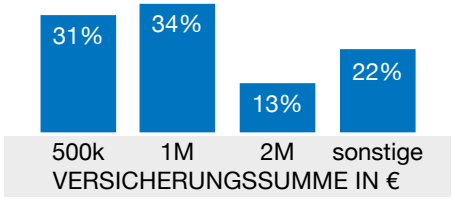
JAHRESUMSATZ DES UNTERNEHMENS
0 - 500K €



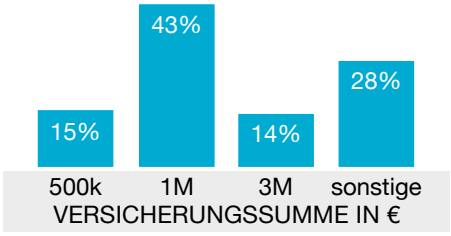
JAHRESUMSATZ DES UNTERNEHMENS
500K - 2,5M €



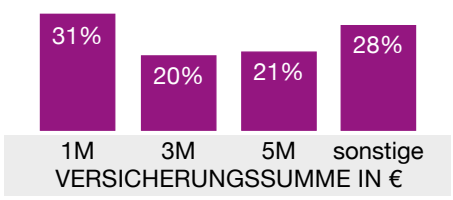
JAHRESUMSATZ DES UNTERNEHMENS
2,5M - 10M €



JAHRESUMSATZ DES UNTERNEHMENS
10M - 25M €



JAHRESUMSATZ DES UNTERNEHMENS
> 25M €



Hiscox bietet Unternehmen bis 25m Euro Umsatz eine schnelle und einfache Abschlussmöglichkeit über elektronische Antragsmodelle.

Nutzen Sie gerne die Möglichkeit im Rahmen dieser Antragsmodelle Kosten für verschiedene alternative Versicherungssummen und Selbstbehalte zu vergleichen.

Hier gehts zum Online-Antrag

INFORMATIONEN AUS DEM HISCOX CYBER READINESS REPORT*

Über 250.000 USD – das ist die Summe, die international **jedes 8. Unternehmen** ein Cyber-Schaden kostet.

20-26 Attacken pro Jahr müssen sich Unternehmen mit **bis zu 49 Mitarbeitern** in Deutschland stellen.

Mehr als jedes 5. Unternehmen in Deutschland gab an, dass die Auswirkungen eines **Cyber Schadens existenzbedrohend** waren.

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

AssCompact -TRENDS 2017-2023- SILBER
Cyber-Versicherung
25 x PLATZ 1
Hiscox SA, Niederlassung für Deutschland

Cyber-Versicherungs-Innovation des Jahres 2023
Euro
Euro
Börse Online

WIE BESTIMME ICH DIE PASSENDE VERSICHERUNGSSUMME FÜR MEINE CYBER-KUNDEN?

Die Bestimmung der passenden Versicherungssumme erfordert eine sorgfältige Analyse, da diese von verschiedenen Faktoren abhängt. Diese Faktoren können zwischen Branchen und Unternehmen variieren, deswegen gibt es auch keine allgemeingültige Formel. Allerdings gibt es entscheidende Aspekte, die bei der Entscheidung immer berücksichtigt werden sollten, und die Sie in Ihr Kundengespräch einbringen können:

Unternehmensgröße und Branche

Bestimmte Branchen sind besonders häufig von Cyber-Angriffen betroffen. Ebenso kann mit steigendem Umsatz auch ein Anstieg von zielgerichteten Angriffen festgestellt werden.* Finden Sie weitreichende Informationen dazu im Hiscox Cyber Readiness Report.

Wichtige Fragen für den Kundentermin:

- In welcher Branche ist das zu versichernde Unternehmen tätig?
- Wie viele Mitarbeiter (inklusive freier Mitarbeiter, Auszubildender, überlassener Mitarbeiter) hat das Unternehmen?

Abhängigkeit vom IT-System

Sofern das IT-System ein unternehmenskritischer Faktor für die Erbringung von Dienstleistungen und/oder Produktion ist, führt dies im Falle eines Angriffs zu hohen Kosten im Rahmen einer Betriebsunterbrechung. Stehen hingegen manuelle Prozesse zur Verfügung, über die ein Großteil der Umsätze auch im Falle der Nicht-Verfügbarkeit von IT-Systemen erwirtschaftet werden können, wirkt dies positiv auf Kosten im Schadenfall.

Wichtige Fragen für den Kundentermin:

- Wie hoch ist der Ertragsausfall pro Monat bestehend aus den fortlaufenden Kosten und dem Betriebsgewinn?
- Wie lange würde die Wiederherstellung der IT-Systeme dauern?
- Multiplizieren Sie Ertragsausfall pro Monat mit der Anzahl an Monaten

Umfang, Aufbau, Komplexität und Sicherheit des IT-Systems

Während eine umfassende Netzwerktrennung und redundanter Aufbau eines IT-Systems Kosten im Falle eines Angriffs verringern können, verursachen eine hohe Komplexität und eine starke Vernetzung meist höhere Kosten in der Wiederherstellung von Daten und Systemen. Die Resilienz eines IT-Netzwerks spielt eine entscheidende Rolle zur Reduzierung von Anzahl und Umfang von Angriffen.

Wichtige Fragen für den Kundentermin:

Systemarchitektur

- Wie umfangreich und komplex sind die Netzwerkstrukturen?
- Gibt es mehrere Standorte und sind diese voneinander unabhängig?
- Gibt es Cloud-Infrastrukturen oder ausschließlich On-Premises-Strukturen?

Netzwerksicherheit

- Gibt es eine IT-Sicherheitsrichtlinie, die Sicherheitsmaßnahmen zum Schutz des Netzwerks definiert ?
- Gibt es z.B. Firewalls, aktuellen Virenschutz, werden Verschlüsselungstechnologien verwendet und existieren Maßnahmen zur Angriffserkennung und – abwehr?
- Gibt es Ransomware sichere Back-Ups mit regelmäßigen Rücksicherungstests?
- Existiert ein Patch-Management Prozess?

Zugriffsmanagement

- Gibt es eine klare Richtlinie für Zugriffsrechte und wird diese konsequent umgesetzt?
- Wie wird der (Fern-) Zugriff auf die IT-Systeme verwaltet?

Notfallpläne

- Gibt es Notfallpläne wie Incidents (Cyber-Vorfälle) behandelt werden?
- Gibt es ein Response-Team, das Incidents (Cyber-Vorfälle) behandelt?
- Was würde es kosten das gesamte IT-System wieder neu aufzustellen?

Umfang sensibler personenbezogener Daten sowie Zahlungsdaten

Werden im großen Umfang sensible personenbezogene Daten gem. DSGVO und/oder Zahlungsdaten (z.B. Bank- oder Kreditkartendaten) verarbeitet, kann dies im Fall einer Cyber-Attacke zu hohen Kosten für z.B. Datenschutzanwälte, Benachrichtigung Betroffener sowie Kosten für PR-Beratung führen. Nehmen Sie für Ihre Beispielrechnung 10 Euro pro Kreditkartendatensatz sowie 100 Euro pro Datensatz sensibler Daten an.

Wichtige Fragen für den Kundentermin:

- Welche Daten werden in den IT-Systemen erfasst, verarbeitet und gespeichert?
- Gibt es sensible Daten, personenbezogene Daten?
- Müssen Firmengeheimnisse geschützt werden, z.B. geistige Eigentumsrechte?

*Daten aus dem Hiscox CRR 2023

Besonderer Hinweis: Wiederaufholeffekte

Besteht die Möglichkeit Umsatzausfälle im Rahmen einer Cyber-Attacke nach Wiederherstellung der Systeme aufzuholen, wirkt dies positiv auf die Gesamtschadenkosten.

Risikobereitschaft, Liquidität und Reputation

Die Bereitschaft des Unternehmens einen Teil des Risikos selbst zu tragen, spielt eine wesentliche Rolle beim Abschluss einer Versicherung. Dies kann in Form von Selbstbehalten oder limitierten Deckungssummen erfolgen. Auch vorhandene Liquidität, um im Schadenfall einen Teil der Kosten selbst zu übernehmen, sollte Berücksichtigung finden.

Steht das Unternehmern in der Öffentlichkeit, so sollten auch unbedingt gegebenenfalls anfallende Kosten für Unterstützung bei PR- und Krisenkommunikation berücksichtigt werden.

Expertentipp: Simulieren Sie mit Ihren Kunden regelmäßig mögliche Szenarien und Konsequenzen einer Cyber-Attacke unter Berücksichtigung des individuellen Risikoprofils eines Unternehmens. Gleichzeitig sollten auch externe Faktoren und die aktuelle Risikosituation Berücksichtigung finden. Zu der aktuellen Cyber Risikolandschaft erhalten Sie umfassende Informationen aus dem **aktuellen Hiscox Cyber Readiness Report.**

Weiterführende Informationen zu Hiscox CyberClear finden Sie in Ihrem **Hiscox Maklerportal.**

Hiscox
Bernhard-Wicki-Straße 3, 80636 München

Für Makler
T +49 89 54 58 01 100
E hiscox.info@hiscox.de
W makler.hiscox.de

Für Endkunden
T +49 89 54 58 01 700
E myhiscox@hiscox.de
W hiscox.de

Hiscox in Social Media
Makler Service & News
Business Blog
Classic Cars Blog