Markel

MARKEL PRO Cyber für Vermittler

KANZLEI MICHAELIS®
RECHTSANWÄLTE

MAILBOMBE

Unter einer Mailbombe versteht man das organisierte Verschicken einer Vielzahl von E-Mails (mit oder ohne Anhängen), um die E-Mail-Kommunikation des Empfängers zu blockieren. Inzwischen bietet das Internet eine Vielzahl frei downloadbarer Tools, über die es möglich ist, tausende von Mails gleichzeitig an einen Empfänger zu versenden. Dies führt – abhängig von Stückzahl und Mailgröße – zu immensen Verzögerungen im Arbeitsalltag. Nicht selten dauert es mehrere Stunden, bis alle Mails empfangen wurden und man sich wieder z. B. der Kommunikation mit Kunden zuwenden kann. Es ist zudem möglich, dass der Mailserver durch die Bombe überlastet wird und gar keine Mails mehr verarbeitet werden können.

Schadenbeispiel: Ein Callcenter wickelt u. a. für eine Direktbank die Kunden-, Telefon- und Mail-Hotline ab (First-Level). Ein Kunde der Bank startet aus Ärger über eine Anlageempfehlung eine Mailbombe, die aber natürlich beim Callcenter „einschlägt“ und die Mailkommunikation dort lahmlegt. Es vergehen zwei Tage, in denen keinerlei Mails beantwortet werden können. Es entstehen Kosten für die Untersuchung und Überstunden der Belegschaft zur Aufarbeitung des Rückstands.

DOS-ATTACKE (DENIAL OF SERVICE)

Denial of Service (kurz DoS; engl. für „Dienstverweigerung“) bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz verursacht werden. Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird von einer verteilten Dienstblockade oder Distributed Denial of Service (DDoS) gesprochen.

Schadenbeispiel: Ein mittelständischer Versand für Outdoor- und Military-Zubehör betreibt auch einen erfolgreichen Onlineshop, dessen Anteil am Gesamtumsatz über die Jahre auf 70 % anstieg. Bedingt durch das Sortiment machen ein paar studentische Aktivisten aus „dem linken Lager“ das Unternehmen als „Naziversand“ aus und starten über ein Bot-Net eine DDoS-Attacke, bei der der Shop tausende von Malen immer und immer wieder angefragt wird, bis der Server kapituliert. Da die Attacke über eine komplette Woche fortgesetzt wird, ist der Shop erst nach einigen technischen Änderungen wieder erreichbar. Die entstandenen Kosten: Technische Optimierung, Untersuchung, entgangener Umsatz für eine Woche, Imageschaden wg. Nichterreichbarkeit, etc.

DATENMISSBRAUCH

Datenmissbrauch hat ebenfalls viele Gesichter. Am häufigsten ist hier der betrügerische Missbrauch von Bank- und Kreditkartendaten der Kunden eines Unternehmens, da hiermit sehr schnell Geld ergaunert werden kann. Auch das Ausspionieren eines Unternehmens („Industriespionage“) fällt unter diese Kategorie der Cyber-Risiken. Zugang kann der Täter über Schadsoftware (z. B. Keylogger), Hardware (z. B. gestohlener PC) oder über Mitarbeiter (z. B. „geborgten“ Zugang) erhalten.

Schadenbeispiel: Die Kundendatenbank eines Autohauses wird gehackt. Dabei erbeuten die Täter u. a. sämtliche gespeicherten Kreditkartendaten der Kunden. Dem Autohaus entstehen Kosten für Forensik, technische Optimierung, Schadenersatzforderungen der betroffenen Banken, etc.

DATENSABOTAGE

Bei einem Datensabotageakt werden Daten beschädigt, verändert oder gelöscht. Dies kann über ein Schadprogramm erfolgen oder gezielt durch einen Eindringling vorgenommen werden.

Schadenbeispiel: Ein Auszubildender einer Werbeagentur nutzt seine Mittagspause dazu, im Betrieb einen Film herunterzuladen. Diesen legt er auf dem Firmenserver ab, wo ihn sich auch zwei Kollegen kopieren. Die Datei war mit einem Virus versehen, der beim Aufruf des Films die Computer befällt und sich über das Firmennetzwerk verbreitet. Der Virus löscht eine ganze Reihe von Dateien unwiederbringlich. Die Arbeit, die in diese Kundenaufträge investiert wurde, ist verloren - trotz angeordneter Überstunden können nicht alle Abgabetermine eingehalten werden. Es entstehen Kosten für die Forensik, technische Optimierung, Schadenersatzforderungen der Kunden, Kunden wandern ab und das Image der Firma hat schweren Schaden genommen.

DIGITALE ERPRESSUNG

Digitale Erpressung kann in verschiedenen Formen auftreten. Die größte Verbreitung findet über sog. „Ransomware“ statt, Schadprogramme wie z. B. der bekannte „BKA-Trojaner“. Hier wird in der Regel der Zugriff auf den eigenen Rechner blockiert und suggeriert, dass diese Blockade aufgehoben wird, wenn man eine Zahlung tätigt (z. B. als Bußgeld „getarnt“). Allerdings gibt es natürlich auch Fälle, in denen Firmen mit angedrohten DDoS-Attacken zur Lösegeldzahlung erpresst werden. Auch die Drohung, erbeutete Kundendaten zu veröffentlichen, etc. ist ein häufiger Erpressungsansatz.

Schadenbeispiel: Hackern gelingt es, Zugriff auf die Patientenakten eines Allgemeinmediziners zu erlangen. Nachdem die Datenbank erfolgreich kopiert wurde, schreiben sie den Praxisinhaber per Mail an und drohen mit der Veröffentlichung der Anamnesen – natürlich mit dem Vermerk, woher die Daten stammen. Gegen Zahlung einer gewissen Geldsumme via Western Union könne er die Veröffentlichung verhindern.

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

Es gibt keine unknackbare Sicherheit

Schadenshöhe pro Unternehmen
ø70.000€

Wer haftet bei Sicherheitslücken?

- Wiederherstellung von Betriebssystemen
- Umsatzeinbußen
- Technisches personal
- juristische Betreuung

EIGENSCHADEN

Die Haftpflicht Ansprüche Dritter

Die Haftpflicht
Ansprüche Dritter

- Überschneidungen mit Vermögenshaftpflichtversicherung
  Wer zahlt zuerst?
- Besondere Versicherungsbedingungen

Schäden ohne persönliches Verschulden des Versicherungsmaklers sind auch vom Versicherungsschutz erfasst

Die Haftpflicht Ansprüche Dritter

- A.1 Cyber- und Dateneigenschaden
- A.2 Betriebsunterbrechung
- A.3 Cyber-Erpressung
- A.4 Cyber-Zahlungsmittel
- A.5 Cyber-Vertrauensschaden
- A.6 Cyber-Haftpflicht

Bausteine des Produkts

- **A.1 Cyber- und Dateneigenschaden**
- A.2 Betriebsunterbrechung
- A.3 Cyber-Erpressung
- A.4 Cyber-Zahlungsmittel
- A.5 Cyber-Vertrauensschaden
- A.6 Cyber-Haftpflicht

Versicherungsschutz für Beschädigung, Zerstörung, Veränderung Blockierung oder Missbrauch von Daten infolge eines Hackerangriffs.

Bausteine des Produkts

- A.1 Cyber- und Dateneigenschaden
- **A.2 Betriebsunterbrechung**
- A.3 Cyber-Erpressung
- A.4 Cyber-Zahlungsmittel
- A.5 Cyber-Vertrauensschaden
- A.6 Cyber-Haftpflicht

Versicherungsschutz für Cyber-Betriebsunter-brechungsschäden durch Unterbrechung oder Beeinträchtigung des versicherten Geschäftsbetriebs der Versicherten

Bausteine des Produkts

- A.1 Cyber- und Dateneigenschaden
- A.2 Betriebsunterbrechung
- **A.3 Cyber-Erpressung**
- A.4 Cyber-Zahlungsmittel
- A.5 Cyber-Vertrauensschaden
- A.6 Cyber-Haftpflicht

Versicherungsschutz im Falle von Geld- oder Warenforderung durch Dritte im Zusammenhang mit angedrohter oder bereits erfolgter Beschädigung, Zerstörung, Veränderung, Blockierung oder den Missbrauch der IT-Systeme

Bausteine des Produkts

- A.1 Cyber- und Dateneigenschaden
- A.2 Betriebsunterbrechung
- A.3 Cyber-Erpressung
- **A.4 Cyber-Zahlungsmittel**
- A.5 Cyber-Vertrauensschaden
- A.6 Cyber-Haftpflicht

Versicherungsschutz bei dem Verstoß gegen Vertrags-pflichten von Kreditkarten-verarbeitungsvereinbarungen mit einem Kreditinstitut

Bausteine des Produkts

- A.1 Cyber- und Dateneigenschaden
- A.2 Betriebsunterbrechung
- A.3 Cyber-Erpressung
- A.4 Cyber-Zahlungsmittel
- **A.5 Cyber-Vertrauensschaden**
- A.6 Cyber-Haftpflicht

Versicherungsschutz für unmittelbar entstandene Vermögensschäden, die durch mitversicherte Personen bei Gelegenheit einer dienstlichen Tätigkeit durch vorsätzliche Verwirklichung eines Vermögensdeliktes verursacht werden.

Bausteine des Produkts

- A.1 Cyber- und Dateneigenschaden
- A.2 Betriebsunterbrechung
- A.3 Cyber-Erpressung
- A.4 Cyber-Zahlungsmittel
- A.5 Cyber-Vertrauensschaden
- **A.6 Cyber-Haftpflicht**

Versicherungsschutz, wenn sie von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden

Bausteine des Produkts

Markel

MARKEL PRO Cyber für Vermittler

KANZLEI MICHAELIS®
RECHTSANWÄLTE

Das oder die Geschäfts- und Fremdgeldkonten ist/sind im Rahmen “Cyber-Vertrauensschaden” mitversichert.

Sonderbedingungen von KMR

In Klarstellung zu dem A.2 Nummer 3 („Zeitlicher Selbstbehalt“) findet der vereinbarte zeitliche Selbstbehalt keine Anwendung auf den Ersatz der Mehrkosten.

Sonderbedingungen von KMR

- Versichert gelten fremde Vermögensschäden wegen
  - des Versäumens von Fristen, insbesondere bei dem Abschluss, der Änderung und Kündigung von Versicherungsverträgen und bei der berechtigten Schadenregulierung,
  - …
- infolge
  - eines unbefugten Eingriffs in die IT-Systeme (Hacker-Einbruch),
  - …
- durch
  - Dritte (zum Beispiel Hacker, Kriminelle),
  - eine mitversicherte Person bei Gelegenheit einer dienstlichen Tätigkeit mit der Absicht, den Versicherungsnehmer vorsätzlich zu schädigen (Innentäter) handelt.

Sonderbedingungen von KMR

Im Rahmen der Daten- und Cyber-Schaden gelten auch IT-Forensik-Kosten im Zusammenhang mit Spionage versichert.

Sonderbedingungen von KMR

Der Versicherer gewährt den Versicherten Versicherungsschutz für die Verletzung von Geheimhaltungs- oder Schweigepflichten sowie Vereinbarungen über Datenvertraulichkeit durch die Versicherten.

Hierunter fallt z.B. eine Verletzung besonderer berufsständischer oder branchenüblicher Geheimnisse, wie z.B. der ärztlichen Schweigepflicht, des Bankgeheimnisses oder der anwaltlichen Verschwiegenheitspflicht.

Sonderbedingungen von KMR

Versicherungsschutz erstreckt sich auf die Erstellung von Coupons, die im Falle eines Schadens an die Kunden ausgegeben werden.

Preisnachlass

Gutschein

Rabatt

Sonderbedingungen von KMR

Die Erstprämie gilt als unverzüglich entrichtet, wenn diese innerhalb 4 Wochen nach Erhalt der Police und Prämienrechnung bezahlt wird.

Sonderbedingungen von KMR

Werden während eines Versicherungsjahres prämienneutrale Bedingungsverbesserungen zwischen Alltrad GmbH, Kanzlei Michaelis und Markel vereinbart, so finden diese Verbesserungen mit sofortiger Wirkung Anwendung auf diesen Versicherungsvertrag.

Sonderbedingungen von KMR

Günstige Prämie
Erstjahresrabatt von 25 %

Exklusiv!!!

Schadenhilfe des VN durch die Kanzlei Michaelis

Der Versicherer ist damit einverstanden, dass im Falle einer Ablehnung von Versicherungsleistungsansprüchen die Kanzlei Michaelis durch den Versicherungsnehmer eingeschaltet werden kann.

Die Kanzlei Michaelis unterstützt den Versicherungsmakler in seiner beruflichen Aufgabe der Unterstützung bei der Schadenregulierung.

Die außergerichtlichen Kosten der Kanzlei Michaelis werden von dem Versicherungsmakler, der Alltrad GmbH, übernommen.

KANZLEI MICHAELIS®
RECHTSANWALTE

appRIORI Plus appRIORI Klara

Abonnement: 13306

NEU BEI APPRIORI

Fachtagung Kanzlei Michaelis

Videos der Vorträge

VERTRAGSMUSTER

Maklervertrag Schnellversion

Maklervertrag

Makleruftrag

Zusatzdokumente

Service-Vereinbarung

EIGENE VORLAGEN & DOKUMENTE

Merkliste

Dokumentenarchiv

DOKUMENTE

Care-Paket DSGVO

CarePaket DSGVO

Makler-Kompendium

Beratungs-Dokumentation

Betriebliche Altersversorgung

Betriebliche Krankenversicherung

FACHARTIKEL & NEWS

Stephan Michaelis, LL.M.

Prof. Dr. Schwintowski

Harald Müller-Delius, MBA

appRIORI

Kanzlei Michaelis

BUSINESS & UNTERNEHMEN

Kundenmagazin in:takt

An- & Verkauf

Cyber

SERVICE

FACHARTIKEL & NEWS

Stephan Michaelis, LL.M.

Prof. Dr. Schwintowski

Harald Müller-Delius, MBA

appRIORI

Kanzlei Michaelis

BUSINESS & UNTERNEHMEN

in:takt
Das Online-Magazin für eine sichere Zukunft

Kundenmagazin in:takt

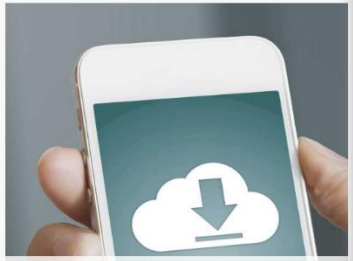
An- & Verkauf

Cyber

- Antrag Cyberdeckung Kanzlei Michaelis // Markel
- Verzichtserklärung Cyberdeckung Kanzlei Michaelis // Markel
- Sicherheit im Maklerbetrieb
- Feststellung IT-Sicherheit
- Verantwortlicher in der IT-Sicherheit

SERVICE

Einstellungen



Downloads

Klara Verwaltung

» Logout

Markel

MARKEL PRO Cyber für Vermittler

KANZLEI MICHAELIS®
RECHTSANWÄLTE

Musterrechnung

Vermittler-Name	Alltrad GmbH
Vermittler-Nr.	52547254

☑ Neuantrag
☐ Änderungsantrag

ANGABEN ZUM VERSICHERUNGSNEHMER

Name/Firma	Versicherungsmakler GmbH
E-Mail Adresse	info@kanzlei-michaelis.de
Straße/Nr.	Glockengießerwall 2
PLZ/Ort	20095
Firmengründung	

1 - RISIKOINFORMATIONEN

1. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: JA ☑
   - ☑ § 34d GewO Versicherungsvermittler,
   - ☐ § 34e GewO Versicherungsberater,
   - ☐ § 34f GewO Finanzanlagenvermittler,
   - ☐ § 34h GewO Honorar-Finanzanlagenberater,
   - ☐ § 34i GewO Immobiliardarlehensvermittler,
   - ☐ Vermögensverwalter, Anlagevermittler und sonstige Finanzdienstleistungen.
2. Der Antragsteller speichert von mehr als 7.500 natürlichen Personen die personenbezogenen Daten. NEIN ☑
3. Der Antragsteller erwirtschaftet oder erbringt in den USA direkte Umsätze oder Leistungen. NEIN ☐
4. Der Antragsteller bearbeitet, speichert oder übermittelt im Jahr mehr als 20.000 Kreditkartendaten. NEIN ☐
5. Der Antragssteller hatte in den letzten 5 Jahren Schäden durch eine Daten- oder Cyberrechtsverletzung, einen Hacker-Angriff oder -Eingriff oder eine Cyber-Erpressung, die zusammen 1.500 € übersteigen und/oder es sind Umstände bekannt, die zu einem Schadenseintritt oder einer Inanspruchnahme führen können. (Eine Warnung der Firewalls und Virenscanner ohne weitere Auswirkungen auf die IT-Systeme ist kein Vorschaden). NEIN ☐
6. 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 ☐
7. Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: JA ☑
   - 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)

Sollten Sie eine der oben genannten Risikoinformationen **nicht** ankreuzen können, bitten wir Sie um eine kurze Erläuterung im nachfolgenden Feld zu der jeweiligen Risikoinformation oder senden Sie uns den ausgefüllten Fragebogen Markel Pro Cyber zu.

2 - BEISPIELE FÜR HIGHLIGHTS UND VERSICHERTE RISIKEN

- Soforthilfe über unsere 24-Stunden-Schadenshotline
- Cyber-Notfallpläne und -Trainings
- Gezielte und ungezielte Hacker-Angriffe
- Gezielte und ungezielte Vireninfektionen
- Phishing von Bankdaten
- Diebstahl von Kunden- und Auftragsdaten
- Verschlüsselung von Firmendaten
- Geldforderungen von Hackern infolge eines Cyber-Angriffs
- Betrugsschäden durch Dritte
- Vertragsstrafen bei Verletzung von Geheimhaltungs- und Datenschutzverpflichtungen
- Hilfe und Unterstützung durch das Markel-Expertennetzwerk
- Ertragsausfallschäden durch Cyber-Vorfälle
- Schäden durch DDoS-Angriffe (Distributed Denial of Service)
- Schäden durch Fake President und Social-Engineering
- Diebstahl von EC- und Kreditkarten-Daten
- Cybervorfälle und Vertrauensschäden durch böswillige Mitarbeiter
- Bedienfehler an IT-Systemen
- Kosten bei behördlichen Verfahren
- Mitversicherung interner Datenschutzbeauftragter
- Schutz bei Abmahnungen und Urheberrechtsverletzungen

Die oben genannten Beispiele für versicherte Risiken beziehen sich auf alle Bausteine der Cyber-Versicherung und sind nicht abschließend. Versicherungsschutz wird gemäß den jeweils gewählten Bausteinen A.1 - A.6 des Bedingungswerkes Markel Pro Cyber 04.2019 gewährt.

3 - BEITRAGSTABLEAU

☑ 25 % Aktions-Nachlass für das erste Versicherungsjahr

Dieser Nachlass gilt einen Neuabschluss im Aktionszeitraum von 01.02.2020 bis 30.09.2020 (Versicherungsbeginn spätestens 01.01.2021). Der Nachlass wird für das erste Versicherungsjahr gewährt und erlischt automatisch zur nächsten Hauptfälligkeit.

Bitte wählen Sie eine Versicherungssumme für die Cyber-Versicherung. Die gewählte Versicherungssumme gilt als Jahreshöchstentschädigung für alle gewählten Bausteine.

VOLLSTÄNDIGE CYBER-VERSICHERUNG MIT ALLEN BAUSTEINEN A.1 - A.6

Jahresumsätze bis	Versicherungssumme				
	100.000 €	250.000 €	500.000 €	750.000 €	1.000.000 €
100.000 €	495 € ☐	620 € ☐	775 € ☑	900 € ☐	1.020 € ☐
250.000 €	545 € ☐	675 € ☐	845 € ☐	980 € ☐	1.120 € ☐
500.000 €	600 € ☐	750 € ☐	935 € ☐	1.085 € ☐	1.235 € ☐
1.000.000 €	720 € ☐	905 € ☐	1.130 € ☐	1.315 € ☐	1.495 € ☐
1.500.000 €	870 € ☐	1.085 € ☐	1.360 € ☐	1.495 € ☐	1.625 € ☐
2.500.000 €	1.000 € ☐	1.145 € ☐	1.510 € ☐	1.605 € ☐	1.705 € ☐
5.000.000 €	1.145 € ☐	1.235 € ☐	1.630 € ☐	1.845 € ☐	2.055 € ☐

Jahreshöchstleistung	Die Versicherungssumme steht einmal im Jahr zur Verfügung
Selbstbehalt	☑ 500 € ☐ 1.000 € (-5 % Nachlass) ☐ 2.500 € (-10 % Nachlass) ☐ 5.000 € (-15 % Nachlass) Es gilt ein zeitlicher Selbstbehalt von 8 Stunden in der Cyber-Betriebsunterbrechung, mindestens jedoch der gewählte Selbstbehalt.

Erzielen Sie einen höheren Jahresumsatz oder benötigen Sie eine höhere Versicherungssumme, verwenden Sie bitte den Fragebogen Markel Pro Cyber, um ein individuelles Angebot zu erhalten.

Rabatt: 100 €

Prämie: 358,67 €

ABWAHL VON EINZELBAUSTEINEN DER CYBER-VERSICHERUNG

Baustein A.1	Cyber- und Dateneigenschaden (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 %	☑

ZUWAHL DES BAUSTEINS CYBER-PRÄVENTION PREMIUM

Baustein A.7	Zuwahl Cyber-Prävention Premium (Online-Präventionsplattform von Perseus)	+ 20 %	☐

E-Mail Adresse des Ansprechpartners im Unternehmen:

4 - BEITRAGSBERECHNUNG

Grundbeitrag					775,00 €
Abwahl Baustein A.2 (Cyber-Betriebsunterbrechung)					- 116,25 €
Abwahl Baustein A.3 (Cyber-Erpressung)					- 77,50 €
Abwahl Baustein A.4 (Cyber-Zahlungsmittel)					- 58,13 €
Abwahl Baustein A.5 (Cyber-Vertrauensschaden)					- 38,75 €
Abwahl Baustein A.6 (Cyber-Haftpflicht)					- 77,50 €
Nachlass für abweichenden Selbstbehalt					- 0,00 €
Zuwahl Baustein A.7 (Cyber-Prävention Premium)					0,00 €
E-Mail Versandnachlass	-5 €	E-Mail:	info@kanzlei-michaelis	JA ☑	- 5,00 €
Bündelnachlass Bei Bestehen einer aktiven Berufshaftpflicht bei Markel	-5 %	Nummer:		JA ☐	- 0,00 €
Aktionsnachlass 25 %					- 100,47 €
1 Jahr Laufzeit des Vertrags mit automatischer Verlängerung				JA ☐	
10 % Laufzeitnachlass bei 3 Jahren Laufzeit des Vertrags mit automatischer Verlängerung				JA ☐	- 0,00 €

Zahlweise: ☑ jährlich ☐ halbjährlich (3 % Zuschlag) ☐ vierteljährlich (5 % Zuschlag)

(Bei halb- und vierteljährlicher Zahlung ist die SEPA-Lastschrift obligatorisch)

Gesamtjahresnettobeitrag (zuzüglich 19 % Versicherungssteuer und gegebenenfalls Ratenzuschlag)	301,41 €
Bruttobeitrag gemäß Zahlungsweise	358,67 €

5 - BEGINN UND HAUPTFÄLLIGKEIT

Beginn des Versicherungsvertrags (0.00 Uhr)	
Hauptfälligkeit (soweit abweichend vom Beginndatum)	
Laufzeit des Vertrags	**1 oder 3 Jahre mit automatischer Verlängerung**

Beginn: ↓ maximal **3 Monate** in der Vergangenheit (frei von bekannten Schäden und Verstößen) ↑ maximal **12 Monate** in der Zukunft (bis zu einen Monat vor Versicherungsbeginn eingetretene Schäden seit der Antragstellung sind bei Markel zu melden)

MARKEL®

6 - SEPA-LASTSCHRIFTMANDAT

Markel Insurance SE, Sophienstraße 26, 80333 München

Gläubiger-Identifikationsnummer	Mandatsreferenz
DE36ZZZ00002141857	Wird separat mitgeteilt

Ich ermächtige (Wir ermächtigen) Markel Insurance SE Zahlungen von meinem (unserem) Konto mittels Lastschrift einzuziehen. Zugleich weise ich mein (weisen wir unser) Kreditinstitut an, die von Markel Insurance SE auf mein (unser) Konto gezogenen Lastschriften einzulösen.

Hinweis: Ich kann (Wir können) innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem (unserem) Kreditinstitut vereinbarten Bedingungen.

Vorname und Name (Kontoinhaber)

Straße/Nr.

PLZ/Ort/Land

IBAN

Automatische IBAN Prüfung. Falsche IBAN wird **rot** angezeigt.

☐ **Hiermit bestätige ich das SEPA-Lastschriftmandat.**

Sollte das SEPA-Mandat nicht ausgefüllt werden, erhält der Antragsteller eine Rechnung ohne SEPA-Lastschrift.

7 - SCHLUSSERKLÄRUNG

Diese ausgefüllte Erklärung sowie die beigefügten Anlagen werden bei Vertragsabschluss Grundlage und Bestandteil des Versicherungsvertrags. Die Risikoangaben sind vorvertragliche Anzeigen. Hinsichtlich der Folgen bei Verletzung vorvertraglicher Anzeigepflichten verweisen wir auf die beigefügte Belehrung. Sie bestätigen, dass die gemachten Angaben vollständig und richtig sind und dass Sie folgende Dokumente rechtzeitig vor Antragsstellung erhalten und zur Kenntnis genommen haben: Markel Pro Cyber Bedingungen 04.2019, Informationspflichten Markel Pro Cyber 04.2019, Belehrung gemäß § 19 Absatz 5 VVG.

Sie bestätigen ferner, dass Sie unsere Allgemeine Datenschutzerklärung 04.2019 erhalten und deren Inhalt – insbesondere Ihre Rechte als Betroffener – zur Kenntnis genommen haben. Im Rahmen der Durchführung des Versicherungsvertrags sind wir auf die Verarbeitung von allgemeinen und personenbezogenen Daten angewiesen, welche wir unter Beachtung der maßgeblichen datenschutzrechtlichen Vorschriften und Einhaltung der gesetzlich vorgeschriebenen Standards verarbeiten, speichern und löschen.

☐ **Hiermit bestätige ich die Schlusserklärung.**

Durch wen erfolgt die Bestätigung?

☐ Versicherungsnehmer

☐ Versicherungsmakler/-betreuer

Name des Bestätigenden (keine Unterschrift notwendig).

Bitte drucken Sie diesen Antrag nicht aus, sondern senden Sie uns diesen am Computer ausgefüllt zurück.

Antrag prüfen und Versand vorbereiten

Vielen Dank für Ihre Aufmerksamkeit !

Ihr,

Stephan Michaelis

KANZLEI MICHAELIS®
RECHTSANWÄLTE