



Markel Pro Cyber

Einführung in die Cyber-Versicherung

Markel Insurance SE

Sophienstraße 26 | 80333 München | Telefon: +49 89 8908 316 50 | www.markel.de | service@markel.de



Ihr heutiger Referent

Daniel Blazquez



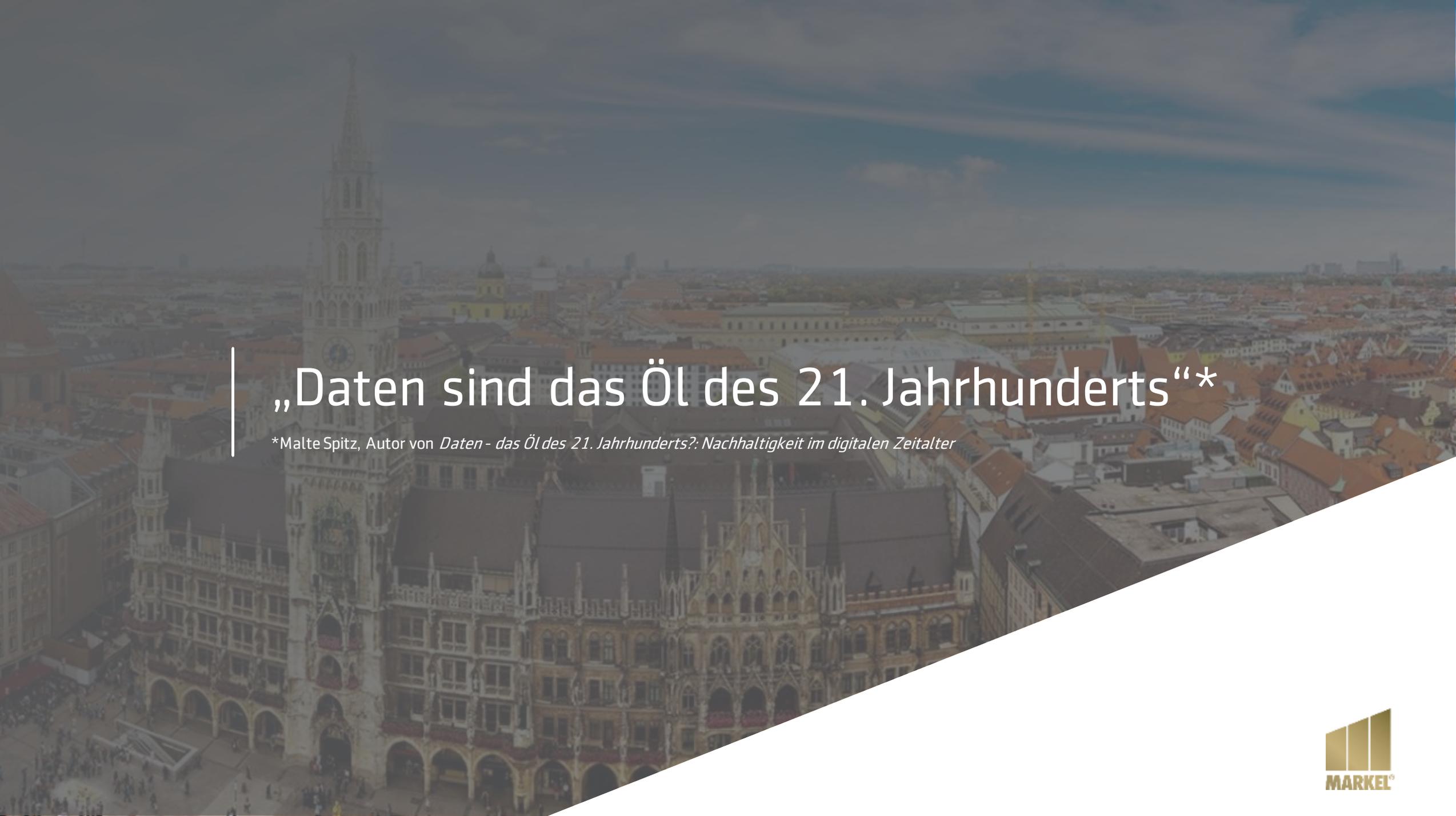
● **Head of Technology Lines**

● „Ich arbeite gerne bei Markel weil das Unternehmen **großes Potential** hat“

● **Langjährige Erfahrung** in der Versicherungsbranche

● Bei **Markel** Seit 2016

● Verantwortlich für **VSH und Cyber**



„Daten sind das Öl des 21. Jahrhunderts“*

*Malte Spitz, Autor von *Daten - das Öl des 21. Jahrhunderts?: Nachhaltigkeit im digitalen Zeitalter*

An aerial photograph of a city at dusk or dawn. The central focus is a large, ornate building with a prominent dome, likely a cathedral or government building. To its left, a tall, dark church spire rises above the rooftops. The city is densely packed with buildings, and the sky is a mix of dark blue and light grey, suggesting the time is either early morning or late evening. The overall atmosphere is quiet and somewhat somber.

Ihre Kunden, ihre Risiken

Cyberrisiken

Neue Herausforderungen für Ihre Kunden

COVID-19

Erhöhte Anzahl an Hacker-Angriffe aufgrund der Tätigkeit im Home Office



Anstieg von Ransomware Attacken

Unternehmen sind heutzutage einer großen Anzahl von Cyberrisiken ausgesetzt (Hacking, Phishing, DDOS etc.)

Internet of Things (IoT)

Vernetzte Geräte (auch Wearables) führen zu großen Sicherheitslücken



Meltdown und Spectre

Hardware-Hacks der Schwachstellen der Prozessoren der IT-Systeme

Erhöhte Gefahr von Cyberattacken in der Corona-Krise

Der digitale Virus greift die Cybersicherheit an

- Unzureichende IT-Kapazitäten
- Nicht ausreichend gesicherte VPNs (Virtual Private Networks)
- Fehlende Datenregulierungen
- Kein gesichertes Netzwerk
- Gebrauch von privaten IT-Systemen ohne Überprüfung von Datenschutz
- Mangelnde Datenschutzbildungen über das Arbeiten im Home Office

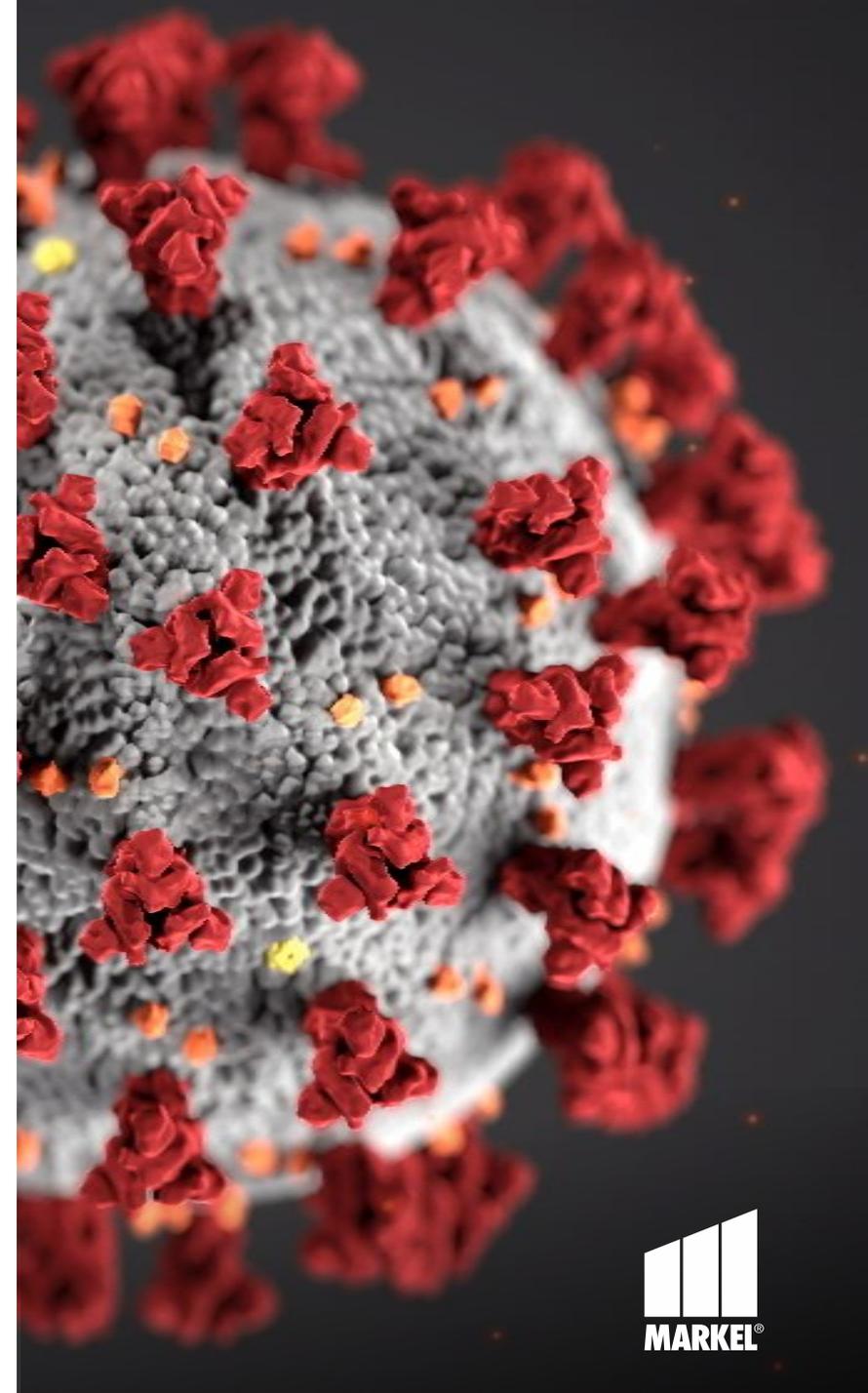


Die Cyber-Versicherung im Home Office

Markel Pro Cyber im Home Office

- ✓ Geltungsbereich der Cyberversicherung weltweit
- ✓ Vorbeugende Sensibilisierung der Mitarbeiter
- ✓ Mitversicherung der IT-Systeme und Daten des Arbeitgebers
- ✓ Mitversicherung des Zugriffs auf Programme und Daten des Arbeitgebers mit einem privaten Gerät

Tipp: Jedoch müssen die Mindeststandards an IT-Sicherheit auch im Home Office eingehalten werden. Das bedeutet auch für den Arbeitsplatz im Home Office müssen folgende Sicherheitssysteme aktiv sein.



Absicherung des heimischen Arbeitsplatzes

Tipps für das Arbeiten im Home Office



Verwenden Sie eine aktuelle Antivirensoftware mit Phishing-Schutz



Vertrauen Sie keinem E-Mail-Absender, den Sie nicht kennen



Geben Sie niemals Login-Daten preis



Machen Sie regelmäßig Backups auf externen Datenträgern, die vom System getrennt werden können



Sicherheitscheck auf den eingerichteten Remotesystemen



Nach dem Home Office:
„Quarantäne“ für die verwendeten IT-Systeme



Ransomware, Meltdown und Spectre

Gefahr für die Wirtschaft

Ransomware



Meltdown und Spectre



- Anstieg von internationalen Attacken von Malware im 2017 um 500 Prozent im Vergleich zum Vorjahr
- In Deutschland wurde ein Anstieg von 900 Prozent gemessen. Jedes achte Unternehmen war 2016 Opfer eines Cyberangriffs
- Im Jahr 2018 betrug die Anzahl an Cyberangriffen weltweit 116,5 Mio. €
- Der gesamte Schaden in diesem Bereich beläuft sich auf **55 Mrd. €**

Internet of Things (IoT)

Das Internet der Dinge

- Cyberrisiken die von neuen IoT-Geräten ausgehen, werden noch immer stark vernachlässigt
- Vernetzte TV-Geräte, Wearables und IP-Kameras sind meist ungenügend gesichert
- Unternehmen sind sich oft der Gefahr dieser Systeme nicht bewusst

Je mehr Geräte miteinander vernetzt werden, desto mehr steigt die Gefahr durch Cyberangriffe.



01

Cyber-Versicherung
Die Evolution von Cyberrisiken

Industrialisierung von Cyber-Attacken

Früher

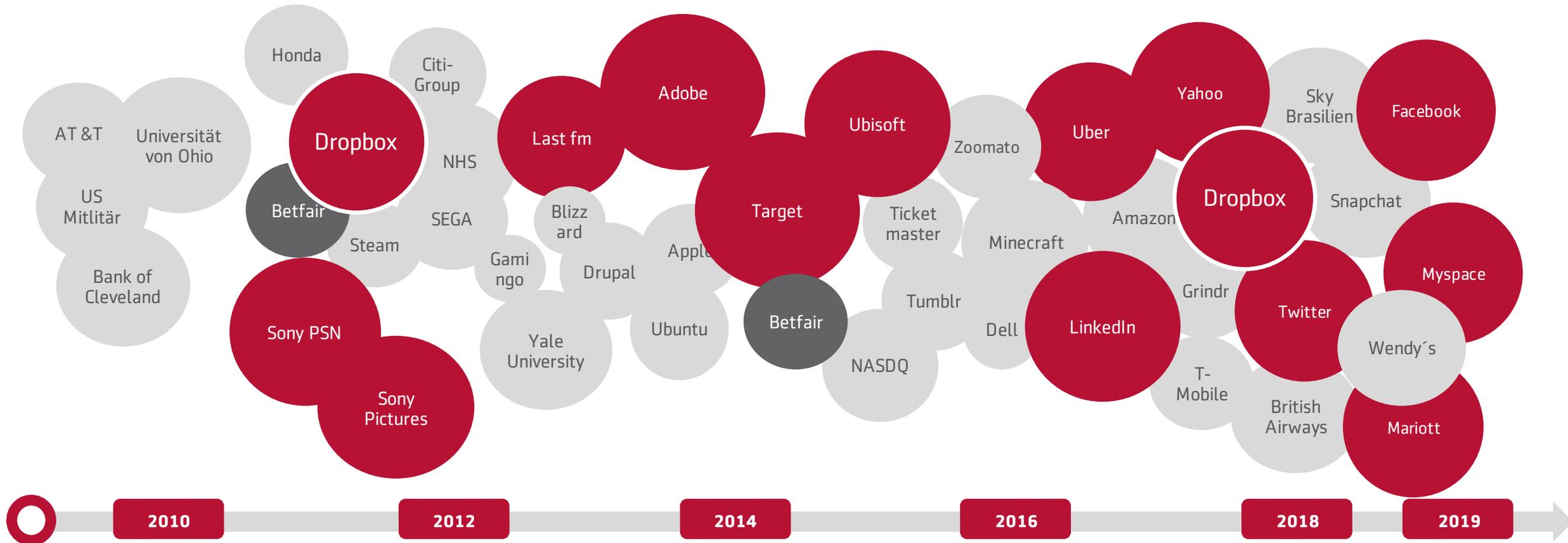


Heute



Die Evolution von Cyber-Angriffen

(● Angriffe mit mehr als 30.000 entwendeten Datensätzen)



Die Angreifer

Kennen Sie die Gegenspieler?

Hacker



Ziele

- Anerkennung
- Neugier befriedigen
- Spaß

Beispiele

- Script Kiddies
- Anonymous
- LulzSec

Kriminelle



Ziele

- Geld

Beispiele

- Lazarus Group (Wannacry)
- Mazafaka (Zeus Malware)

Staatliche Angreifer



Ziele

- Industriespionage
- Zerstörung der Infrastruktur
- Spionage/ Überwachung

Beispiele

- Stuxnet (USA/Israel vermutet)
- Ukrainische Kraftwerke (Russland vermutet)

An aerial photograph of a city, likely Munich, Germany, featuring a prominent Gothic cathedral with a tall spire in the foreground. The city is densely packed with buildings, and the sky is overcast. A white diagonal line runs from the bottom right corner towards the center of the image.

02 | Die Cybergefahren

Die Cybergefahren

Eingriff in die IT-Systeme

Identifizierung der Schwachstelle

Eingriff in die Systeme

Attacke auf die Systeme

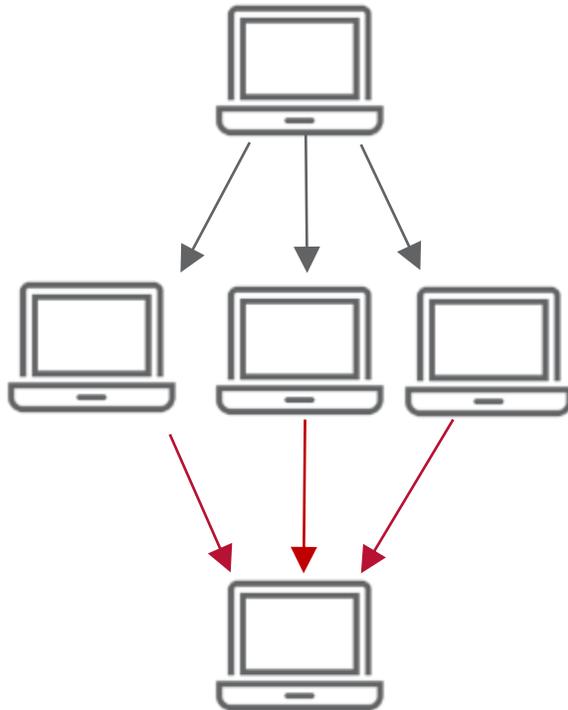


Hacker Attackieren die Systeme mit dem Ziel Daten zu **klauen**, zu **verändern**, zu blockieren oder zu **zerstören**.

22	sf-test.wko.at	194.107.236.108	80-10	SRV	Nein	Nein
23	sf-test.wko.at	194.107.236.108	80-08	SRV	Nein	Nein
24	mobile.sf-test.wko.at	194.107.236.109	80-10	SRV	Nein	Nein
25	mobile.sf-test.wko.at	194.107.236.109	80-08	SRV	Nein	Nein
26	ftp.wko.at	194.107.236.140	21 ftp	SRV	Ja	Nein
27	sftp.wko.at	194.107.236.171	22-22	SRV	Nein	Nein
28	webshop.wko.at	62.99.255.29	110 pop3	SRV	Nein	Nein
29	webshop.wko.at	62.99.255.29	21 ftp	SRV	Ja	Nein
30	webshop.wko.at	62.99.255.29	465 smtps	SRV	Nein	Nein
31	webshop.wko.at	62.99.255.29	995 pop3s	SRV	Nein	Nein
32	webshop.wko.at	62.99.255.29	993 imaps	SRV	Nein	Nein
33	webshop.wko.at	62.99.255.29	143 imap	SRV	Nein	Nein
34	webshop.wko.at	62.99.255.29	25 smtp	SRV	Nein	Nein
35	webshop.wko.at	62.99.255.29	587 smtp	SRV	Nein	Nein
36	epu.meinmarktplatz.wko.at, meinmarktplatz.wko.at, wkk.wko.at	91.216.249.66	21 Microsoft ftpd	SRV	Ja	Nein
37	quickcheck.wko.at	91.250.115.221	995 pop3s	SRV	Nein	Nein
38	quickcheck.wko.at	91.250.115.221	84-43	SRV	Nein	Nein
39	quickcheck.wko.at	91.250.115.221	25 Postfix smtpd	SRV	Nein	Nein

Die Cyber-Gefahren

Angriff auf die IT-Systeme

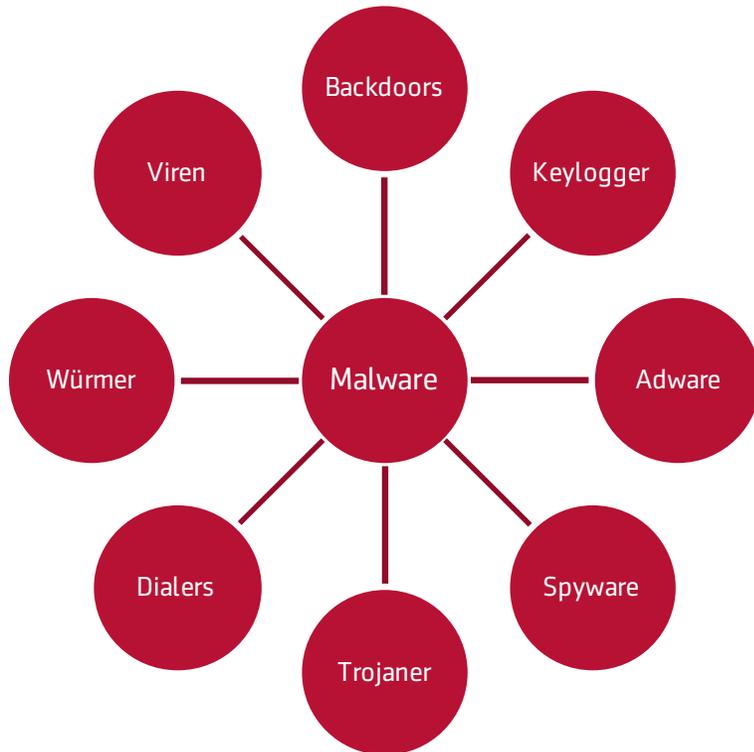


Hacker Attackieren die Systeme mit dem Ziel diese zu **unterbrechen** oder zu **blockieren**

Hierzu belasten Hacker meist Internetleitungen oder die Server durch eine Vielzahl von Anfragen, die dann zum **Absturz** oder **Blackout** der Systeme führen.

Die Cyber-Gefahren

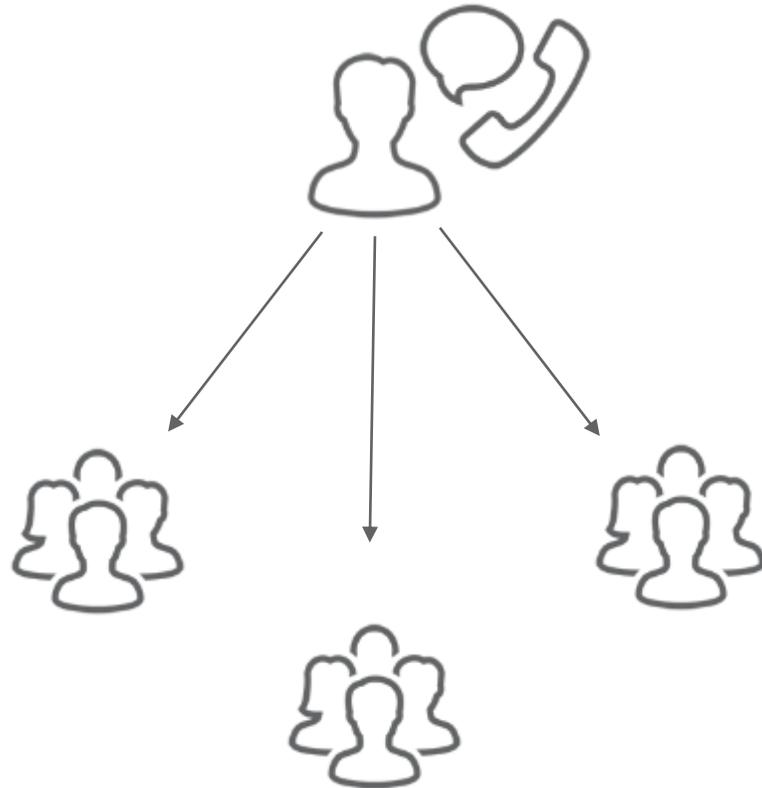
Infektion durch Schadsoftware



- **Infektion** der IT Systeme mit Schadsoftware, insbesondere Viren und Trojaner
- Hierdurch können Cyber-Eingriffe auf die **eigenen** IT Systeme ermöglicht werden
- Versehentliche Übermittlung von **Schadsoftware an Dritte kann zu Haftpflichtansprüchen führen**
- Viele Infektionen führen zu Straftaten, manche sind jedoch **willkürlich**, um einfach nur Schaden zu verursachen.

Risiko Mensch

Social Engineering

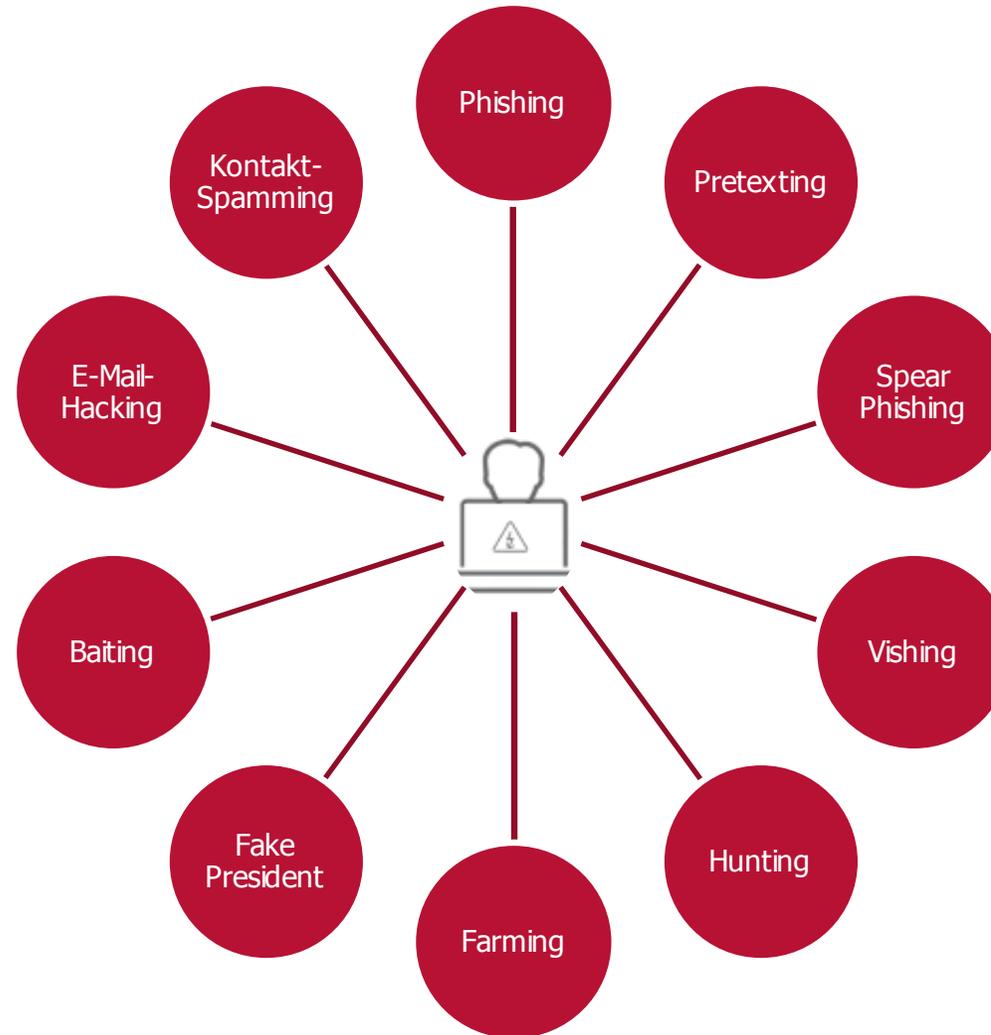


Als **Social Engineering** bezeichnet man die Beeinflussung von Personen mit dem Ziel von diesen geheime Informationen oder die Freigabe von Finanzmitteln zu erreichen (Phishing, Baiting, CEO-Fraud, Fake President, etc.)

- Angreifer sammeln alle öffentlich verfügbaren Daten, um die Abläufe innerhalb des Zielunternehmens grob kennenzulernen
- Hacker verteilen infizierte USB-Sticks in der Hoffnung, dass ein Mitarbeiter diesen verwendet (Dropping)

Social Engineering

Welche Arten von Social Engineering gibt es?



03 | Schadenbeispiele

Schadenfall bei Markel

Ungewöhnliche Netzwerkaktivitäten und Schadenmeldung über unseren IT-Forensiker

Nach telefonischer Rücksprache mit dem VN ist die Lage wie folgt:

- Der VN **meldet ungewöhnliche Netzwerkaktivitäten** seit Juni, welche er in den letzten Monaten immer wieder analysiert hat. Diese zeigen sich darin, dass Einstellungen auf PCs, Netzwerkspeichern und Internetroutern mehrfach verändert und Dokumente gelöscht worden sind.
- Während der Netzwerkanalysen sind ihm Netzwerkverbindungen nach Holland, Slowenien und Russland aufgefallen, welche durch keinen der vier PC Arbeitsplatz initiiert wurden.
- Er hat bereits alle gesammelten Informationen an das Bundeskriminalamt weitergeleitet, welches auch vor Ort war, aber keine Hilfestellung in der Beseitigung der Bedrohung geleistet hat.
- Aktuell sind alle Internetverbindungen getrennt, sodass Mitarbeiter die E-Mails privat abrufen. Er klagt außerdem darüber, dass die privaten E-Mailkonten der Mitarbeiter durch diese nicht mehr zugänglich sind, da die Passwörter geändert worden seien.



Schadenfall bei Markel

Regulierung der Schadens

Der VN ist bei europäischen Forschungsprojekten an Universitäten und Kliniken beteiligt. Inhalt dieser Projekte sind Gesundheitsplattformen, über welche Arzt- und Patientendaten verwaltet werden.

Aus unserer Einschätzung heraus in Bezug auf die Kritikalität der Daten, auf welche der VN direkt oder indirekt Zugang innerhalb der Forschungsprojekte hat, stellt der VN ein ernstzunehmendes Ziel für Gruppierungen dar, die auf das Infiltrieren von IT-Systemen zum Abgriff von Daten spezialisiert sind. Die o.g. Auswirkungen (verändern von Einstellungen, löschen von Dokumenten) sprechen dafür, dass das IT-Netzwerk des VN befallen ist. Wir können aktuell nur mutmaßen, dass PCs von außen gesteuert und Tastatureingaben mitgeschnitten werden, wenn eine Internetverbindung bestünde.

Dieser Fall bedarf einer weitergehenden Vor-Ort Analyse mit ggf. beauftragter Unterstützung zur Bereinigung der Systeme.

Markel hat die gesamten Kosten für Forensik, Betriebsunterbrechung, Systemwiederherstellung und –Verbesserung übernommen.

Diese Kosten beliefen sich in diesem Fall auf 48.000 €



Schadenfall und Regulierung

Aufwendige Wiederherstellung zweier Server nach Erpressungs-Trojaner

Versicherungsnehmer betreibt eine große Reinigungsfirma. Durch eine Ransomware-**Cyber-Attacke** wurden beide Server unseres Versicherungsnehmers verschlüsselt und eine Forderung von 700 Bitcoin zur Entschlüsselung der Systeme gestellt.

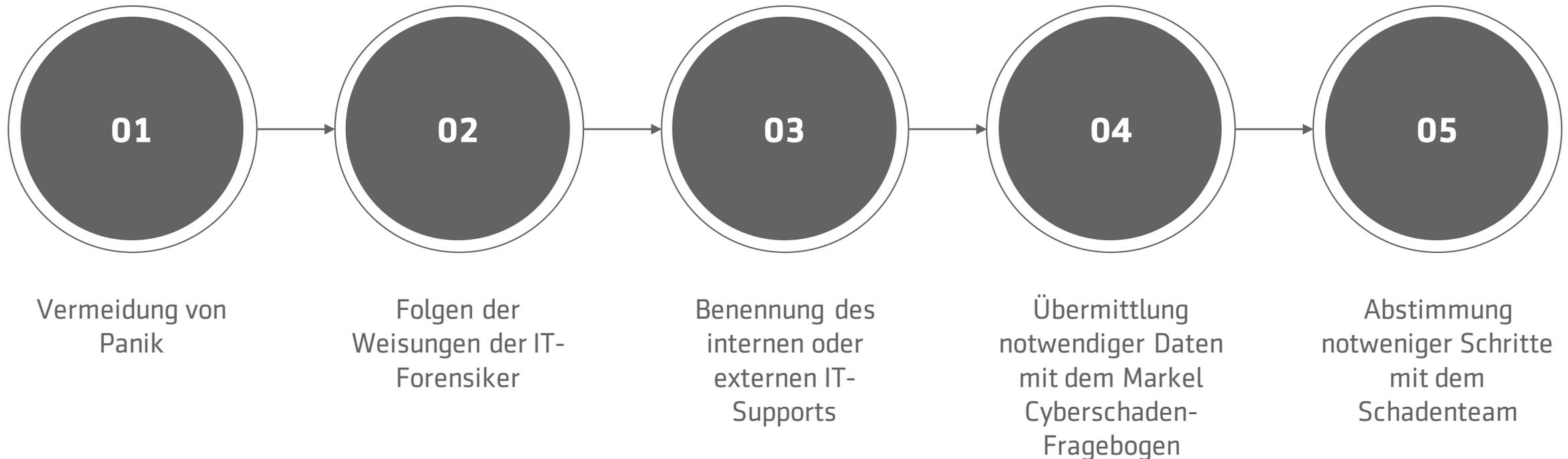
- Nach Absprache mit der Polizei wird auf die Forderung nicht eingegangen.
- Die Wiederherstellung aller Systeme zur Behebung des **Schadens** durch den eigenen, permanenten IT-Support des Versicherungsnehmers verursachte einen Aufwand von 150,5 Arbeitsstunden, die mit 12.040 € in Rechnung gestellt wurden. Um während der Zeit der Wiederherstellung noch größere Auswirkungen auf die Betriebsfähigkeit des Unternehmens zu vermeiden, musste zudem ein Leihserver angemietet und eingerichtet werden.

Zur **Regulierung** des Schadens wurden dem Versicherungsnehmer von uns die vom IT-Support in Rechnung gestellten Kosten in Höhe von 12.040 € sowie 1.915 € für den Leihserver erstattet.



Was tun im Schadenfall?

Halten Sie sich immer an diese fünf Punkte



04

Markel Pro Cyber
Ihre Kunden, ihre Vorteile

Ihr Kundenkreis

Diese Personengruppen können Sie absichern

Dienstleistung



- Arbeitsvermittlung
- Buchführungshelfer/-berater
- Call-Center
- Immobilienmakler
- Reisebüro
- U.v.m.

Freie Berufe



- Rechtsanwälte
- Steuerberater
- Wirtschaftsprüfer

Handwerk- und Baugewerbe



- Baugewerbe
- Handwerk
- Logistik- und Transport

Heilwesen



- Ärzte
- Pflegeeinrichtungen
- Krankenhäuser

Vereine, Verbände und Bildung



- Sportvereine
- Interessensvereine
- Berufsverbände
- Schulen

Markel Pro Cyber

Modularer Versicherungsschutz

- **Modularer** Aufbau mit sechs Bausteinen
- Deckungsinhalte **frei wählbar**
- **Eigenschaden und Drittschadenkomponenten**



Die 6 Bausteine der Cyber-Versicherung

Schadenbeispiele



Cyber- und Daten-Eigenschaden

Der Mitarbeiter einer Rechtsanwaltskanzlei öffnet den Anhang einer E-Mail, welcher einen Verschlüsselungstrojaner beinhaltet. Alle Daten auf den Systemen der Kanzlei werden somit unlesbar gemacht. Die Kosten für die IT-Forensik sowie die Entfernung der Schadsoftware und Installation neuer Sicherheitssoftware betragen 26.000 €.



Cyber-Betriebsunterbrechung

Ein Unternehmen wird mit einer Denial-of-Service-Attacke (DOS) angegriffen. Die Plattform und damit verbundene Dienste, sind 2 Tage für Kunden nicht erreichbar. Die Kosten für die Anmietung zusätzlicher Serverkapazitäten sowie die Kosten der Betriebsunterbrechung und Wiederherstellung der ursprünglichen Homepage belaufen sich auf 80.000 €.



Cyber-Zahlungsmittelschaden

Versicherungsschutz beim Verlust oder der Beschädigung von Kreditkartendaten und -programmen, Verstöße gegen Kreditkartenverarbeitungsvereinbarungen, Verletzungen der PCI Data-Security-Standards oder Verstöße gegenvertragliche Vereinbarungen im Zusammenhang mit Bezahlssystemen.

Die 6 Bausteine der Cyber-Versicherung

Schadenbeispiele



Cyber-Vertrauensschaden

Der Mitarbeiter eines Unternehmens hat Zugang zu mehreren Konten seines Arbeitgebers. Dies nutzt er aus, um sich über einen längeren Zeitraum kleine Beträge auf sein Privatkonto zu überweisen. Der über ein Jahr entstandene Schaden beträgt insgesamt 32.000 €.



Cyber-Haftpflicht

Ein Onlinebuchversand stellt kostenlose Leseproben zum Download zur Verfügung. Trotz aller Sicherheitsmaßnahmen wird eine infizierte Datei zum Download angeboten. Die IT-Systeme mehrerer Kunden werden dadurch infiziert. Der entstandene Gesamtschaden beläuft sich auf 30.000 €.



Cyber-Forderung

Ein Hacker verschafft sich Zugriff auf die IT-Systeme eines Steuerberaters und verschlüsselt wichtige Mandanten-Daten. Kurze Zeit später erhält der Steuerberater eine E-Mail mit der Forderung, den Betrag in Höhe von 8.000 € in Form von Bitcoins zu zahlen.

Cyber-Prävention mit perseus

Neu: Baustein A.7

ABWAHL VON EINZELBAUSTEINEN DER CYBER-VERSICHERUNG

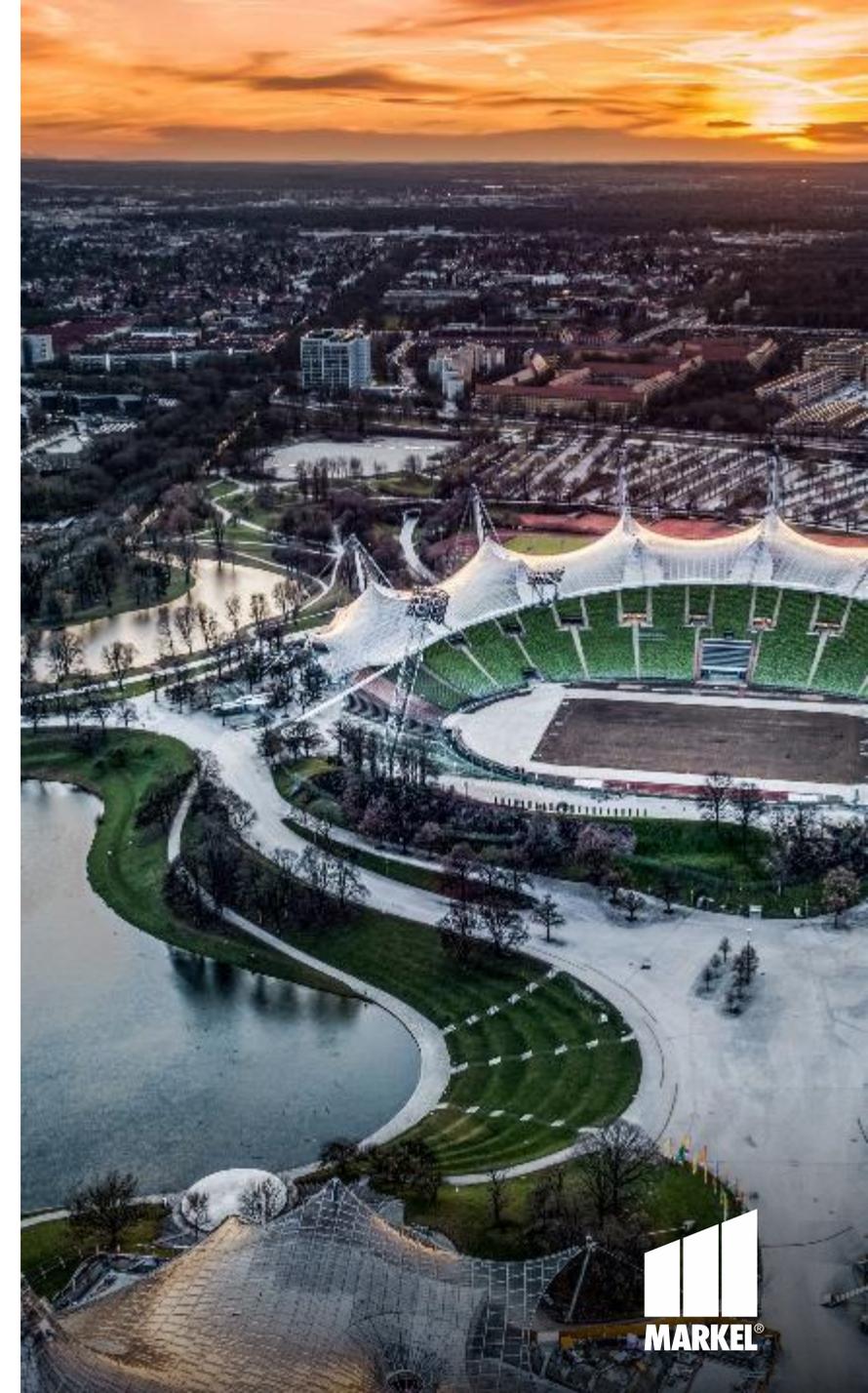
Baustein A.1	Cyber- und Dateneigenschaden (Grunddeckung und Pflichtmodul, nicht abwählbar)		
Baustein A.2	Abwahl Cyber-Betriebsunterbrechung	- 15 %	<input type="checkbox"/>
Baustein A.3	Abwahl Cyber-Erpressung	- 10 %	<input type="checkbox"/>
Baustein A.4	Abwahl Cyber-Zahlungsmittel	- 7,5 %	<input type="checkbox"/>
Baustein A.5	Abwahl Cyber-Vertrauensschaden	- 5 %	<input type="checkbox"/>
Baustein A.6	Abwahl Cyber-Haftpflicht	- 10 %	<input type="checkbox"/>

ZUWAHL DES BAUSTEINS CYBER-PRÄVENTION PREMIUM

Baustein A.7	Zuwahl Cyber-Prävention Premium (Online-Präventionsplattform von Perseus)	+ 20 %	<input type="checkbox"/>
--------------	---	--------	--------------------------

E-Mail Adresse des Ansprechpartners im Unternehmen:

Premium Dienstleistung zur Cyber-Prävention



Cyber-Prävention Premium

Neu: Baustein A.7

Cyber-Prävention Basis (prämienneutral enthalten)

- ✓ Einmalige IT-Sicherheitsprüfung
- ✓ Online-Training Cybersicherheit & Datenschutz für maximal 3 Mitarbeiter
- ✓ Einmaliger Phishing-Test
- ✓ Browser-Check
- ✓ Passwort Generator
- ✓ Checklisten

Cyber-Prävention Premium

- ✓ Online-Training für Cybersicherheit und Datenschutz für unbegrenzte Anzahl von Mitarbeitern
- ✓ Laufende Phishing-Tests
- ✓ Online -Konten-Check
- ✓ E-Mail-Scanner
- ✓ Systematische und gezielte Aktivierung der Mitarbeiter zur Nutzung der Tools
- ✓ Angriffsalarm
- ✓ Reporting Bereich mit Online-Trainings-Statistik und Cyber-Sicherheits-Scores

Markel Pro Cyber Mehrwerte

Was macht unser Produkt aus?

Verständlichkeit

- ✓ **verständliche** und **klare Sprache** der Bedingungen
- ✓ **Verständnis** für den **Versicherungsschutz und - Umfang**
- ✓ Die meisten Unternehmer sind keine Experten!

Modularität

- ✓ Versicherungsschutz ist an die **Bedürfnisse des Kunden** angepasst
- ✓ **niedrige Einstiegsprämie**, besonders für kleine Unternehmen interessant

Umfang

- ✓ Mitversicherung von **ungezielten Angriffen**
- ✓ Mitversicherung **aller Arten von Schadsoftware**
- ✓ Umfangreiche **Assistance** Leistungen

Highlights I

Markel Pro Cyber

24-Stunden-Cyber-Hotline mit IT-Support und
IT-Forensik

Mitversicherung von **ungezielten Angriffen**
(keine Einschränkung auf gezielte Angriffe)



Modularer Aufbau für **maßgeschneiderten**
Versicherungsschutz für den
Versicherungsnehmer

Mitversicherung **aller Arten von Cyber-**
Angriffen ohne Einschränkungen (zum Beispiel
DoS, DDoS)

Highlights II

Markel Pro Cyber

Mitversicherung **aller Arten** von **Cyber-Einbrüchen ohne Einschränkungen** (zum Beispiel Golden-Tickets, Zero-Day-Lücken)



Mitversicherung **aller Kundendaten** des Versicherungsnehmers, insbesondere Kreditkarten, Internetbankingdaten, Zugangsdaten für Bezahlssysteme, E-Mail-Accounts

Absicherung **aller IT-Systeme, Programme und Daten** des Versicherungsnehmer (auch auf mobilen Geräten)

Primäre Cyber-Deckung ohne Subsidiarität

An aerial photograph of a city, likely Munich, featuring a prominent Gothic cathedral with a tall spire in the foreground. The city is densely packed with buildings, and the sky is overcast. A white diagonal line cuts across the bottom right corner of the image.

05 | Markel Pro Cyber
Vertriebsunterstützung

Die Digitale Informationsmappe Cyber

Unterlagen für die Beratung von Cyber



Die Infobroschüre

Wie kann ich den Kunden einfach und plausibel für Cyber sensibilisieren und ihm das Thema vermitteln?

In einfachen Worten und wenigen Punkten dem Kunden das Thema Cyber näher bringen. Einstieg in den Sales Funnel.



Die Produktbroschüre

**Schadenbeispiele gefällig?
Dezierte Infos zum Produkt?**

Fachinformationen zum Produkt, Schadenbeispiele für jeden Baustein.



Die Cyber-Synopse

Unsicher, ob Markel der richtige Partner ist?

Vergleichen Sie einfach und schnell mit unserer ausführlichen Synopse die Leistungen von 6 Versicherern.



Vertriebsunterstützung **Highlights**

Die Kundenanalyse

Der perfekte Leitfaden für Ihr Kundengespräch

Die Cyberversicherung

Die größten Cyberrisiken für Unternehmen

Stillstand des Betriebs

Ungewolltes infizieren Dritter
(Kunden oder Lieferanten)
mit Schadsoftware

Datenschutzverstöße

Diebstahl oder Zerstörung
aller Daten



Zerstörung der
Soft- oder Hardware

Cyberspionage

Gezielte Manipulation wie
Fake President und
Social Engineering

Erpressung

Die Cyberversicherung

Zahlen, Daten & Fakten

70%

erfolgreicher Cyberangriffe erfolgen per E-Mail

24%

der befragten Unternehmen waren bereits
Opfer einer erfolgreichen Cyberattacke

80%

gehen davon aus, ausreichend gegen
Cyberkriminalität geschützt zu sein

50%

der KMUs waren mindestens einmal Opfer eines
Cyberangriffs im vergangenen Jahr

Quellenangaben: Forsa Befragung Frühjahr 2019 im Auftrag des GDV

Ermittlung der passenden Versicherungssumme

Mit ein paar Klicks

MARKEL PRO CYBER

ERMITTLUNG DER VERSICHERUNGSSUMME

TEIL 1 DER VERSICHERUNGSSUMME

Für die Wiederherstellung der IT-Systeme (ca. 50% des Wertes des vorhandenen IT-Systems)
(Detail: 100.000 € Wert der IT-Systeme, bestehend aus Teilbeständen, (eigenen Computer-Clients, Server, Clouds, mobile Geräte, Know-How) / Wert bis zu 50% (bis zu 50.000 € Versicherungssumme))

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

*Sensible Daten: Daten zu rechtlicher und ethischer Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Genetik, Biometrie, Gesundheit, Sexualleben oder sexuelle Orientierung

TEIL 3 DER VERSICHERUNGSSUMME - CYBER-BETRIEBSUNTERBRECHUNG

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

TEIL 4 DER VERSICHERUNGSSUMME - CYBER-ZAHLUNGSMITTEL

Anzahl der selbst gespeicherten Bank-/Kreditkartendaten

10% Sicherheitsaufschlag

GESAMTVERSICHERUNGSSUMME

DIE MARKEL PRO CYBER BAUSTEINE

Sollten Sie eine der Fragen mit "JA" beantworten, empfehlen wir Ihnen den

A.1 Cyber- und Datenschutzschaden

Der Grundbaustein für die Datenforensik, Wiederherstellung und die weiteren

A.2 Cyber-Betriebsunterbrechung

Ohne funktionierende IT steht mein Betrieb still?

A.3 Cyber-Erpressung

Ohne Zugang zu meinen Unternehmensdaten steht mein Betrieb still?

A.4 Cyber-Zahlungsmittel

Speichern oder verarbeiten Sie Zahlungsdaten Ihrer Kunden auf Ihrem System?

A.5 Cyber-Vertrauensschaden

Haben Mitarbeiter Zugang zu Firmenkonten?
 Haben Sie Befürchtungen, dass Ihre Firma Opfer von Cyberbetrug werden könnte?

A.6 Cyber-Haftpflicht

Speichern oder verarbeiten Sie personenbezogene Daten (DSGVO) auf Ihrem System?
 Vereinbaren Sie mit Kunden Vertragsstrafen bei Verletzungen von Geheimnissen?

A.7 Cyberprävention Premium

Legen Sie Wert darauf, dass Sie und alle Ihre Mitarbeiter dauerhaft zum Thema Cybersicherheit sensibilisiert werden?

JA NEIN

DIE CYBERLÖSUNG VON MARKEL – MEHR ALS NUR VERSICHERUNG

- Cyberprävention – Leistung bereits ab Vertragsabschluss
- Notfallhilfe – 24h professionelle Unterstützung von Spezialisten im Schadensfall
- Zahlung – Kostenübernahme beim Schadensfall

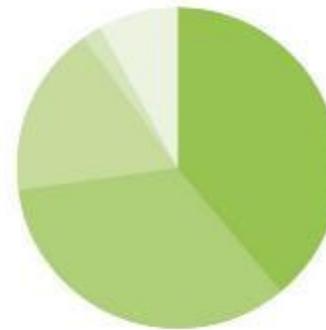


TIPPS ZUR ERMITTLUNG IHRER OPTIMALEN VERSICHERUNGSSUMME FÜR MARKEL PRO CYBER

UNSERE KUNDENENTSCHEIDUNGEN

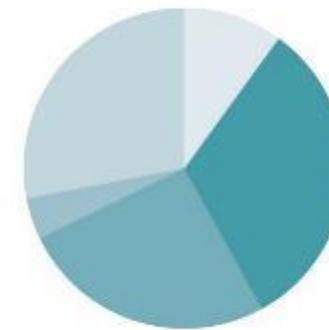
Um Ihnen die Entscheidung der für Sie richtigen Versicherungssumme etwas zu erleichtern, haben wir die Versicherungssummenentscheidung von 2.000 unserer Kunden nach dem Umsatz des Unternehmens analysiert — So haben sich unsere Kunden entschieden!

→ Bewegen Sie Ihren Mauszeiger über den jeweiligen Bereich des Diagramms, um die Versicherungssummenverteilung zu erfahren.



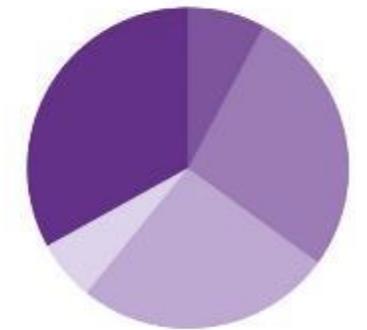
Unternehmen mit bis 1 € Mio. Umsatz

Die meisten Kunden (39%) wählten eine Versicherungssumme von 100.000 €



Unternehmen mit 1 - 2,5 € Mio. Umsatz

Die meisten Kunden (32%) wählten eine Versicherungssumme von 250.000 €



Unternehmen mit 2,5 - 10 € Mio. Umsatz

Die meisten Kunden (33%) wählten eine Versicherungssumme von 1.000.000 €



06 | Markel Pro Cyber
Antrag und Fragebogen

Das Antragsmodell der Cyber-Versicherung

- ✓ **Selbstrechnend & intelligent**
- ✓ Häkchen setzen – und der **Kunde ist versichert**
- ✓ **VVG konform und haftungssicher**

Vermittler-Name

Wahlverband/* pool

Vermittler-Nr.

Neuantrag Änderungsantrag

Vertrags-Nr.

Noch keine Anbindung (www.markel.de/anbindung/)

ANGABEN ZUM VERSICHERUNGSNEHMER

Name/Firma

E-Mail-Adresse

Straße/Nr.

PLZ/Ort

Firmengründung

1 - RISIKOINFORMATIONEN

1. Der Antragsteller betreibt ein produzierendes Gewerbe. NEIN
Unter die Kategorie produzierendes Gewerbe fallen Unternehmen mit Fertigungsanlagen, -anlagen und -stellen. Beispiele sind Hersteller von Spiel- und Sportausrüstung, KFZ-Zulieferbetriebe und werkzeugherstellende Kraftwerke.
Dieses Antragsmodell gilt für Dienstleistungsunternehmen, Selbstständige, freie Berufe (Rechtsanwälte, Steuerberater, Ärzte), Gesundheits- und Heilberufe, Handel, Bildungseinrichtungen, Gastronomie, Hotellerie, Vereine, Verbände, Baugewerbe, Handwerk, Transport, Logistik sowie Land- und Forstwirtschaftsbetriebe.
2. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: NEIN
 - Zahlungsbücherei, -dienstleistung, Inkassodienstleistung
 - Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck)
 - Ratingagentur, Vermögensverwaltung, Finanzdienstleistung, Direktvertrieb
 - Anbieter, Vermittler oder Berater von Versicherungen oder Finanzdienstleistungsprodukten
-> diese Tätigkeiten können Sie über unser Produkt **Markel Pro Cyber für Vermittler** absichern
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 Antragsteller hatte in den letzten 5 Jahren Schäden durch eine Daten- oder Cyberrechtverletzung, einen Hacker-Angriff oder -Eingriff oder eine Cyber-Erpressung, die zusammen 1.500 € übersteigen und/oder es sind Umstände bekannt, die zu einem Schadensereignis oder einer Inanspruchnahme führen können. (Eine Warnung der Firewalls und Virusscanner ohne weitere Auswirkungen auf die IT-Systeme ist kein Vor Schaden). 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 Virusdatenbanken (davon ausgenommen sind die Betriebssysteme von Apple, Unix und Linux)
 - Firewalls an allen Übergängen in das interne für geschäftliche IT-Systeme
 - regelmäßige (bis 1.000.000 € Umsatz mindestens wöchentliche, ab 1.000.000 € Umsatz mindestens tägliche) Datensicherungen auf separaten Speichermedien oder Datenträgern (zum Beispiel NAS, externe Festplatte, separater Server)

Sollten Sie eine der oben genannten Risikoinformationen **nicht** antworten können, bitten wir Sie um eine kurze Erläuterung im nachfolgenden

Der Fragebogen der Cyber-Versicherung

Fragebogen nur nötig bei negativ beantworteten Risikofragen oder höheren Deckungssummen/Umsätzen

Vermittler-Name	<input type="text"/>	<input type="checkbox"/> Neuantrag	
Vermittler-Nummer	<input type="text"/>	<input type="checkbox"/> Änderungsantrag	Vertrags-Nr. <input type="text"/>
Maklerverbands/-pool	<input type="text"/>		

ANGABEN ZUM VERSICHERUNGSNEHMER

Name/Firma	<input type="text"/>
Straße/Nr.	<input type="text"/>
PLZ/Ort	<input type="text"/>
Firmengründung	<input type="text"/>

1 - TÄTIGKEITS-, BETRIEBSBESCHREIBUNG:

2 - RISIKOINFORMATIONEN

1. Sie erwirtschaften derzeit einen Jahresumsatz von mehr als 10.000.000 € und die benötigte Versicherungssumme beträgt mehr als 1.000.000 €. NEIN
2. Der Antragsteller betreibt ein produzierendes Gewerbe. NEIN

Unter die Kategorie produzierendes Gewerbe fallen Unternehmen mit Fertigungsanlagen, -anlagen und -stätten. Beispiele sind Hersteller von Spiel- und Sportgeräten, KFZ-Fabrikbetriebe und werkzeugherstellende Kraftwerke.

Dieses Antragsmodell gilt für Dienstleistungsunternehmen, Selbstständige, freie Berufe (Rechtsanwälte, Steuerberater, Ärzte), Gesundheits- und Heilberufe, Handel, Bildungsrichtungen, Gastronomie, Hotellerie, Vereine, Verbände, Baugewerbe, Handwerk, Transport, Logistik sowie Land- und Forstwirtschaftsbetriebe.
3. Der Tätigkeitsbereich des Antragstellers liegt in den folgenden Bereichen: NEIN
 - Zahlungsbewältigung, -dienstleistung, Inkassodienstleistung
 - Glücksspiel, Pornografie, Datensammlung und -speicherung (Hauptgeschäftszweck)
 - Ratingagentur, Vermögensverwaltung, Finanzdienstleistung, Ökonomieberatung
 - Anleiher, Vermittler oder Broker von Versicherungen oder Finanzdienstleistungsprodukten
-> diese Tätigkeiten können Sie über unser Produkt [Markel Pro Cyber für Vermittler](#) abdecken
4. Der Antragsteller erwirtschaftet oder erbringt in den USA direkte Umsätze oder Leistungen. NEIN
5. Der Antragsteller bearbeitet, speichert oder übermittelt im Jahr mehr als 20.000 Kreditkartendaten. NEIN
6. Der Antragsteller 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 Vor Schaden). NEIN
7. 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
8. Der Antragsteller nutzt folgende IT-Sicherheitsvorkehrungen: JA
 - Anti-Virus-Schutz mit aktuellen Virensensorenbanken (Nur von ausgenommen sind die Betriebssysteme von Apple, Unix und Linux)

MarkelNow

www.markel.de/markelnow

Das neue exklusive Maklerportal für den modernen Makler.

- ✓ Direkt online beantragen
- ✓ Policen ohne Wartezeit
- ✓ 24/7 – rund um die Uhr
- ✓ Einfach und intuitiv
- ✓ Service für Ihre Kunden optimieren
- ✓ Kundenzufriedenheit steigern
- ✓ Sicherer, DSGVO-konformer Zugang

Wie Sie Ihre Zugangsdaten beantragen können, erfahren Sie unter:
www.markel.de/markelnow



07 | Über Markel

Markel

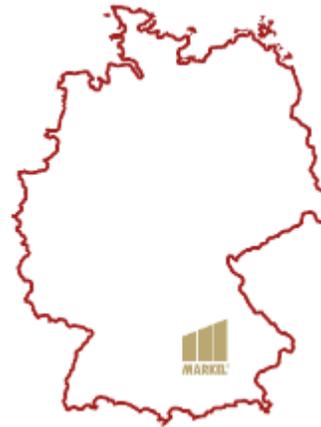
Zahlen, Daten & Fakten

Markel Insurance SE

Seit 10.2018 deutscher Versicherer

Spezialist VSH & D&O

Dynamisches Team aus 30 Mitarbeitern



Markel Corporation

Gegründet 1930 in Richmond von Sam Markel

15.600 Mitarbeiter in 21 Ländern

6,1 Mrd. USD Bruttoprämien 2017



| Einführung in die Cyber-Versicherung

| Markel Insurance SE



Das Maklerportal

www.markel.de/maklerportal

Immer auf dem neusten Stand

- ✓ Keine Zugangsbeschränkung
- ✓ Immer die aktuellsten Unterlagen

Sämtliche Unterlagen & Informationen

- ✓ Alle Unterlagen zur Vertriebsunterstützung
- ✓ Antragsmodelle und Fragebögen
- ✓ Alle Ansprechpartner auf einen Blick
- ✓ Erklärfilme



Markel Academy

www.academy.markel.de

Webinare & Videos

- ✓ Kostenlos
- ✓ Einfache Bedienung
- ✓ Live und auf Band

Erklärfilme

- ✓ Kurz und einfach
- ✓ Zu verschiedenen Themen

gut beraten

- ✓ Akkreditierter Bildungsdienstleister
- ✓ Ihre Aufmerksamkeit wird belohnt!

Produktschulung

- ✓ Für Anfänger
- ✓ Und Fortgeschrittene





Markel Insurance SE
**Ihr Spezialversicherer für
gewerbliche Haftpflicht**