

Thomas Pache

Cyberversicherung für Vermittler

Risiko, Bewertung und Deckung

Thomas Pache

Cyberversicherung für Vermittler

Risiko, Bewertung und Deckung

Thomas Pache

Cyberversicherung für Vermittler

Risiko, Bewertung und Deckung

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© 2019 VVW GmbH, Karlsruhe

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urhebergesetz zugelassen ist, bedarf der vorherigen Zustimmung der VVW GmbH, Karlsruhe. Jegliche unzulässige Nutzung des Werkes berechtigt die VVW GmbH zum Schadenersatz gegen den oder die jeweiligen Nutzer.

Bei jeder autorisierten Nutzung des Werkes ist die folgende Quellenangabe an branchenüblicher Stelle vorzunehmen:

© 2019 VVW GmbH, Karlsruhe

Jegliche Nutzung ohne die Quellenangabe in der vorstehenden Form berechtigt die VVW GmbH zum Schadenersatz gegen den oder die jeweiligen Nutzer.



Beachten Sie bitte stets unseren Aktualisierungsservice auf unserer Homepage unter: **vvw.de** → **Service** → **Ergänzungen/Aktualisierungen**. Dort halten wir für Sie wichtige und relevante Änderungen und Ergänzungen zum Download bereit.

Gleichstellungshinweis

Zur besseren Lesbarkeit wird auf geschlechtsspezifische Doppelnennungen verzichtet.

ISBN 978-3-96329-294-1

Vorwort

Aufgrund der nachfolgend genannten Überlegungen wird die Cyberversicherung von Vermittlerseite häufig als ein „Problembär“ gesehen, den zu „erlegen“ man gezwungen wird. Diese Jagdfibel soll daher diejenigen unterstützen, die „Cyber“ als Akquise-Chance begreifen oder die ihre Bestände sichern und ihrem Beratungsauftrag bestmöglich nachkommen wollen, ohne sich nur auf scheinbar simple Lösungen wie Werbeflyer, Onepager oder Klauselsynopsen zu verlassen.

Neben „Fintec“ ist „Cyber“ in Versicherungskreisen das Buzzword des Jahres 2019. Selbst wenn man es als Vermittler in den vergangenen Jahren geschafft hat sich dem Thema Cyberversicherung zu entziehen, wird man nun doch davon eingeholt und ist dann oftmals mit folgender Situation konfrontiert:

- Die Managementebene mancher Versicherer haben nach Lesen der KPMG-Studie Versicherer recht ehrgeizige Ziele formuliert und machen entsprechend Druck.
- Die Versicherungsbedingungen der verschiedenen Konzepte sind von Grund auf verschieden und machen Vergleiche aufwändig.
- Bei der Multispartlichkeit der Konzepte führen erlernte Spartenansätze oftmals in die Irre.
- Informations- und kommunikationstechnische Risiken sind
 - unterschiedlich komplex,
 - unterschieden sich teilweise auch innerhalb derselben Branche und
 - entwickeln sich schneller als andere Risiken.
- Die Zeitspanne von Erstansprache bis zu Abschluss eines Versicherungsvertrages ist im Vergleich zu anderen Versicherungssparten überdurchschnittlich groß.

Themen, die dem Autor in seiner siebenjährigen Beschäftigung mit Cyberversicherung untergekommen sind, werden anhand einer Fragen- und Antworten-Struktur – soweit möglich – jeweils abschließend beantwortet.

Inhaltsverzeichnis

Vorwort	V
Grundlagen „Cyber-Risiken“	1
1 Warum wird behauptet, dass die Cyberrisiko-Versicherung eine „große“ Zukunft hat?	1
2 Welche typischen Angriffsarten gibt es?	3
3 Was versteht man unter dem Begriff Informationssicherheit?	5
4 Welche Begriffe sollte ein Vertriebsmitarbeiter verwenden/verstehen?	6
5 Auf welchen rechtlichen Grundlagen fußt die IT-Sicherheit in Deutschland? ..	8
6 Gibt es besonders gefährdete Branchen?	10
7 Welche deutschen/europäischen Organisationen beschäftigen sich mit Informationssicherheit?	12
8 Welche Informationen zu rechtlichen Regelungen/Gesetzen sind im Internet verfügbar?	13
9 Welche Haftungsnormen sind relevant?	14
10 Welche (technischen) Normen sind aus Sicht der Cyberversicherer relevant?	16
11 Welche Kumulrisiken existieren?	18
12 Wie werden sich Cyberrisiken und Cyberversicherungen in Zukunft entwickeln?	20
13 Wie hängen die Begriffe IT-Sicherheit, Datensicherheit und Datenschutz zusammen?	24
14 Welche Zertifizierungen geben Aufschluss über die Qualität der ITK-Sicherheit?	25
Erfragen des individuellen Kundenrisikos	27
15 Warum unterscheidet man zwischen IT und OT?	27
16 Gibt es besondere Risikobranchen (vs. Geschäftsmodelle)?	28
17 Welche Fachbegriffe sollten Fachberater von Vermittlern beherrschen?	29
18 Wie gelange ich an zielgruppenbezogene Schadenbeispiele?	30
19 Welche Risikoinformationen müssen zur Risikobeurteilung erhoben werden?	30
20 Wie erhalte ich relevante Risikoinformationen über zu versichernde Unternehmen?	31

21	Welcher Fragebogen für welches Risiko?	32
22	Wo liegen – aus Cyber-Sicht – die Risikoschwerpunkte eines Produktionsbetriebs und eines Wohnungsunternehmens?	33
23	Welche Cyberrisiken herrschen bei Freiberuflern vor?	35
24	Wie sieht eine typische Risikolandkarte eines Einzelhandelsunternehmens aus?	37
Risikoevaluierung – Risiko des Kunden bei herkömmlichen Deckungen einschätzen.		41
25	Welches sind die häufigsten Schäden?	41
26	Wie ermittle ich die korrekte Gesamt-Versicherungssumme?	42
27	Wie ermittle ich die richtige BU-Versicherungssumme?	43
28	Wie ermittle ich die potentiellen Kosten von Cyber-Schadenfällen?	45
29	Welche Überschneidungen haben Cyberversicherungen mit herkömmlichen Versicherungen?	47
Erklären des neuen Versicherungsschutzes		51
30	Wie ist eine „Cyberversicherung“ definiert?	51
31	Was versteht man unter „Silent Cyber Risk“?	52
32	Was bringt die Integration präventiver Maßnahmen?	53
Deckungsumfang von Cyber-Versicherungen.		55
33	Wie läuft das mit der Versicherung von Erpressungsgeldern?	55
34	Sind Bußgelder versicherbar?	56
35	Wie relevant sind Obliegenheiten vor Eintritt des Versicherungsfalls (z.B. Stand der Technik)?	58
36	Wie wirken Selbstbehalte bzw. Selbstbeteiligungen und Wartezeiten?	58
37	Wodurch wird der Versicherungsschutz einer Cyberversicherung ausgelöst?	59
38	Welche Obliegenheiten gibt es im Versicherungsfall?	62
39	Wie wirkt eine Erprobungsklausel in Cyberversicherungen?	62
40	Was ist im Zusammenhang mit Rückwärtsdeckungen zu beachten?	63
41	Was ist im Zusammenhang mit Vorwärtsdeckungen zu beachten?	64
42	Was versteht man unter Eigenhandel?	65

43	Was versteht man in der Cyberversicherung unter „reinen Vermögensschäden“?	67
44	Über welche Haupt-Versicherungsbestandteile verfügt eine Cyberversicherung?	67
45	Welche Deckungserweiterungen finden sich derzeit auf dem Markt?	68
46	Wie gut sind die unverbindlichen GDV-Musterbedingungen?	70
47	Was bedeutet der Baustein PCI Bußgelder?	71
48	Inwieweit ist auch eine vertragliche Haftung versicherbar?	72
49	Was ist bei der Festlegung des räumlichen Geltungsbereiches zu beachten?	73
50	Wo erhalte ich Informationen zu Versicherungslösungen?	73
Einwandbehandlung		75
51	Wie verhält es sich mit der „Kriegsklausel“?	75
52	Inwieweit deckt eine Cyberversicherung Vorsatztaten?	76
53	Warum bieten viele Versicherungskonzepte Versicherungsschutz für Aufwendungen vor Eintritt des Versicherungsfalls?	77
54	Was ist mit Blick auf Produkt- und Leistungsrisiken zu beachten?	78
55	Wieso werden Fake-President-Angriffe in Cyberversicherungen nicht als versichertes Cyberrisiko angesehen?	79
56	Welche cyberrisiko-induzierten Schäden sind (Stand heute) nicht/kaum versicherbar?	80
57	Welche Kommunikationsfallen sollte man vermeiden?	82
58	Welche Schadenbeispiele gibt es?	83
59	Wer sind die Stakeholder in einem Cyberrisiko-Transfer-Prozess?	85
60	Ist die Cyberversicherung eine Konkurrenz für Cyber-Investitionen in einem Unternehmen?	86
61	Welche Informationen zu aktuellen Cyber-Vorfällen sind im Internet frei verfügbar?	87
62	Welche Informationen zu Statistiken und Reports im Zusammenhang mit Cyberrisiken sind im Internet frei verfügbar?	88
Abbildungsverzeichnis		89
Stichwortverzeichnis		93

