



# ERGEBNISSE DER GVNW-UMFRAGE CYBER-RISIKO UND CYBER-VERSICHERUNG

Holger Tittko, Gesamtverband der versicherungsnehmenden Wirtschaft e.V.

Gesamtverband der versicherungsnehmenden Wirtschaft e.V.

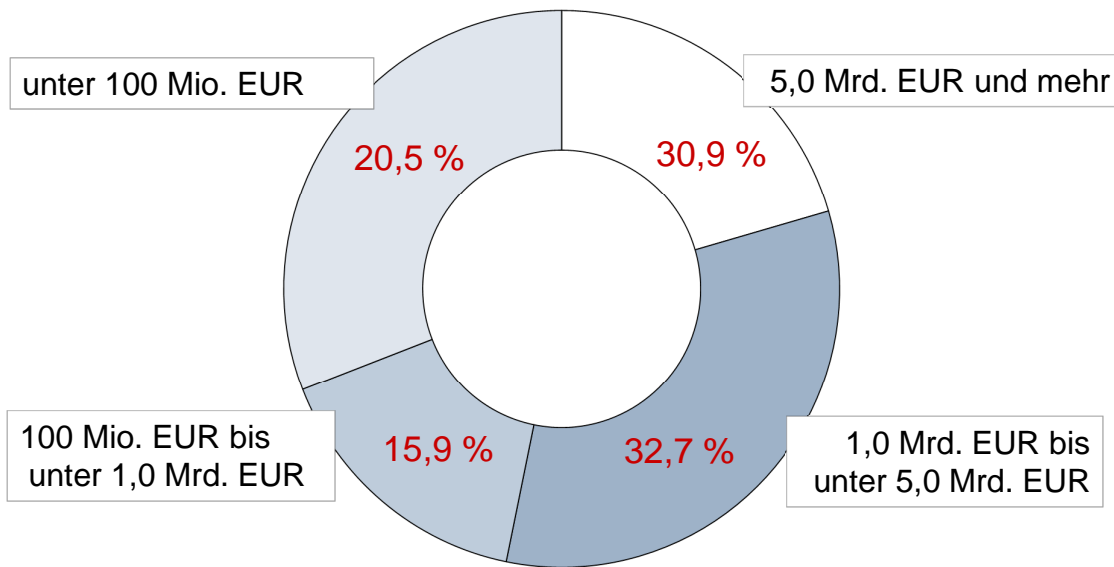
Umfrage unter den Mitgliedsunternehmen des GVNW,  
Gesamtverband der versicherungsnehmenden Wirtschaft e.V.,

zu den Themen

## Cyber-Risiken und Cyber-Versicherung

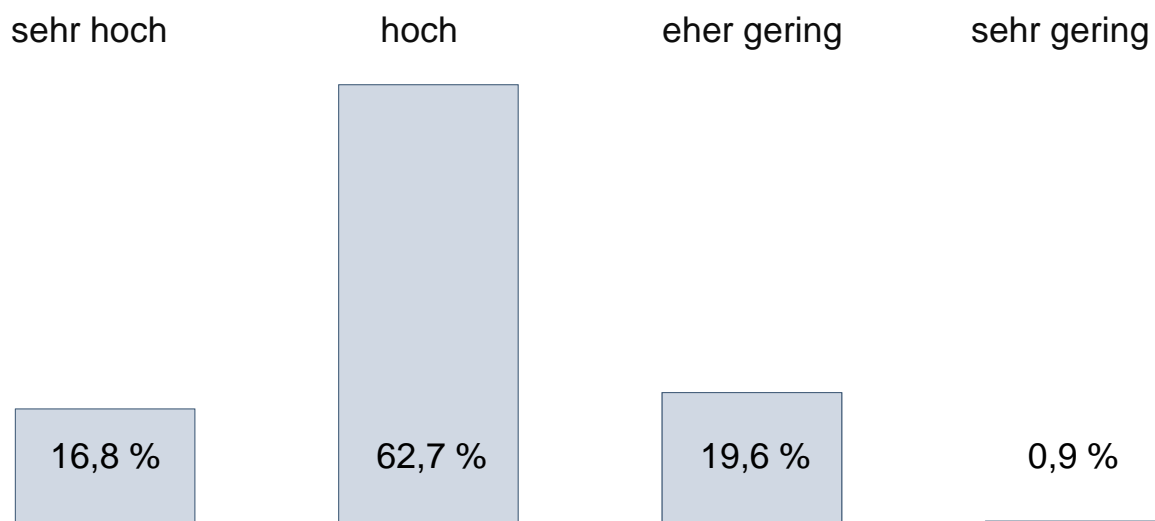
- im Zeitraum vom 25. Januar 2018 an bis 14. Februar 2018,
- anonym, über das Portal eines Internet-Dienstleisters,
- an der über 100 Teilnehmer mitgewirkt haben.

## Umfrageteilnehmer nach Umsatzgrößen



3

## Wie schätzen Sie die Cyber-Risiken gegenüber anderen Risiken, die den Unternehmenserfolg bedrohen, ein?

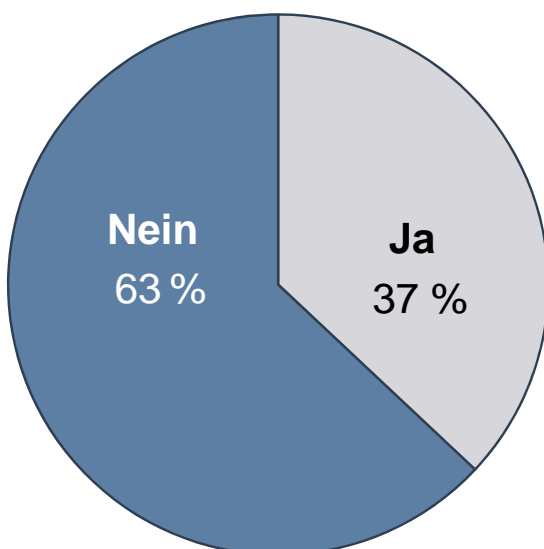


4

Wie schätzen Sie die Cyber-Risiken gegenüber anderen Risiken, die den Unternehmenserfolg bedrohen, ein?

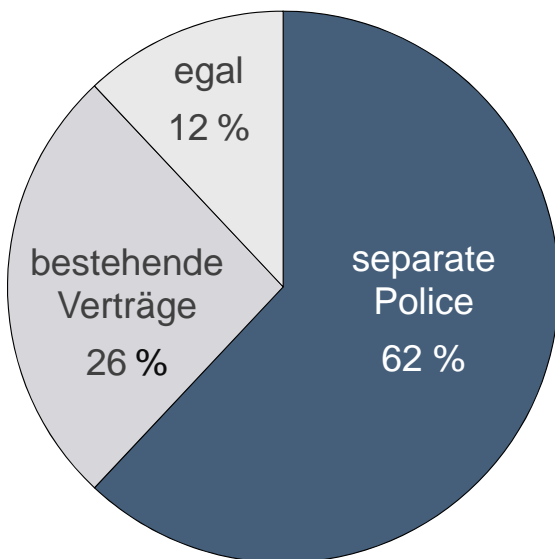
- „Sehr hoch. Trotz erhöhter awareness und Budgets für Sicherheit. Erinnert an ein Hase/Igel-Rennen.“
- „Hoch, Tendenz steigend.“
- „Eigentlich ein mittleres Risiko, da wir nicht mit Endkundendaten arbeiten.“
- „Eher gering. Elementargefahren stellen ein höheres Schadenpotential dar.“

Sind Sie in die Entscheidungsprozesse über die IT-Sicherheit in Ihrem Unternehmen eingebunden?



- „Investitionen: nein; Absicherung und Risikodialoge: ja“
- „Themen zu komplex; Kommunikation allerdings in regelmäßigen Workshops“
- „Derzeit nicht, wird jedoch von unserer Seite intensiver angegangen“
- „Sehr technisch und unterliegt daher der IT“

Sollten die Cyber-Gefahren mit einer eigenständigen Cyber-Police oder im Rahmen bestehender Deckungskonzepte versichert werden?



- „separate Police ermöglicht eine höhere Flexibilität und Detaillierungsgrad“
- „zum größten Teil bereits über bestehende Verträge“ [gedeckt]
- „Ist egal, wenn man maßgeschneiderte Deckungen zu akzeptablen Kosten erhält“
- „vermutlich sowohl als auch / Cyber-Police ist nicht zur umfassender Deckung aller denkbaren Risiken“ [geeignet]

[...] = redaktionelle Ergänzung

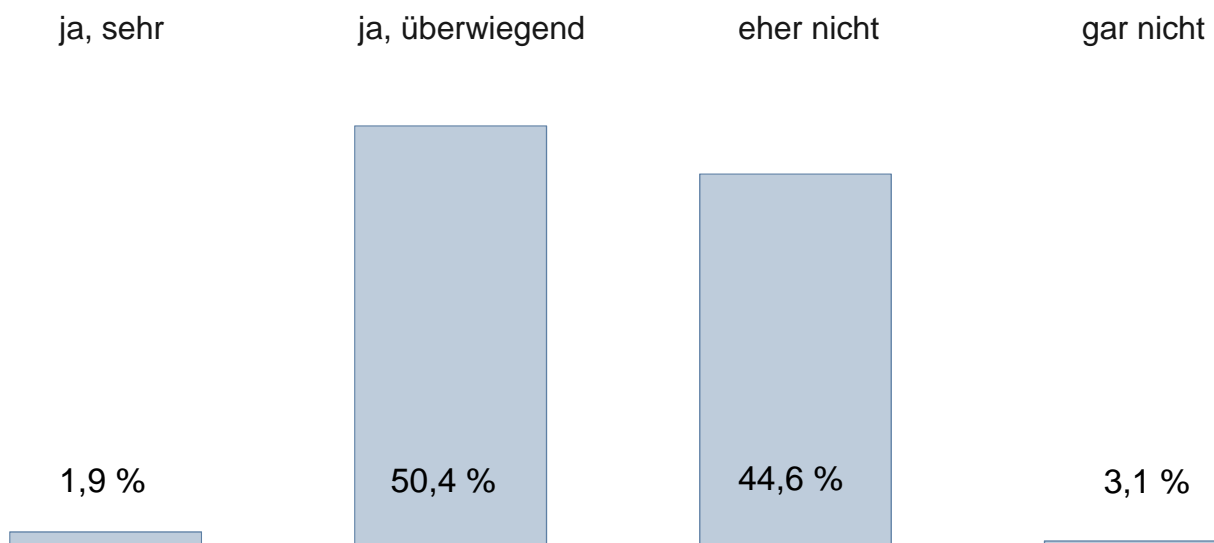
Welchen Prioritätsgrad ordnen Sie den nachfolgenden Deckungselementen zur **Drittschadens-Versicherung** zu? (Zahlenangaben in Prozent)

	sehr wichtig	wichtig	weniger wichtig	unwichtig
ausreichende Summen bzw. Sublimits	59,0	38,0	3,0	0,0
Versicherung der gesetzlichen Haftung	50,5	43,9	5,6	0,0
Versicherung vertraglicher Haftung (Erfüllung)	37,4	48,6	13,0	1,0
vorgezogene Rettungskosten	24,1	43,5	28,7	3,7
Versicherung von Vertragsstrafen	19,4	37,0	34,3	9,3

Welchen Prioritätsgrad ordnen Sie den nachfolgenden Deckungselementen zur **Eigenschaden-Versicherung** zu? (Zahlenangaben in Prozent)

	sehr wichtig	wichtig	weniger wichtig	unwichtig
ausreichende Summen bzw. Sublimits	61,3	33,0	5,7	0,0
Ertragsausfälle (insbesondere BU)	55,1	33,6	11,3	0,0
Schäden durch Infiltration der IT-Systeme von Kunden und Zulieferern	40,2	38,3	20,6	0,9
Versicherung von Kostenpositionen (IT-Forensik, Benachrichtigung Dritter etc.)	43,0	43,9	13,1	0,0
Kapitalabflüsse durch kriminelle Handlungen Dritter oder durch Mitarbeiter	32,7	42,1	23,4	1,9
vorgezogene Rettungskosten	26,7	45,7	24,8	2,8

Sind Sie mit den Deckungsangeboten der Cyber-Versicherer zufrieden?



## Sind Sie mit den Deckungsangeboten der Cyber-Versicherer zufrieden?

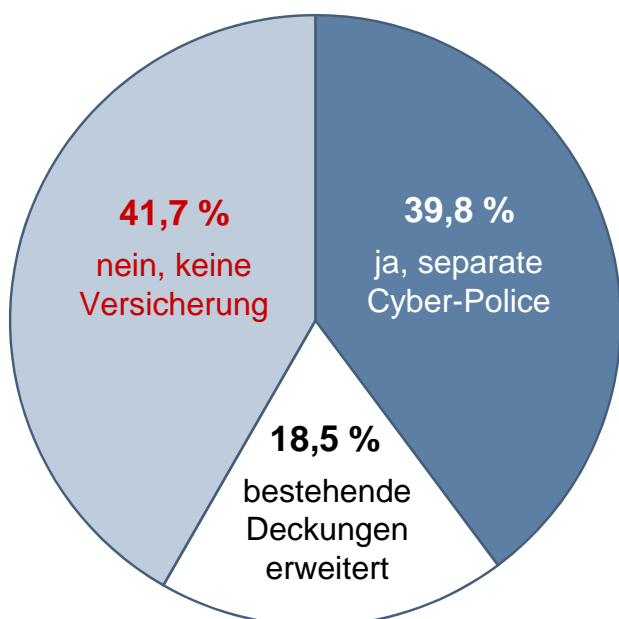
wenig Lob:

- Versicherungsangebote sind attraktiv, schwierig ist der Prozess der Eindeckung

viel Kritik:

- produktorientiert - nicht lösungsorientiert
- zu pauschal, zu unübersichtlich, intransparent
- kein Schadenersatz für BU/Bandstillstand beim Kunden
- Deckungssummen sind ausbaufähig
- EU-DSGVO Strafzahlungen nicht versichert
- Umweltschäden sind kaum abzusichern
- endlose Prüfung der Einhaltung von Sanktionsklauseln

## Sind Sie gegen schädigende Cyber-Vorfälle versichert?



- „Ja, seit vier Jahren“
- „Wir haben nicht erweitert, wir hatten diese Deckung schon“
- „vollständige Deckung nur in Teilbereichen des Unternehmens“
- „Findungsphase ist undurchsichtig“
- „Wir prüfen die Notwendigkeit einer Cyber-Police jedes Jahr erneut“

Gründe, weswegen eine Cyber-Versicherung bisher nicht in Betracht kam und vorerst auch nicht in Betracht gezogen wird *(Mehrfachantworten möglich)*



Risikoanalyse/-bewertung noch nicht abgeschlossen .....	65,5 %
Auflagen und Sanktionen wg. Vertragspflichtverletzungen ....	19,0 %
Keine risikoadäquate Deckung .....	17,3 %
Prämie unverhältnismäßig hoch .....	17,2 %
ausreichendes Sicherheitskonzept .....	13,8 %
Abschluss einer Cyber-Police zu aufwendig .....	12,1 %
geringer Gefährdungsgrad .....	3,4 %
sonstige Gründe .....	15,5 %

Eine Cyber-Versicherung kam/kommt nicht in Betracht, weil („sonstige Gründe“)



- „wir uns zuvor noch nicht intensiv mit den Gefahren und möglichen Deckungen befasst haben“
- „Ausschnittdeckungen noch nicht separat angeboten werden“
- „keine katastrophalen Risiken aufgrund von voneinander unabhängig operierender Geschäftsbereiche“ [existieren]
- „das Risikobewusstsein in der Entscheidungsebene nicht sehr ausgeprägt ist“
- „aus Sicht des Risk Managements das Ziel eine Versicherungsdeckung des Restrisikos“ [ist]

[...] = redaktionelle Ergänzungen

Wenn Sie bereits die Abwicklung eines versicherten Cyber-Schadens begleitet haben, waren Sie mit der Regulierung zufrieden?

Die häufigsten Anmerkungen:

- es ist noch kein Cyber-Schaden eingetreten
- wir hatten bisher keinen versicherten Cyberschaden
- bislang in keine Abwicklung eines Cyber-Schadens involviert

Einzelne Stimmen:

- reine Kostenpositionen, Forensik-Kosten, sind gut zu regulieren.
- nur Erfahrung mit nicht versicherten Schäden

Aus den Kommentaren:

*„Es stellt sich langfristig die Frage, ob die Cyberversicherung in der aktuellen Form noch Bestand haben wird, wenn die Daten zur Verarbeitung künftig einem Cloudanbieter überlassen werden.“*

*Da viele Unternehmen sich derzeit in der Digitalisierungsphase befinden und Cloudanbieter einen wesentlich höheren Schutz bieten können, benötigt man vielleicht keine eigenen Deckungen mehr – oder?“*