Marvin Knorr → Legal Claims Handler

Vertrauensschäden und Cyber-Haftpflicht – Risiken im digitalen Zeitalter

Bedrohungen für die Unternehmenssicherheit und -kontinuität verstehen

MARKEL

Ihr heutiger Referent

Marvin Knorr

Legal Claims Handler

→ Legal Claims Handler für Cyber seit 2023

→ Ansprechpartner für Cyberschäden, IT-Schadenfälle u. a.

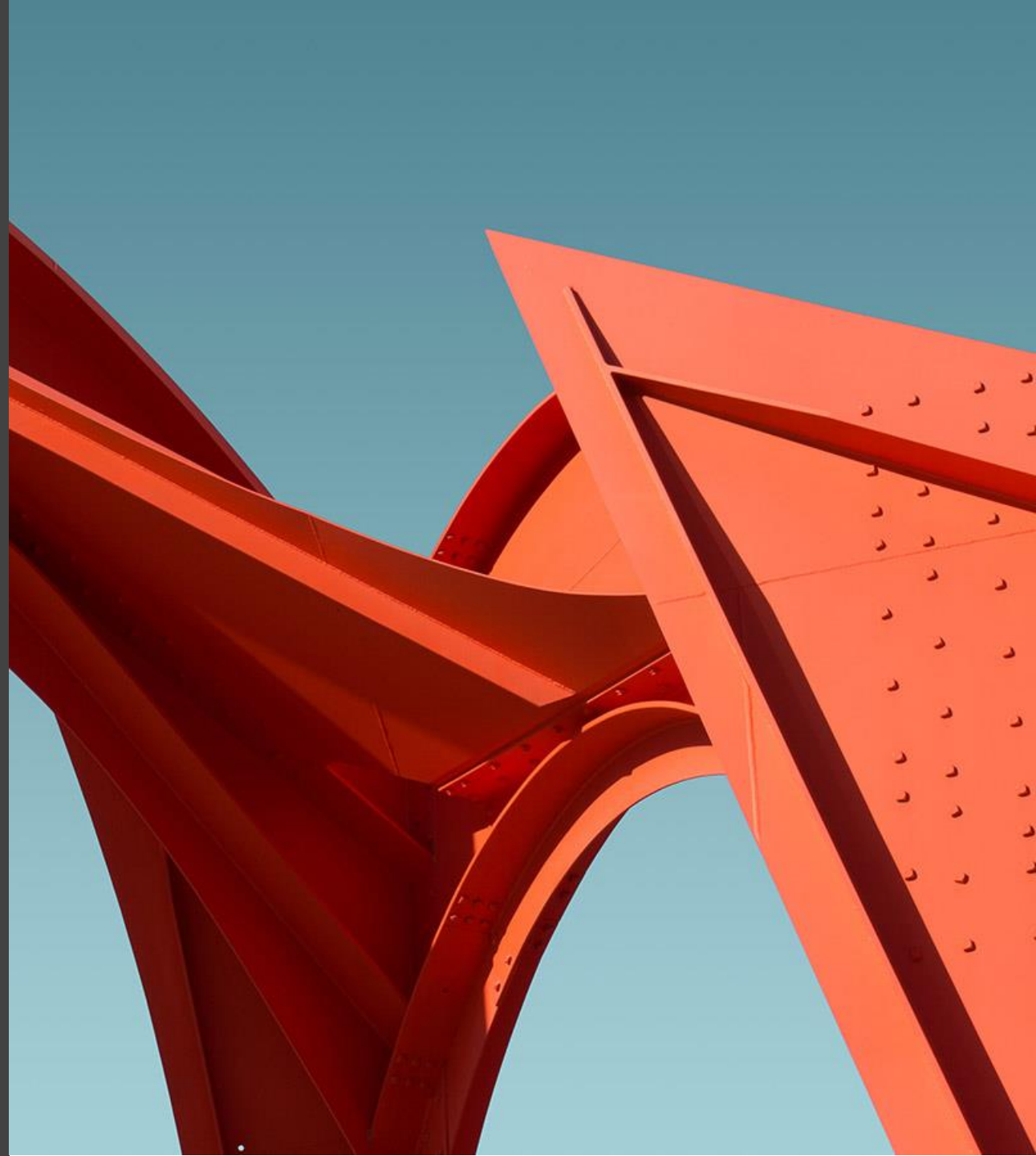
→ IT-Recht als Studienschwerpunkt

Agenda

Überblick über aktuelle Zahlen und Trends
Aktuelle Statistiken zeigen die stark zunehmende Bedeutung von Cyberkriminalität für Unternehmen jeder Größe.

Relevanz von Vertrauensschäden
Im Mittelpunkt stehen typische Betrugsszenarien wie Social Engineering, Zahlungsumleitungen und Business E-Mail Compromise (BEC).

Cyber-Haftpflichtversicherung
Darstellung der Funktionsweise und des Leistungsumfangs von Cyber-Haftpflichtversicherungen. Welche Risiken sind abgedeckt sind, wo liegen Grenzen liegen und inwiefern gibt es Unterschiede zur klassischen Vermögensschadenhaftpflicht.



Überblick über aktuelle Zahlen und Trends

01

Überblick über aktuelle Zahlen und Trends

87 %

Von Angriffen betroffen oder vermuten Opfer eines Cyberangriffs gewesen zu sein

289,2 Mrd. €

Gesamtschaden 2025 aufgrund Diebstahl, Sabotage oder Industriespionage

49 %

Von Social Engineering betroffen

China und Russland

Größte Bedrohungsquellen

Deutschland dritthäufigstes Ziel

von Cyerangriffen weltweit

Überblick über aktuelle Zahlen und Trends

Arten von Cyberangriffen

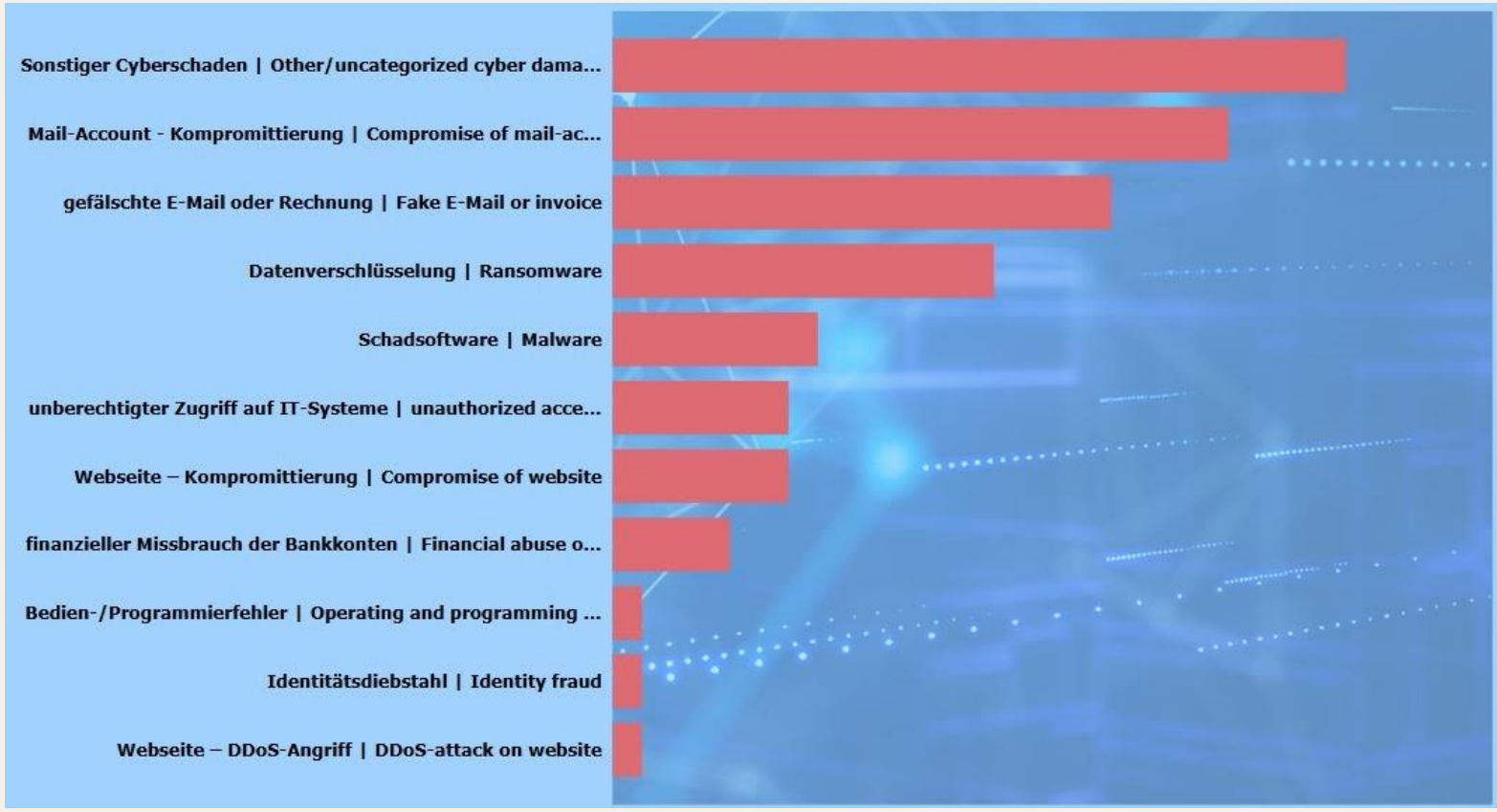
Nicht nur klassische Angriffe wie Ransomware dominieren, sondern vor allem E-Mail-basierte Betrugsformen. Kompromittierte Mail-Accounts und gefälschte Rechnungen zählen zu den häufigsten Ursachen für Schäden.

Zunehmende Bedrohungslage

Die Zahlen verdeutlichen eine klare Entwicklung: Cyberangriffe werden vielfältiger und gezielter. Besonders Social-Engineering-Methoden nehmen zu, da sie menschliche Schwachstellen ausnutzen und oft einfacher umzusetzen sind als rein technische Angriffe.

Finanzielle und operative Auswirkungen

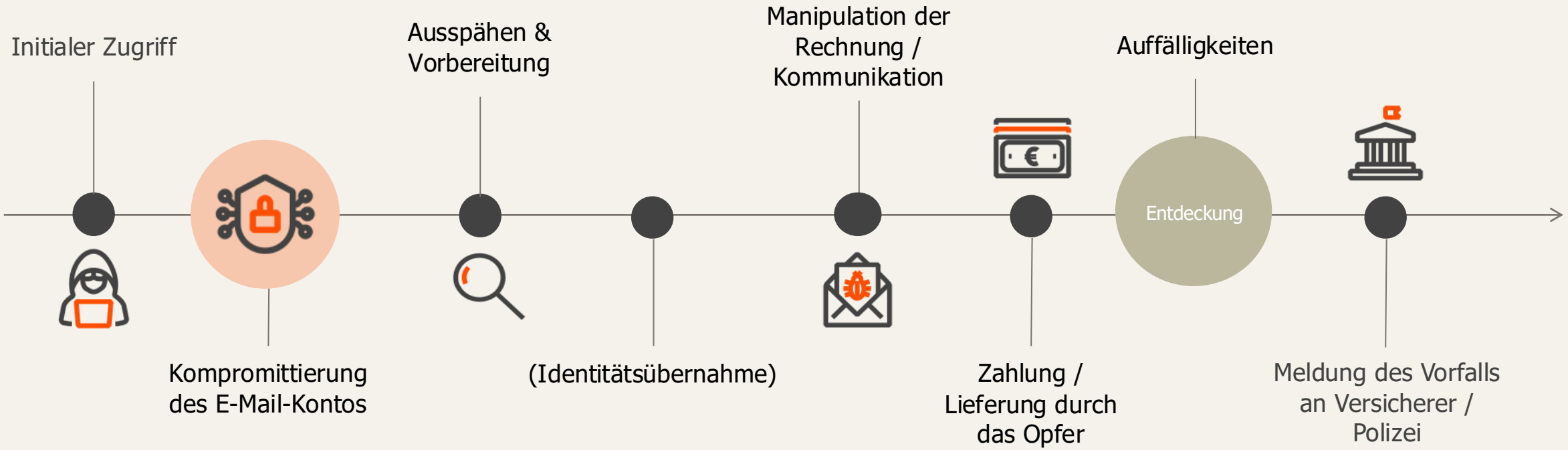
Die größten Schäden entstehen häufig nicht durch technische Ausfälle, sondern durch betrügerische Transaktionen und Datenkompromittierung.



Relevanz von Vertrauensschäden

02

Mail-Account-Kompromittierung (Business-Email-Compromise) und Zahlungsumleitung



Auch ohne initialen Zugriff auf Zugangsdaten möglich –> typosquatting (z. B. sachbearbeiter@markel.con statt sachbearbeiter@markel.com)

Manipulierte Rechnung

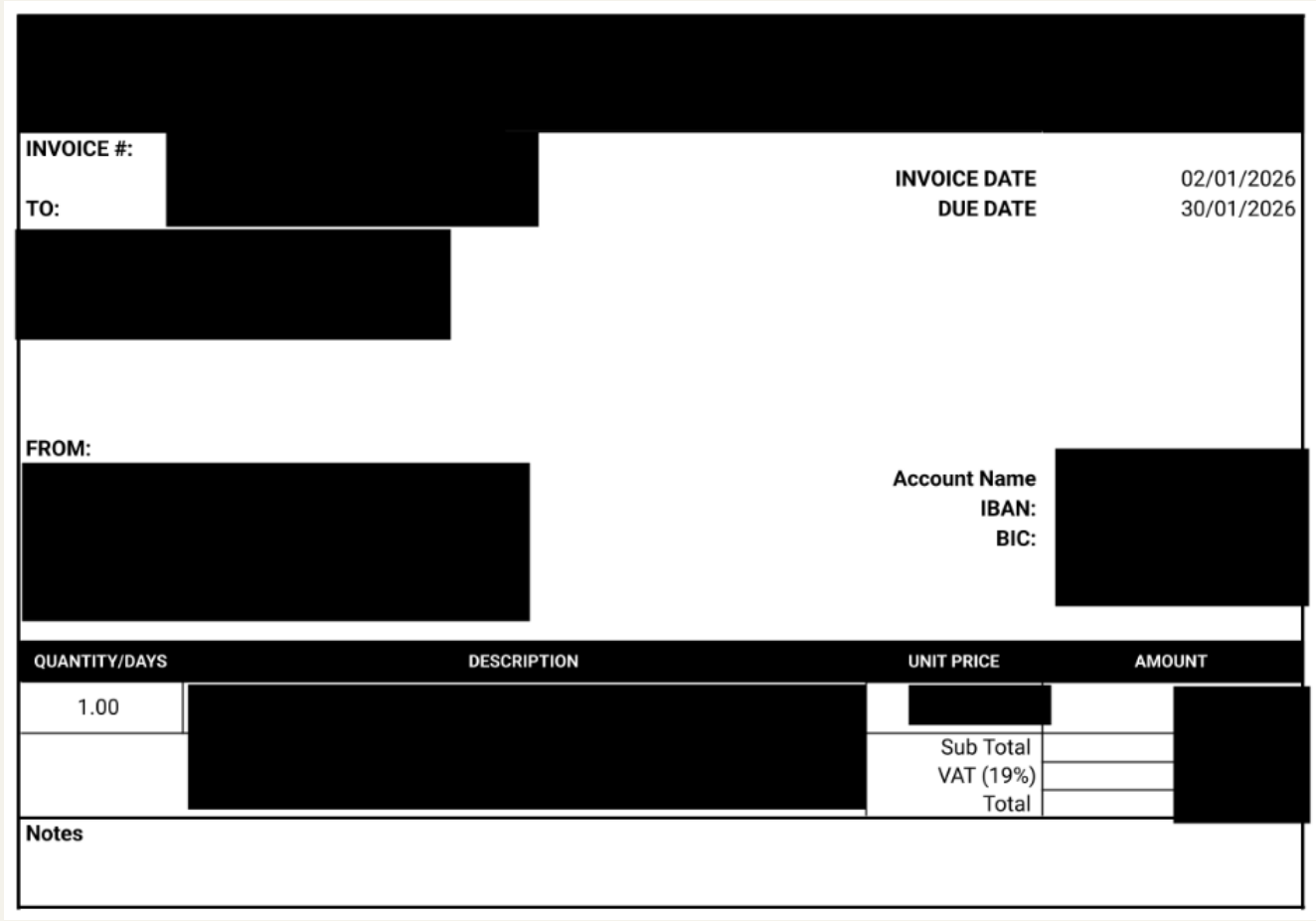
→ In der Regel wird lediglich IBAN verändert

→ Rechnungsersteller und –empfänger, Rechnungsdatum, Rechnungsnr. etc. bleiben gleich

→ Manchmal Vorwand: Bankverbindung hat sich geändert

→ Sachbearbeiter lassen sich geänderte Bankverbindung oft durch den Betrüger bestätigen oder gar nicht

→ Andere Formen: Neues Konto für Lohnzahlung, Insolvenzverwalter, Rechnung für nicht erbrachte Leistungen


[redacted]
INVOICE #: [redacted]
TO: [redacted]
INVOICE DATE 02/01/2026
DUE DATE 30/01/2026
FROM: [redacted]
Account Name [redacted]
IBAN:
BIC:
QUANTITY/DAYS | DESCRIPTION | UNIT PRICE | AMOUNT
1.00 | [redacted] | [redacted] | [redacted]
Sub Total
VAT (19%)
Total
Notes

Fehlüberweisung: Wer haftet?

VN: „Ich habe meine Rechnung bezahlt.“

- → Ich habe die Leistung/Ware bezahlt, warum nochmal zahlen?
- → Ich bin Opfer des Betruges

Kunde: „Ich habe das Geld nicht erhalten.“

- → Ich bekomme kein Geld für meine Leistung/Ware
- → Ich habe nicht falsch überwiesen
- → Ich habe einen fälligen Anspruch

Rechtsprechung: „Es kommt darauf an.“

- → Erfüllung gem. § 362 BGB?
- → Schadensersatz?
- → Aufrechnung?

Finanzieller Missbrauch von Bankkonten

1. Initialer Kontakt
•Anruf / SMS / E-Mail („Ihre Bank", „Sicherheitsabteilung")
•Hinweis auf auffällige / verdächtige Transaktionen

2. Aufbau von Vertrauen
•Auftreten als Bankmitarbeiter / IT-Support
•Verwendung echter Daten (Name, IBAN-Fragmente, letzte Transaktionen)
•Erzeugung von Dringlichkeit und Druck

3. Steuerung des Opfers
•Opfer wird angeleitet, sich ins Online-Banking einzuloggen
•„Wir prüfen gemeinsam die Buchungen"

4.Täuschung über Vorgänge
•Tatsächlich werden neue Überweisungen durch den Täter initiiert
•Diese werden als „Storno", „Sicherungsbuchung" oder „Testtransaktion" dargestellt

5. Freigabe durch das Opfer
•Opfer bestätigt TAN / Push-Freigabe
•In dem Glauben, Betrug zu verhindern, autorisiert es tatsächlich die Zahlung

6. Abfluss der Gelder
•Überweisung geht auf Täterkonto / „Money Mule"
•Sofortige Weiterleitung / Abhebung

7.Verschleierung
•Kontakt bricht ab („Problem behoben", „wir melden uns")
•Rückverfolgung erschwert

Cyber-Haftpflichtversicherung

03

VSH-Versicherung vs. Cyber-Versicherung

VSH	Cyber	Wesentliche Unterschiede
➢ Versicherungsschutz für reine Vermögensschäden aufgrund **beruflicher Pflichtverletzungen** ➢ Anknüpfungspunkt: fehlerhafte Beratung, Prüfung oder sonstige Dienstleistung ➢ Schutz umfasst regelmäßig: Haftpflichtansprüche Dritter (Mandanten), Abwehr unbegründeter Ansprüche (passiver Rechtsschutz)	➢ Versicherungsschutz für Schäden infolge von **IT-Sicherheitsvorfällen** ➢ Anknüpfungspunkt: Verletzung der Informationssicherheit / Datenverfügbarkeit ➢ Schutz umfasst regelmäßig: Eigenschäden (z. B. Betriebsunterbrechung, Datenwiederherstellung, Forensik, Krisenmanagement)	➢ Schadensart: Fremdschaden vs. Drittschaden ➢ Risikosphäre: inhaltliche/fachliche Tätigkeit vs. technische Infrastruktur / IT-Systeme

Reine Cyber-Deckung greift regelmäßig nicht bei Schäden gegenüber Dritten –> **erhebliches Absicherungsdefizit**

Lösung: Cyber-Haftpflicht (Baustein)

Versichertes Risiko gemäß Markel Pro Cyber v2

„Der Versicherer gewährt den Versicherten Versicherungsschutz, wenn sie von einem Dritten aufgrund gesetzlicher – auch verschuldensunabhängiger – Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden (inklusive eines etwaigen immateriellen Schadens) in Anspruch genommen werden, sofern der Schadensersatzanspruch auf einem der nachfolgenden Verstöße beruht“

- Verstöße gegen Cyber-Sicherheit **->** Weitergabe von Schadsoftware, insbesondere Viren, Schadcodes und Trojaner an Dritte oder durch die Nutzung der IT-Systeme der Versicherten für Angriffe auf Computersysteme Dritter
- Verstoß gegen Datenschutz **->** Verletzung anwendbarer datenschutzrechtlicher Bestimmungen (beispielsweise DSGVO/BDSG)
- Verstoß gegen Benachrichtigungspflichten **->** DSGVO
- Verstoß gegen Geheimhaltungspflichten **->** Verschwiegenheitspflicht von z. B. Anwälten
- Vertragsstrafen bei Verletzung von Geheimhaltungspflichten und Datenvertraulichkeitserklärungen
- Vertragsstrafen wegen verzögerter Leistungserbringung
- Verstöße gegen Namens- und Persönlichkeitsrechte
- Verstöße durch Werbung und Marketing **->** Verletzung gewerblicher Schutzrechte

Beispielfall (Cyberangriff mit Mehrfachfolgen)

Cyber-Kriminelle

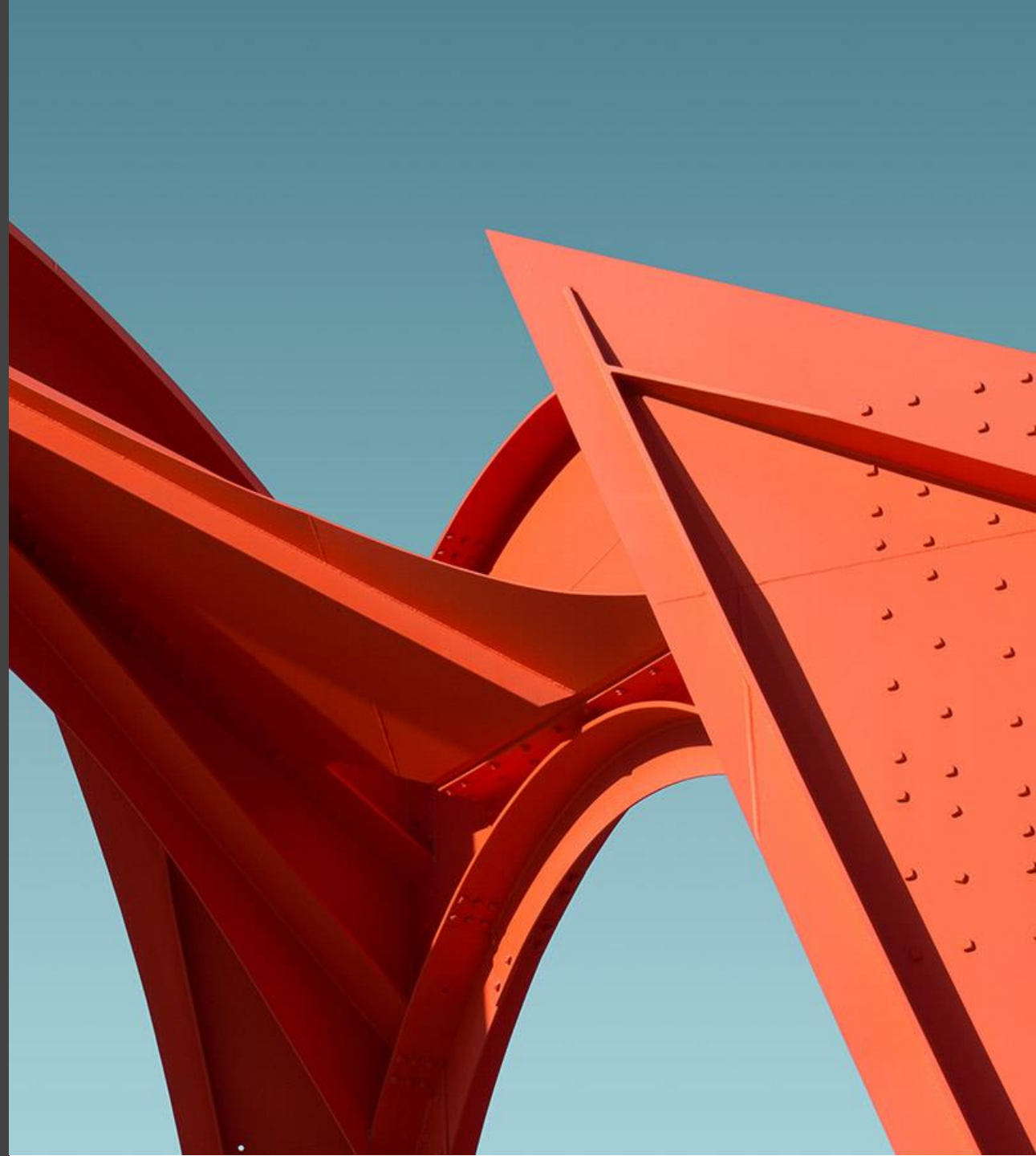
Mittelständische Kanzlei (12 Mitarbeiter, ca. 1,8 Mio. € Jahresumsatz)

Mandanten

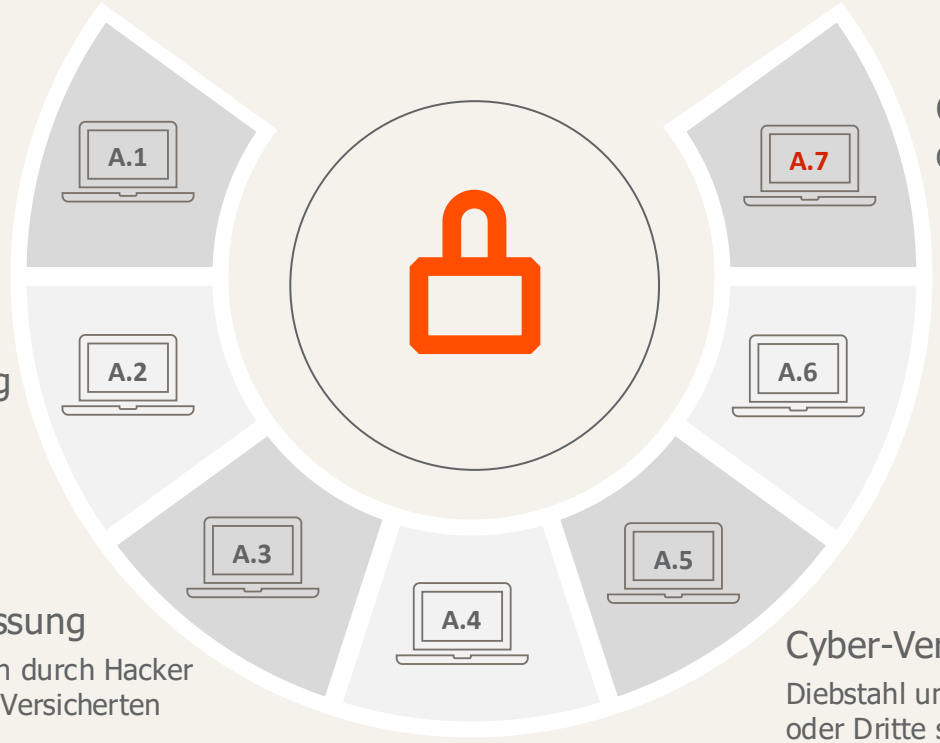
Über ein kompromittiertes E-Mail-Konto verschaffen sich Angreifer Zugriff auf das Kanzleisystem. Es werden rund 2.500 Mandantendatensätze (inkl. sensibler Informationen) exfiltriert und teilweise im Darknet veröffentlicht. Es werden Mails an Mandanten versendet.

- Verstoß gegen Cyber-Sicherheit: **Schadensersatz 100.000 €**
- Verstoß gegen Benachrichtigungspflichten: **Bußgeld 15.000 €**
- Verstoß gegen Datenschutz: **immaterieller Schadensersatz (z. B. 2.000–5.000 € pro Person)**
- Vertragsstrafen (NDA): **z. B. 25.000 €**
- Verzögerte Leistungserbringung: **Vertragsstrafe von 10.000 €**

Markel
Pro Cyber v2



Modularer Versicherungsschutz (Markel Pro Cyber v2)



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

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

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

Cyber-Prävention Premium
Online-Präventionsplattform von Perseus

MARKEL