Daniel Blazquez – Line Manager Cyber

Cyber-Versicherung: Risiken erkennen und passende Versicherungslösung ermitteln

MARKEL

Ihr heutiger Referent

Daniel Blazquez

Line Manager Cyber

- → Seit Januar 2016 bei Markel
- → Verantwortlich für das Underwriting und die Produktentwicklung im Bereich Cyber
- → Mehr als 20 Jahre Berufserfahrung in der Versicherungswirtschaft

Neu:
IDD-Zertifizierung unserer Markel Academy Webinare jetzt auch in Österreich!

In Kooperation mit „Die Bildungsstelle” können Teilnehmende aus Österreich nicht nur ihr Fachwissen vertiefen, sondern auch ihre IDD-Pflichtzeiten erfüllen.

So einfach geht’s: Nach dem Webinar die Lernerfolgskontrolle bestehen und IDD-Zeit erhalten

MARKEL

die Bildungsstelle

Problemstellung: Erkennung des Versicherungsbedarfs

01

Cyber-Risiko: Was ist das?

Fehlende Awareness

- Viele Versicherungsnehmer erkennen nicht, welche Cyber-Risiken sie tatsächlich haben.
- Versicherungsnehmer unterschätzen oft ihre digitale Abhängigkeit.

Komplexität der Risiken

- Cyber-Risiken sind oft schwer greifbar und nicht direkt sichtbar.
- Versicherungsnehmer sind sich ihrer komplexen IT-Infrastruktur oft nicht bewusst.

Veraltete Risikoeinschätzung

- Herkömmliche Risikomanagement-Methoden sind auf physische Risiken fokussiert und berücksichtigen digitale Bedrohungen nicht ausreichend.

Dynamik der Bedrohung

- Cyber-Bedrohungen ändern sich ständig, was die Risikoabschätzung erschwert.

Wie helfe ich meinem Kunden sein Risiko zu verstehen?

Mit wenigen Fragen können Sie das Risikobewusstsein des Kunden erhöhen:

- Steht mein Betrieb **ohne funktionierende IT** still?
- Steht mein Betrieb ohne Zugang zu meinen **Unternehmensdaten** still?
- Speichert mein Unternehmen **personenbezogene Daten**? Wenn ja, wo? Wie viele?
- Arbeitet mein Unternehmen mit **externen Partnern** zusammen, die Zugriff auf meine Daten haben? Wenn ja, wie sicher sind deren Systeme?
- Welche Art von **Software, Netzwerken oder Cloud-Diensten** benutze ich in meinem Unternehmen?
- Kann ich mir den Stillstand meines Unternehmens für **längere Zeit finanziell leisten**?
- Kann ich mir den **Austausch meiner gesamten IT-Infrastruktur** finanziell leisten?

Einwände des Kunden sind Ihre Chance!

"Cyber-Risiken betreffen mich nicht, wir sind zu klein, um ein Ziel zu sein."

Tatsächlich werden immer mehr kleine und mittel-ständische Unternehmen (KMU) angegriffen, da sie oft weniger gut abgesichert sind und als leichtere Ziele gelten. Angriffe wie Phishing, Ransomware oder Datendiebstahl betreffen auch kleine Unternehmen.

43% aller KMUs wurden bereits Opfer von Hackern.

"Unsere IT-Sicherheit ist gut genug, wir brauchen keine zusätzliche Versicherung."

Eine Cyberversicherung ist keine Alternative zur IT-Sicherheit, sondern eine Ergänzung. Sie schützt vor den finanziellen Folgen eines Angriffs, wie zum Beispiel den Kosten für die Wiederherstellung von Systemen, die Reputationsschäden oder gesetzliche Strafen.

"Die Kosten für eine Cyber-Versicherung sind zu hoch."

Die Kosten für einen können Existenzbedrohend sein. Die Versicherung bietet eine Möglichkeit, das Risiko zu managen und schützt das Unternehmen vor unvorhersehbaren finanziellen Belastungen.

"Wir haben noch nie einen Cyber-Angriff erlebt, warum sollten wir jetzt eine Versicherung abschließen?"

Cyber-Bedrohungen sind ständig im Wandel, und Unternehmen müssen sich proaktiv gegen diese Risiken absichern, bevor ein Vorfall eintritt. Es ist wie bei einer Unfallversicherung: Nur weil man nie einen Unfall hatte, sollte man nicht darauf verzichten.

Einwände des Kunden sind Ihre Chance!

"Ich vertraue auf die Absicherung durch meine allgemeinen Versicherungen."

Die meisten allgemeinen Versicherungen bieten keine Deckung für Cyber-Vorfälle wie Datenverlust, Ransomware-Angriffe oder die Kosten für Krisenmanagement und rechtliche Beratung. Eine Cyberversicherung ist speziell darauf ausgerichtet, diese Risiken zu übernehmen.

"Wir können die Risiken durch interne Sicherheits-vorkehrungen selbst managen."

Selbst mit den besten internen Sicherheits-maßnahmen ist es unmöglich, alle möglichen Cyber-Risiken zu eliminieren. Die Bedrohungslage verändert sich ständig, und Cyberkriminelle entwickeln immer raffiniertere Angriffsstrategien.

"Ich verstehe die Bedingungen und den Umfang einer Cyber-Versicherung nicht."

Bedingungswerke werden immer verständlicher. Modulare Versicherungsprodukte können auf die spezifischen Bedürfnisse des Kunden angepasst werden.

"Ich benötige keine Versicherung, weil ich keine sensiblen Daten habe."

Ein Ransomware-Angriff kann Ihre Geschäftsprozesse lahmlegen, selbst wenn keine sensiblen Daten betroffen sind. Der Schaden, der durch einen solchen Angriff entsteht (z. B. durch Betriebsunterbrechung oder den Verlust von Geschäftsdaten), kann erhebliche finanzielle Auswirkungen haben.

Die Risikoanalyse

02

Risikofragebogen: Das nötige Übel oder Vertriebstool?

Risikofragebögen werden oft als zu lang und unverständlich empfunden. Eine verständliche Sprache ist sowohl in der Risikoanalyse als auch in den Versicherungsbedingungen oft ausschlaggebend für den Abschluss einer Cyberversicherung.

Werden „End-of-Life"-Systeme genutzt (Systeme, für die der Hersteller keine Sicherheitsupdates oder Support mehr bereitstellt)?	Ja ☐	Nein ☐
Falls ja:		
a) Sind diese in einer isolierten Netzwerkumgebung betrieben?	Ja ☐	Nein ☐
b) Besteht eine direkte Verbindung zum externen Netzwerk (Internet)?	Ja ☐	Nein ☐
c) Gibt es einen Migrationsplan?	Ja ☐	Nein ☐
Wird eine „Endpoint-Protection-Lösung"(EDR), welche automatisch aktualisiert wird, eingesetzt?	Ja ☐	Nein ☐
Wird ein 24/7 Security Operations Center (SOC) eingesetzt, das sicherheitsrelevante Ereignisse kontinuierlich überwacht und bei Bedarf Maßnahmen zur Gefahrenisolierung ergreifen kann?	Ja ☐	Nein ☐
Findet eine automatisierte Überwachung, Protokollierung und Überprüfung von Protokolldateien (SIEM) statt?	Ja ☐	Nein ☐

Risikofragebogen: Das nötige Übel oder Vertriebstool?

Oft erkennen Unternehmen erst durch die Beantwortung des Fragebogens, dass sie in bestimmten Bereichen der **IT-Sicherheit Lücken** haben.

Der Risikofragebogen ermöglicht eine **systematische und strukturierte** Erfassung der spezifischen Cyber-Risiken eines Unternehmens.

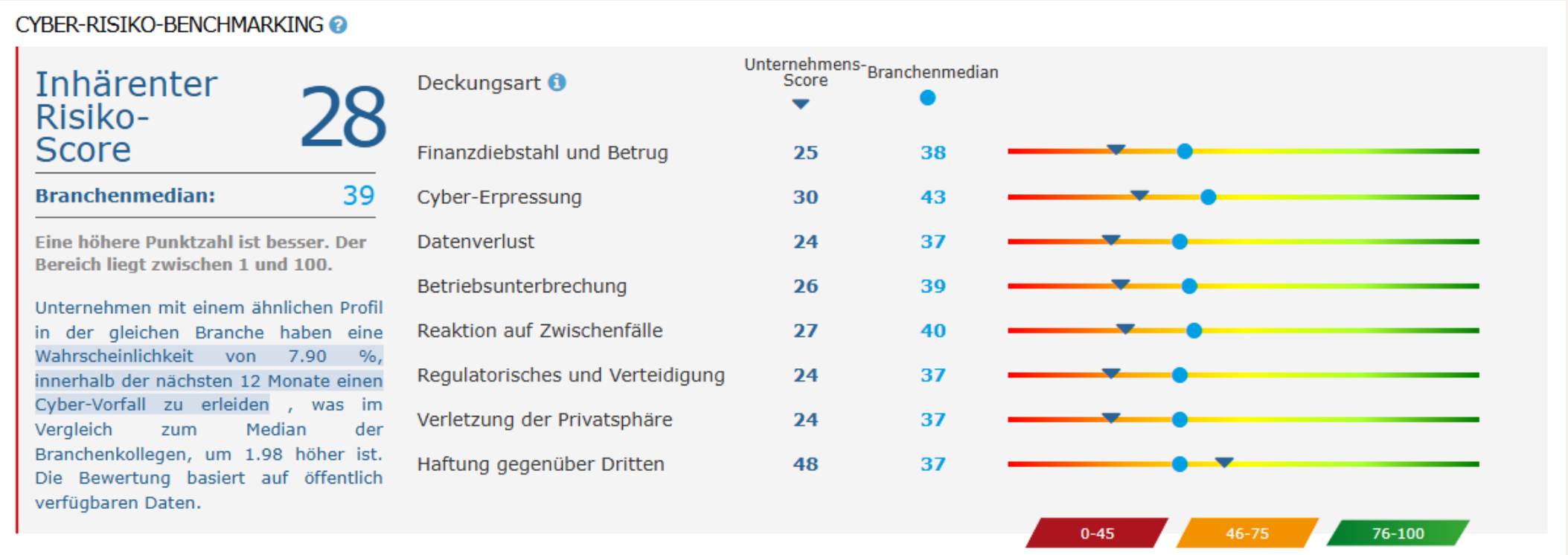
Der Risikofragebogen hilft dabei, **potenzielle Schwachstellen in der IT-Sicherheit und den Betriebsabläufen** des Unternehmens zu identifizieren, die vielleicht vorher nicht offensichtlich waren.

Ohne eine gründliche Risikoanalyse ist es schwierig, die richtige **Deckungssumme und die passenden Versicherungsbedingungen** zu ermitteln.

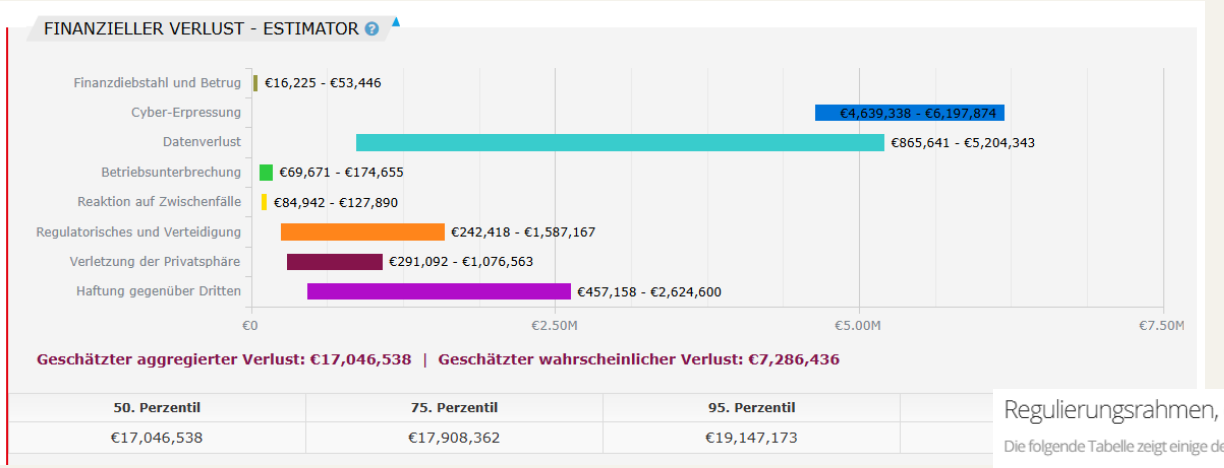
Ausführliche Risikoanalysen **beschleunigen den Angebotsprozess**

Websitescans: Mit Fakten, Fakten schaffen!

Scans der Websites und der im Darknet veröffentlichten Daten können sowohl dem Versicherer als auch dem Versicherungsnehmer Schwachstellen in der Risikostruktur aufzeigen. Versicherte sehen auf Anhieb ihre Schwachstellen in Verbindung mit ihrer Webseite.



Websitescans: Mit Fakten, Fakten schaffen!



50. Perzentil	75. Perzentil	95. Perzentil
€17,046,538	€17,908,362	€19,147,173

→ Mögliche Schadenhöhe kann den Versicherungsnehmer sensibilisieren.

→ Lücken bei Zertifizierungen aufzeigen

Regulierungsrahmen, die von den Ergebnissen beeinflusst werden

Die folgende Tabelle zeigt einige der regulatorischen Rahmenbedingungen, die von den Ergebnissen betroffen sind.

Art finden	AICPA – Trust Service Criteria (SOC 2 SM-Bericht)	Gemeinsame Bewertungen – SIG v6.0	95/46/EG – Datenschutzrichtlinie der Europäischen Union	ISO/IEC 27001:2013	ISO/IEC 27017:2015	NIST SP800-53 R3	PCI DSS v3.0	PCI DSS v3.2
Anfällige Technologien	(S3.10.0) Design, Erwerb, Implementierung, Konfiguration, Änderung und Verwaltung von Infrastruktur und Software stehen im Einklang mit definierten Systemsicherheitsrichtlinien, um autorisierten Zugriff zu ermöglichen und unbefugten Zugriff zu verhindern.	G.15.2, I.3	Artikel 17	8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1	12.6.1 15.1.1 15.1.3	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5	2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3	2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3
Anti-DDoS-Kontrollen					15.1.1 15.1.3			
E-Mail-Sicherheit (DMARC, SPF)				Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	12.4.1 12.6.1 CLD.9.5.2 15.1.1 15.1.3		2.1 2.2 2.5 5.1	2.1; 2.2; 2.5; 5.1

Antrag: Mindestanforderungen schützen den Versicherungsnehmer

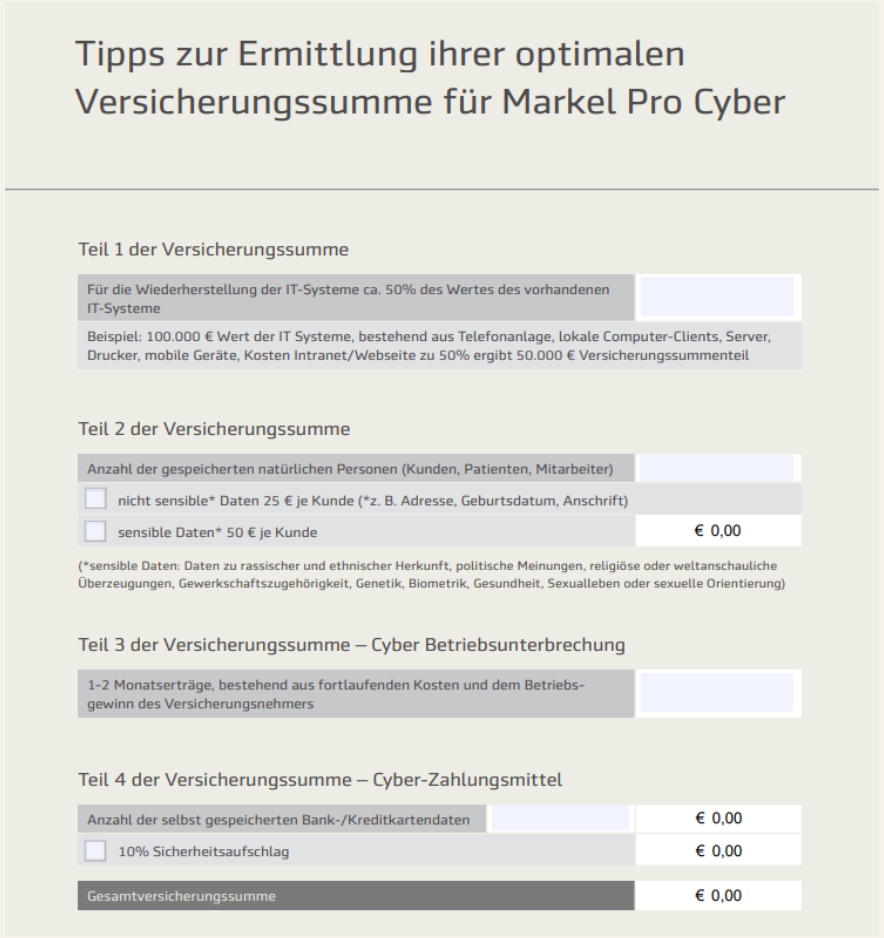
- Bei Antragsfragen handelt es sich um Mindestanforderungen
- „Das Risiko versicherbar gestalten“!
- Anhand weniger Fragen kann der Abschluss erfolgen
- Verständliche Fragestellung erleichtern den Abschluss

1. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: – Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung – Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck) – Klinik, Krankenhaus – Ratingagentur, Direktmarketing – Versorgungsunternehmen (z. B. Energie, Wasser, Telekommunikation)	Nein ☐
2. Der Antragssteller speichert personenbezogenene Daten von in den USA ansässigen Personen.	Nein ☐
3. Hat der Antragsteller in den letzten 5 Jahren Schäden durch Cyber- und Daten-Eigenschäden (z. B. Hacker-Angriffe, Erpressung, Schadsoftware) oder Cyber-Drittschäden über 1.500 € erlitten? Gab es Vorfälle wie Fake-President-Angriffe oder Vertrauensschäden? Sind Umstände bekannt, die zu einem Schaden oder einer Inanspruchnahme führen könnten? (Warnungen durch Firewalls oder Virenscanner ohne Auswirkungen sind nicht zu berücksichtigen.)	Nein ☐
4. Eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Antragsteller eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht.	Nein ☐
5. Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: – Anti-Virus-Schutz mit aktuellen Virendatenbanken, (Hiervon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux.) – Firewalls an allen Übergängen in das Internet für stationäre IT-Systeme, – regelmäßige (bis 1.000.000 € Umsatz mindestens wöchentliche, ab 1.000.000 € Umsatz mindestens tägliche) Datensicherungen auf separierten Systemen oder Datenträgern (zum Beispiel NAS, externe Festplatte, separierter Server).	Ja ☐
6. Bei einem Umsatz größer als 10 Millionen € ist nachfolgende Risikoinformation zusätzlich zu beantworten. Der Antragsteller nutzt darüber hinaus folgende Sicherheitsvorkehrungen: – Vier-Augen-Prinzip: Überweisungen über 10.000 € werden erst nach einer zusätzlichen Freigabe durchgeführt. – Sichere Netzwerkinfrastruktur: Kein Zugriff auf veraltete Systeme ohne Hersteller-Sicherheitsupdates (z. B. Windows 7/XP/NT) oder Nutzung eines separaten Netzwerks für solche Systeme. – Geschützter Fernzugriff: Fernzugriffe auf Systeme mit vertraulichen Unternehmens- und personenbezogenen Daten erfolgt ausschließlich über eine 2-Faktor-Authentifizierung (z. B. Authenticator-App) oder VPN-Tunnel. – Einsatz von Fertigungsmaschinen: Die Fertigungsmaschinen sind von externen Netzwerken und dem Unternehmensnetzwerk separiert.	Ja ☐

Weitere Tools zur Unterstützung

03

Versicherungssumme: Wie wird sie ermittelt?



Tipps zur Ermittlung ihrer optimalen Versicherungssumme für Markel Pro Cyber

Teil 1 der Versicherungssumme

Für die Wiederherstellung der IT-Systeme ca. 50% des Wertes des vorhandenen IT-Systeme	
Beispiel: 100.000 € Wert der IT Systeme, bestehend aus Telefonanlage, lokale Computer-Clients, Server, Drucker, mobile Geräte, Kosten Intranet/Webseite zu 50% ergibt 50.000 € Versicherungssummenteil	

Teil 2 der Versicherungssumme

Anzahl der gespeicherten natürlichen Personen (Kunden, Patienten, Mitarbeiter)	
☐ nicht sensible* Daten 25 € je Kunde (*z. B. Adresse, Geburtsdatum, Anschrift)	
☐ sensible Daten* 50 € je Kunde	€ 0,00

(*sensible Daten: Daten zu rassischer und ethnischer Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Genetik, Biometrik, Gesundheit, Sexualleben oder sexuelle Orientierung)

Teil 3 der Versicherungssumme – Cyber Betriebsunterbrechung

1-2 Monatserträge, bestehend aus fortlaufenden Kosten und dem Betriebsgewinn des Versicherungsnehmers	

Teil 4 der Versicherungssumme – Cyber-Zahlungsmittel

Anzahl der selbst gespeicherten Bank-/Kreditkartendaten	€ 0,00
☐ 10% Sicherheitsaufschlag	€ 0,00
Gesamtversicherungssumme	€ 0,00

- Die Ermittlung der Versicherungssumme stellt Versicherungsmakler immer wieder vor Probleme.
- Unterschiedliche Unternehmen benötigen unterschiedliche Summen.
- Die Cyberversicherung ist keine Sachversicherung. Der Wert der Hardware ist nur ein Anhaltspunkt. Digitale Assets und Daten werden oft zu gering bewertet.

Was gibt es noch?

Cyber-Versicherung für Unternehmen

IT-Sicherheit: Ihre Checkliste für die Cyber-Versicherung

IT-Sicherheit ist der erste Schritt zur Unternehmenssicherheit. Und Voraussetzung für den Abschluss einer Cyber-Police – der letzte Schritt zur Cyber-Sicherheit. Doch welche etablierten IT-Schutzmaßnahmen werden im Antrag abgefragt? Ein Überblick.

1. Virenschutz mit automatischen Updates

Beim Virenschutz sind vor allem zwei Dinge relevant:

- Desktop Computer, Laptops und Terminals müssen mit einem Antivirenprogramm, Virenscanner oder Virenschutzprogramm (AV) ausgestattet sein. Das AV muss sowohl auf Clients als auch auf allen Server-Systemen laufen, auf denen Dateien gespeichert und verarbeitet werden, da diese mit Schadsoftware infiziert sein könnten.
- Das installierte AV muss immer auf dem aktuellen Stand sein. Das ist gewährleistet, wenn der Virenschutz als sogenannter Echtzeitscanner – sprich mit einer Auto-, Internet- oder auch Live-Updatefunktion – arbeitet: aktuelle Virensignaturen werden automatisch beim Hersteller heruntergeladen.

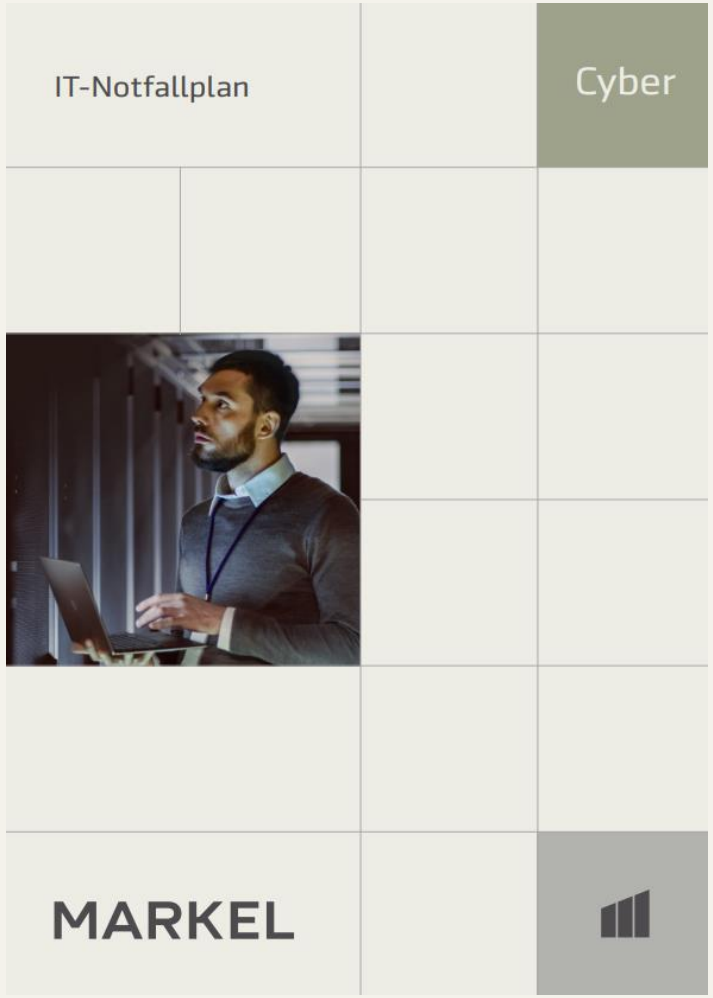
2. Firewalls an Schnittstellen

Besonders Schnittstellen zwischen internen und externen Netzen – beispielsweise zwischen firmeninternem Netz und Internet – müssen durch wirksame, individuelle Firewall-Strukturen an jedem Netzübergang betrieben werden. Nur so können nicht erwünschte Kommunikationsverbindungen zwischen beiden Netzen ausgeschlossen werden, indem das System den Kommunikationsfluss kontrolliert und filtert. Besonders sensible Netzbereiche sollte die Firewall ganz voneinander trennen.

3. Permanente Offline-Datensicherung

Datensicherung ist essenziell. Dafür sind Mindeststandards einzuhalten, die bestenfalls noch erweitert werden.

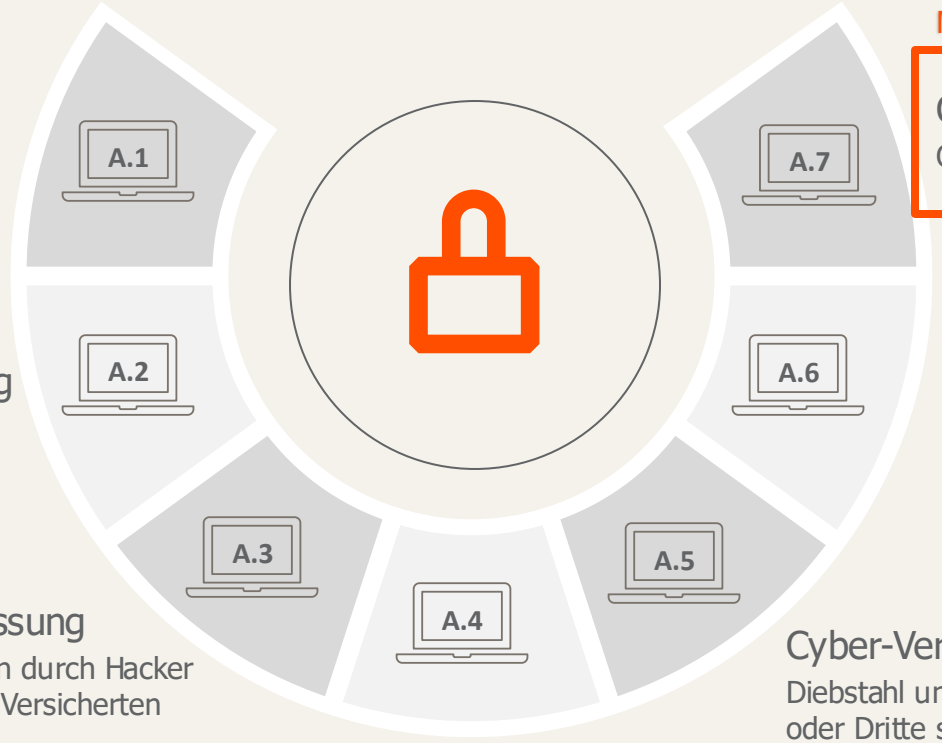
- Die Basis: Es ist mindestens eine vollständige Offline-Datensicherung (ausgesteckte externe Festplatte(n) oder sicher verwahrte Back-up-Bänder) etabliert, die nicht älter als eine Woche ist, damit eine Wiederherstellung sämtlicher kritischer Daten beziehungsweise Anwendungen für die Aufrechterhaltung des Geschäftsbetriebes möglich ist.
- Die Ergänzung: Optional ist es sinnvoll und üblich, stets zwei vollständige Back-ups offline und physisch vom IT-System getrennt vorzuhalten – falls eine Datensicherung einmal ausfällt bzw. nicht erfolgreich war, bleibt immer noch das zweite Back-up, um die Geschäftsfähigkeit aufrecht zu erhalten.



Markel Pro Cyber v2

04

Modularer Versicherungsschutz Markel Pro Cyber



Cyber Daten- und Eigenschäden

Wiederherstellung der Hard- und Software

Cyber-Betriebsunterbrechung

Ertragsausfall für den Zeitraum der versicherten Betriebsunterbrechung

Cyber-Erpressung

Geldforderungen durch Hacker gegenüber den Versicherten

Cyber-Zahlungsmittel

Forderungen der Kreditkartenindustrie wie z. B. Banken oder PayPal

NEU: automatisch inkludiert!

Cyber-Prävention

Online-Präventionsplattform von Perseus

Cyber-Haftpflicht

Haftpflichtansprüche seitens Dritten aus den Bereichen des Datenschutzes (EU-DSGVO, BDSG)

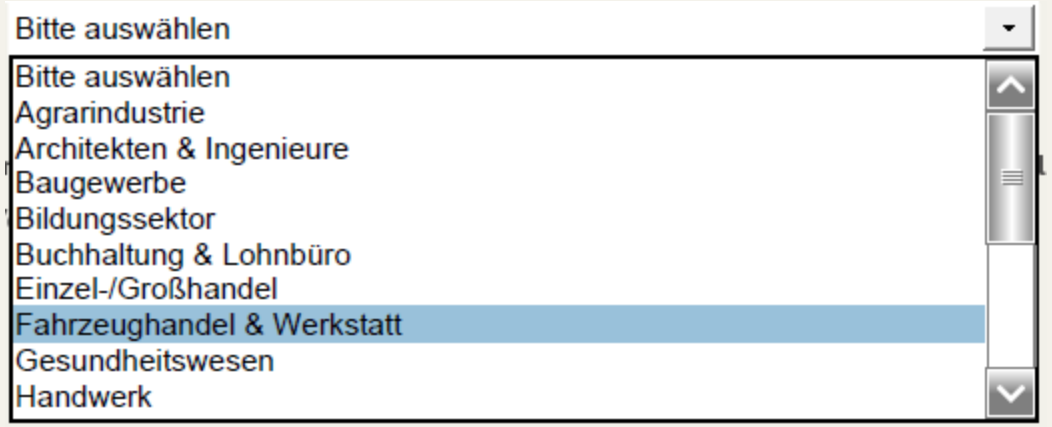
Cyber-Vertrauensschaden

Diebstahl und Betrug durch mitversicherte Personen oder Dritte sowie Fake-President, Social-Engineering.

Auch ohne Informationssicherheitsverletzung!

Neuer Antrag v2: One Fits All

- Branchenauswahl für mehr Sicherheit
- Nur noch 5 Risikofragen
  (bei Umsatz über 10 Mio. € 6 Fragen)
- Produktionsunternehmen und Versicherungsmakler auch versicherbar
- Verständlichere Logik bei Abwahl der Bausteine
- Nur noch Abwahlmöglichkeiten



Abwahl von Einzelbausteinen der Cyber-Versicherung

Baustein A.1	Cyber- und Daten-Eigenschaden (Grunddeckung und Pflichtmodul, nicht abwählbar)	
Baustein A.2	Abwahl Cyber-Betriebsunterbrechung	-15 %
Baustein A.3	Abwahl Cyber-Erpressung	-10 %
Baustein A.4	Abwahl Cyber-Zahlungsmittel	-7,5 %
Baustein A.5	Abwahl Cyber-Vertrauensschaden	-5 %
Baustein A.6	Abwahl Cyber-Haftpflicht	-10 %
Baustein A.7	Abwahl Cyber-Prävention	-5 %

Neuer Antrag v2: One Fits All

- Nicht versicherbare Risiken
- Vorschäden
- IT-Sicherheit

1. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: – Zahlungsabwicklung, -dienstleistung, Inkassodienstleistung – Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck) – Klinik, Krankenhaus – Ratingagentur, Direktmarketing – Versorgungsunternehmen (z. B. Energie, Wasser, Telekommunikation)	Nein ☐
2. Der Antragssteller speichert personenbezogenene Daten von in den USA ansässigen Personen.	Nein ☐
3. Hat der Antragsteller in den letzten 5 Jahren Schäden durch Cyber- und Daten-Eigenschäden (z. B. Hacker-Angriffe, Erpressung, Schadsoftware) oder Cyber-Drittschäden über 1.500 € erlitten? Gab es Vorfälle wie Fake-President-Angriffe oder Vertrauensschäden? Sind Umstände bekannt, die zu einem Schaden oder einer Inanspruchnahme führen könnten? (Warnungen durch Firewalls oder Virenscanner ohne Auswirkungen sind nicht zu berücksichtigen.)	Nein ☐
4. Eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen den Antragsteller eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht.	Nein ☐
5. Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: – Anti-Virus-Schutz mit aktuellen Virendatenbanken, (Hiervon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux.) – Firewalls an allen Übergängen in das Internet für stationäre IT-Systeme, – regelmäßige (bis 1.000.000 € Umsatz mindestens wöchentliche, ab 1.000.000 € Umsatz mindestens tägliche) Datensicherungen auf separierten Systemen oder Datenträgern (zum Beispiel NAS, externe Festplatte, separierter Server).	Ja ☐
6. Bei einem Umsatz größer als 10 Millionen € ist nachfolgende Risikoinformation zusätzlich zu beantworten. Der Antragsteller nutzt darüber hinaus folgende Sicherheitsvorkehrungen: – Vier-Augen-Prinzip: Überweisungen über 10.000 € werden erst nach einer zusätzlichen Freigabe durchgeführt. – Sichere Netzwerkinfrastruktur: Kein Zugriff auf veraltete Systeme ohne Hersteller-Sicherheitsupdates (z. B. Windows 7/XP/NT) oder Nutzung eines separaten Netzwerks für solche Systeme. – Geschützter Fernzugriff: Fernzugriffe auf Systeme mit vertraulichen Unternehmens- und personenbezogenen Daten erfolgt ausschließlich über eine 2-Faktor-Authentifizierung (z. B. Authenticator-App) oder VPN-Tunnel. – Einsatz von Fertigungsmaschinen: Die Fertigungsmaschinen sind von externen Netzwerken und dem Unternehmensnetzwerk separiert.	Ja ☐

- Daten von US-Bürgern
- Klagen und Ermittlungen
- Erweiterte Sicherheitsvorkehrungen

Was ist neu? MARKEL Pro Cyber v2

- Unternehmen bis 25 Mio. € Umsatz
- Versicherungssumme bis 2 Mio. €
- Technische Probleme bis 250.000 €
- Vertragsstrafen wegen verzögerter Leistungserbringung bis 250.000 €
- Haftpflichtansprüche mitversicherter Unternehmen untereinander

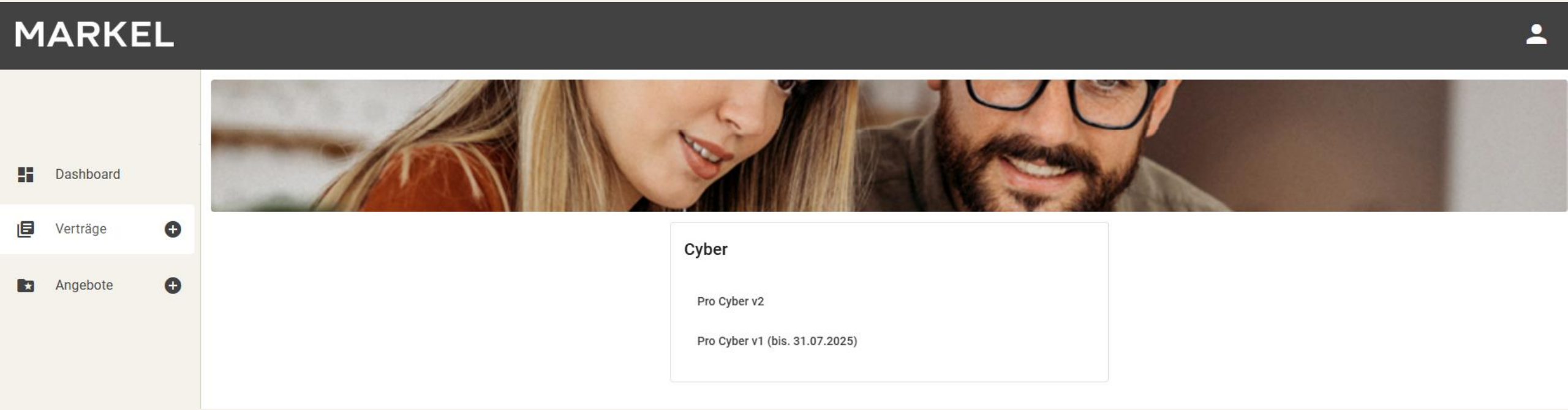
Bitte wählen Sie eine Versicherungssumme für die Cyber-Versicherung.

Vollständige Cyber-Versicherung mit allen Bausteinen A.1–A.7

Jahresumsätze bis \ **Versicherungssumme**	100.000 €	250.000 €	500.000 €	1.000.000 €	2.000.000 €
100.000 €	418 €	523 €	655 €	834 €	1.000 €
250.000 €	462 €	572 €	715 €	946 €	1.135 €
500.000 €	506 €	633 €	792 €	1.045 €	1.254 €
1.000.000 €	611 €	765 €	957 €	1.265 €	1.518 €
1.500.000 €	737 €	919 €	1.150 €	1.375 €	1.650 €
2.500.000 €	847 €	968 €	1.276 €	1.441 €	1.729 €
5.000.000 €	968 €	1.045 €	1.381 €	1.738 €	2.086 €
7.500.000 €	1.040 €	1.315 €	1.584 €	2.134 €	2.561 €
10.000.000 €	1.271 €	1.364 €	1.832 €	2.464 €	2.957 €
12.000.000 €	1.498 €	1.773 €	2.289 €	3.080 €	3.696 €
15.000.000 €	1.612 €	2.217 €	3.022 €	4.029 €	4.835 €
20.000.000 €	1.977 €	2.659 €	3.707 €	4.943 €	5.931 €
25.000.000 €	2.339 €	3.215 €	4.385 €	5.847 €	7.016 €

Weiterhin keine Obliegenheiten im Bedingungswerk!

Antragsstellung auch über MarkelNow



MARKEL