Sicherheit für Unternehmen - Risiko für die Menschen?

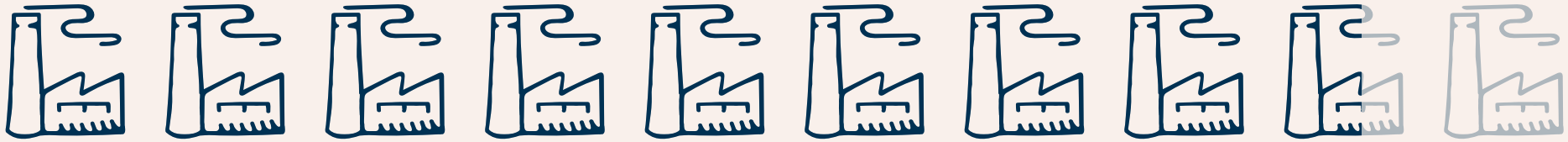
Haftungsfälle und sichere Häfen für Geschäftsleiter, IT-Leiter und CISO im Umgang mit regulierter IT-Sicherheit

RA Dr. Julian Zaudig, **10. IT-Sicherheitsrechtstag am 24.09.2025 in Berlin**

NIS2UmsuCG - so what?

Gefangen im Präventionsparadoxon.

87%



der befragten Unternehmen gaben an, in den letzten 12 Monaten von Industriespionage oder Sabotage betroffen gewesen zu sein.

Bitkom e. V., Wirtschaftsschutz 2025, S. 3.

Die Schadenssummen sind immens und steigen.

Volkswirtschaftlicher Gesamtschaden:

289,2 Mrd. € **8,5% ggü. Vorjahr**

Bitkom e. V.; Wirtschaftsschutz 2025, S. 4.

Der Anteil der durch Cyberangriffe verursachten Schäden steigt überproportional.

Volkswirtschaftlicher Gesamtschaden:

202,44 Mrd. € **13,3% ggü. Vorjahr**

Bitkom e. V., Wirtschaftsschutz 2025, S. 13.

Cyberangriffe werden als existenzielle Bedrohung wahrgenommen.

"Cyberangriffe gefährden unsere geschäftliche Existenz."

59% 9% ggü. Vorjahr

Bitkom e. V., Wirtschaftsschutz 2025, S. 12.

Weniger Unternehmen sind darauf jedoch vorbereitet.

"Unser Unternehmen ist auf Cyberangriffe sehr gut vorbereitet."

50% 6% ggü. Vorjahr

Bitkom e. V., Wirtschaftsschutz 2025, S. 12.

Fazit aus diesen Zahlen:

- **Es gibt ein Problem der Risikobehandlung.**

  50% der befragten Unternehmen sind nicht sehr gut auf einen Angriff vorbereitet, obwohl 87% der Unternehmen Opfer eines Angriffs wurden.

- **Unternehmen nehmen teilweise existentielle Risiken in Kauf.**

  50% der befragten Unternehmen halten sich für sehr gut auf einen Angriff vorbereitet, 59% geben diesen aber als existenzielle Bedrohung an.

- **Die Schäden sind wesentlich und steigen.**

Dennoch begegnen uns Vorbehalte:

„Das BSI wird sich doch kooperativ verhalten."

„Bei der DS-GVO hat es auch keine Bußgeldwelle gegeben."

„Wir achten bei unseren Zulieferern und Projekten auf Zertifizierungen."

„Ich habe einen CISO/Dienstleister, er kümmert sich."

Dies basiert aber auf einem falschen Fokus: Das Zivilrecht wird IT-Sicherheit durchsetzen.

- **Auch bei der DS-GVO ist die zivilrechtliche Durchsetzung ein zentraler Wirkmechanismus geworden.**
- **Die Regulierungstatbestände schaffen durchweg Ansprüche.**

  EG (143) NIS-2 RL: Rechtsbehelf gegen unsichere Datenverarbeitung. Bei Kardinalspflichten scheitert Freizeichnung an 307 Abs. 1 Nr. 1 BGB. DORA zwingt zur vertraglichen Konkretisierung von Pflichten.

- **Die Durchsetzung solcher Ansprüche wird stärker wirken als die bloße Aufsicht.**

Ein praktischer Fall

- **Die A-GmbH erneuert eine Produktionsanlage. Die G-GmbH ist Generalübernehmer. Ressortzuständiger Geschäftsführer ist IT-Leiter I.**
- **Die G-GmbH soll auch die IT-Sicherheit der Anlage "besorgen".**

  Um die Sicherheit zu gewährleisten, muss die G-GmbH sich nach ISO 27001 zertifizieren lassen.
- **Sicherheitsberater S soll ein System zur Angriffserkennung implementieren. Er setzt auf Profilbildung von Nutzern. Es kann nicht eingesetzt werden.**

  Der Betriebsrat wurde nicht befasst und außerdem ist die Rechtmäßigkeit der Datenverarbeitung ungeklärt. S hatte eine kurze Erläuterung verfasst, weswegen die Datenverarbeitung seiner Ansicht nach gemäß Art. 6 Abs. 1 lit. f) DS-GVO zulässig war. Auf Art. 22 DS-GVO ging er nicht ein. Er erteilte auch keinen Hinweis zur Mitbestimmung nach § 87 Nr. 6 BetrVG. Der Datenschutzbeauftragte wurde nicht eingebunden. Sonstige Ressorts ebenfalls nicht.
- **Die A-GmbH wird Opfer eines Ransomware-Angriffs. Ein BCM existiert nicht, I hat keine eigenen Maßnahmen ergriffen, sondern sich auf die G-GmbH und ihre Zertifizierung verlassen.**
- **Der Betriebsausfall ist für die Gesellschaft existenzgefährdend.**
- **I steht dem Krisenstab mit seinem Kollegen P vor. S rät zur Zahlung der Ransom. So geschieht es. Eine Entschlüsselung findet aber nicht statt.**

Praktisch relevante Vorwürfe an Geschäftsleiter:

Unzureichende Risikoüberwachung und -reaktion

Handeln oder Entscheidung ohne angemessene Informationsgrundlage

Verletzung der Kompetenzordnung der Gesellschaft

§ 1 Abs. 1 StaRUG:

“Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht. Berühren die zu ergreifenden Maßnahmen die Zuständigkeiten anderer Organe, wirken die Geschäftsleiter unverzüglich auf deren Befassung hin.„

Die maßgeblichen Entscheidungen können nicht delegiert werden.

- **Ein Geschäftsführer darf Geschäftsführungsangelegenheiten an qualifizierte Personen delegieren.**

  Die Aufgabenerfüllung ist dann allerdings zu überwachen, es verbleibt stets eine Letztverantwortung.

- **Leitungsaufgaben sind hiervon allerdings ausgenommen.**

  Diese müssen stets im Kollegium entschieden und der Gesellschafterversammlung vorgelegt werden (*Übersicht bei MüKoGmbHG/Fleischer § 43 GmbHG Rz. 144*).

- **Dass grundlegende Entscheidungen in der EDV Leitungsentscheidungen sind, ist nichts Neues.**

  Dies wurde für das Outsourcing von EDV bereits angenommen (*LG Darmstadt, Urt, v. 06.05.1986 – 14 O 328/85)*. Generell sind aber Entscheidungen vorzulegen, die außergewöhnlich oder risikobehaftet sind. Dies kann bei IT-Sicherheitsentscheidungen kaum verneint werden.

Dies hat Auswirkungen auf die Vertragsgestaltung:

- **Leitungsaufgaben dürfen zwar nicht delegiert werden.**

  Die maßgeblichen Entscheidungen müssen also stets von den Geschäftsleitern getroffen werden - im Kollegium!

- **Jedoch darf ihre Vorbereitung und Ausführung delegiert werden, auch an Dritte.**

  Hierzu ist gerade im Bereich der IT anerkannt, dass die Einbindung von Experten unerlässlich ist.

- **Die Entscheidungszuständigkeit muss allerdings rechtlich abgesichert werden.**

  Die Delegation an Dritte darf den Einfluss der Geschäftsleitung nicht schmälern. Deshalb ist **der erforderliche Informationsfluss und die Entscheidungszuständigkeit der Geschäftsleitung vertraglich abzusichern**.

§ 1 Abs. 1 StaRUG:

“Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht. Berühren die zu ergreifenden Maßnahmen die Zuständigkeiten anderer Organe, wirken die Geschäftsleiter unverzüglich auf deren Befassung hin.”

Auch § 38 Abs. 1 BSIG-E ist insofern nichts Neues:

“Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.”

Entscheidungen müssen auf angemessener Informationsgrundlage erfolgen.

- **Unternehmerische Entscheidungen unterfallen der Business-Judgment-Rule.**
- **Diese erfordert eine Entscheidung auf angemessener Informationsgrundlage.**
- **Werden Erkenntnisquellen nicht in Anspruch genommen, muss dies gerechtfertigt werden.**

  Dies kann zum Beispiel aufgrund von Zeitdruck oder unter Abwägung von Kosten und Nutzen weiterer Informationsgewinnung erfolgen. Je grundlegender jedoch die Entscheidung, desto umfassender muss die Informationsgrundlage sein.

OLG Köln, Urt. v. 01.10.2019 – 18 U 34/18, zitiert nach NZG 2020, 110 – 116, 113 Tz. 78f.

Insbesondere Zertifizierungen von Dienstleistern enthaften nicht mehr.

- **Dies ergibt sich bereits methodisch.**

  Die Tatsache, dass Sicherheitsmaßnahmen der Risikoneigung eines Dienstleisters angemessen sind, lässt nicht den Schluss zu, dass sie auch für den eigenen Betrieb ausreichen.

- **Im regulierten Bereich lehnt die Rechtsprechung dies ausdrücklich ab.**

  Nach der Rechtsprechung des EuGH darf die Beurteilung, ob Sicherheitsmaßnahmen angemessen sind, nicht von Sachverständigen, sondern nur von Richtern vorgenommen werden darf (EuGH, Urt. v. 14.12.2023 – Az. C 340/21 Rz. 64).

- **Dadurch ist die Aussagekraft von Zertifizierungen und Audits begrenzt.**

  Lediglich die tatsächlichen Feststellungen von Zertifizierungen und Auditberichten können eigenen Entscheidungen zugrunde gelegt werden. Wertungen hingegen nicht.

- **Deshalb ist eine dokumentierte Auseinandersetzung mit Sicherheitsmaßnahmen von Dienstleistern Pflicht.**

Wäre den Geschäftsleitern ein Vorwurf zu machen?

- **Unzulässiges Outsourcing der Entscheidungen zur IT-Sicherheit.**
  Denn die wesentlichen Entscheidungen mussten die Geschäftsführer sich vorbehalten.

- **I durfte nicht allein entscheiden.**
  Die wesentlichen Entscheidungen hätten im Kollegium besprochen und den Gesellschaftern vorgelegt werden müssen.

- **I hätte sich nicht auf den Rechtsrat durch S verlassen dürfen.**
  Er hätte grundsätzlich sämtliche Erkenntnisquellen ausschöpfen müssen, also den Datenschutzbeauftragten, Personalverantwortliche und einen Rechtsanwalt befragen müssen.

- **Die Zertifizierung des Dienstleisters kann eine eigene Bewertung nicht ersetzen.**
  Wird eine Zertifizierung zur Begründung herangezogen, führt dies in aller Regel automatisch zur Pflichtwidrigkeit.

- **Auf ein Business Continuity Management hätte nicht verzichtet werden dürfen.**
  Eine etwaige Verletzung vertraglicher Pflichten der G-GmbH ändert daran nichts. Denn die Geschäftsführer der A-GmbH waren aufgrund ihrer eigenen Legalitätspflicht gehalten ein solches einzurichten (§ 30 Abs. 2 S. 2 Nr. 2, 3 BSIG-E).

- **Die Entscheidung über die Zahlung der Ransom hätte den Gesellschaftern vorgelegt werden müssen.**
  Denn die Maßnahme ist risikobehaftet und außergewöhnlich. Sie wäre außerdem rechtlich zu begutachten gewesen (§ 129b Abs. 1 S. 2 Var. 1 StGB).

Die Haftung von IT-Sicherheitsbeauftragten

- **Arbeitnehmer sind nach dem innerbetrieblichen Schadensausgleich privilegiert.**

  Der Arbeitgeber trägt Schäden aufgrund einfacher Fahrlässigkeit, bei mittlerer Fahrlässigkeit wird der Schaden aufgeteilt, ab grober Fahrlässigkeit haften auch Beschäftigte in der Regel für den ganzen Schaden.

- **Externe IT-Sicherheitsbeauftragte unterliegen der vertraglichen Haftung.**

  Diese ist im Einzelfall zu bestimmen. Der innerbetriebliche Schadensausgleich gilt nicht. Ein Betriebsausfallschaden ist ohne Nachfristsetzung ersatzfähig (*BGH, Urt. v. 19.06.2009 – V ZR 93/08, zitiert nach NJW 2009, 2674 – 2677*).

- **Das Haftungsrisiko ist nicht zu unterschätzen!**

  Durchlaufen Arbeitnehmer Schulungen oder werden Meldewege für Zweifelsfälle ignoriert, spricht dies für ein erhöhtes Maß an Fahrlässigkeit.

Das RDG ist eine vielfach übersehene Haftungsfalle für Dienstleister und sonstige Beteiligte.

- **Nach § 3 RDG ist die Erbringung von Rechtsdienstleistungen Rechtsanwälten vorbehalten.**

  Aufgrund der rechtlichen Prägung von IT-Sicherheitspflichten geht die IT-Sicherheitsberatung nahezu stets auch mit einer Rechtsdienstleistung einher.

- **Sonstige Personen müssten sich auf Ausnahmen von dieser Regel stützen.**

  Bei Datenschutzbeauftragten wird ihre Befugnis aus der DS-GVO abgeleitet. Konzernintern gilt die Ausnahme nach § 2 Abs. 3 Nr. 6 RDG.

- **IT-Sicherheitsbeauftragte müssten argumentieren, dass die Rechtsdienstleistung als Nebenleistung zum Berufsbild gehört.**

  Dies ist zumindest zweifelhaft. Außerdem dürfte angesichts der Komplexität der rechtlichen Fragen in diesem Bereich keine Nebenleistung vorliegen. Die Komplexität oder Tragweite einer rechtlichen Einschätzung kann ihren Charakter als Nebenleistung ausschließen (*BT-Drs. 16/3655, S. 54*).

Beachten Dienstleister diese Grenzen nicht, haften sie wie Rechtsanwälte. Außerdem tragen die Beteiligten das Risiko des Rechtsirrtums.

- **Erbringen Nicht-Anwälte Rechtsdienstleistungen, gereicht ihnen dies nicht zum Vorteil. Sie haften wie Rechtsanwälte.**

  BGH, Urt. v. 27.11.2019 – VIII ZR 285/18, zitiert nach NJW 2020, 208 – 235, 219 Tz. 94.

- **Rechtliche Fragestellungen können falsch sein, auch wenn sie vertretbar sind.**

  Denn von der nach den Regeln der juristischen Methodik erstellten rechtlichen Stellungnahme "sind unrichtige deskriptive Aussagen über das Recht zu unterscheiden." Auch vertretbare Aussagen können deshalb falsch sein, wenn gewichtige Gegenargumente oder -positionen nicht berücksichtigt und offengelegt werden (*BGH, Beschl. v. 07.07.2025 – 1StR 484/24, zitiert nach BeckRS 2025, 23556 Tz. 5*).

- **Ein Rechtsanwalt dürfte sich jedoch auch gegen die Ansicht der Rechtsprechung stellen und Beteiligte vom Vorwurf des Rechtsirrtums befreien.**

  In dieser entlastenden Wirkung von anwaltlichem Rechtsrat liegt der wesentliche Vorteil von anwaltlichem Rat im Bereich der IT-Sicherheit. Nicht anwaltlichem Rat kommt diese Wirkung hingegen nicht zu.

Wie wäre der Fall zu bewerten?

- **S wäre an den strengen Maßstäben anwaltlicher Rechtsberatung zu messen gewesen.**

- **Die Einschätzung war falsch.**

  Zwar dürfen auch abweichende Meinungen vertreten werden. Dies setzt aber eine Offenlegung von Gegenansichten und eine Auseinandersetzung mit der Quellenlage voraus. Typische Stellungnahmen von Beratern erreichen diese Anforderungen nicht.

- **Hierin liegt eine Pflichtverletzung, ein kausaler Betriebsausfallschaden ist ersatzfähig.**

  Bei Zweifeln hinsichtlich der Kausalität von Pflichtverletzungen und Schaden greift im Mehrpersonenverhältnis § 830 Abs. 1 S. 2 BGB (*"allgemeiner Rechtsgedanke" - BGH, Urt. v. 16.01.2001 – X ZR 69/99, zitiert nach NJW 2001, 2538 – 2541, 2539*).

Exkurs: IT-Sicherheit und Untreue

- **Der Wortlaut des Untreuetatbestands ist sehr weit.**

  Ausreichend ist eine Vermögensbetreuungspflicht des Täters, dessen pflichtwidriges Verhalten und die Verursachung eines Schadens. Die Untreue ist ein Vorsatzdelikt.

- **Sie ist jedoch verfassungskonform auszulegen.**

  Sie bedroht nicht jede Pflichtverletzung mit Strafe, sondern nur "gravierende" Pflichtverletzungen (*BVerfG, Beschl. v. 23.06.20120 – 2 BvR 2559/08, zitiert nach NJW 2010, 3209 – 3221, 3215 Tz. 112*).

- **Sie bedroht den Verstoß gegen DORA und das BSIG-E nicht mit Strafe.**

  Denn untreuerelevant sind nur Verstöße gegen Normen, welche das Vermögen des Prinzipals schützen (*BGH, Beschl. v. 13.04.2011 – 1 StR 94/10, zitiert nach NJW 2011, 1747 – 1752, 1749 Tz. 25*). Die Regulierungstatbestände zur betrieblichen IT-Sicherheit nehmen die Unternehmen jedoch im öffentlichen Interesse in die Pflicht.

- **Untreue ist jedoch auch in diesem Bereich nicht ausgeschlossen.**

  Als untreueverdächtig gilt zum Beispiel die Entscheidung ohne angemessene Informationsgrundlage (*BGH, Urt. v. 12.10.2016 – 5 StR 134/15, zitiert nach NJW 2017, 578 – 582, 579f. Tz. 31*). Auch in diesem Fall muss die Untreue positiv festgestellt werden, der Verdacht erlaubte jedoch wenigstens die Einleitung eines Ermittlungsverfahrens.

IT-Sicherheitsbeauftragte und Strafrecht

- **IT-Sicherheitsbeauftragte kann eine straf- und bußrechtliche Verantwortung treffen.**

  Erforderlich ist jeweils, dass sie ausdrücklich mit der eigenständigen Wahrnehmung von Aufgaben beauftragt wurden. Dies muss über die bloße Beratung hinausgehen.

  Zum Beispiel kann dies im Rahmen einer Ernennungsurkunde geschehen.

- **Auch ein Unterlassen kann strafbar sein.**

  Der Bundesgerichtshof hat bereits zu Compliancebeauftragten entschieden, dass diese strafrechtlich verantwortlich sein können, wenn sie Straftaten aus dem Unternehmen heraus nicht verhindern (*BGH, Urteil vom 17.07. 2009 – 5 StR 394/08, zitiert nach NJW 2009, 3173 - 3177, 3175*).

  Überträgt man diese Begründung auf IT-Sicherheitsbeauftragte, wären diese abhängig von ihrem Auftrag verpflichtet, Straftaten aus den betreuten Systemen und gegen die dort gesicherten Daten zu verhindern.

- **Gremienentscheidungen enthaften nicht!**

  Die Rechtsprechung erkennt den Einwand, die eigene Stimme sei bei Abstimmungen nicht ausschlaggebend gewesen, grundsätzlich nicht an. Bedenken sind aktiv vorzutragen und Beauftragte müssen gegen rechtswidrige Maßnahmen stimmen
  (*BGH, Urteil vom 06.07.1990 – 2 StR 549/89, zitiert nach NJW 1190, 2560 - 2569, 2566*).

Anwendungsfälle

Rechtswidrige Penetrationstests und Verstöße gegen die Informationssicherheit.

Bußgelder nach dem BSIG-E.

Fazit: Wir sind mit verhaltenen Risiken konfrontiert.

Es besteht jedoch ein hoher Anreiz, Haftung geltend zu machen um Schadensersatz zu erhalten. Dies bewirkt mittelbar eine Durchsetzung der Pflichten zu angemessenen IT-Sicherheitsmaßnahmen.

Best Practices folgen deshalb nicht aus regulatorischen Überlegungen, sondern aus dem allgemeinen Zivilrecht:

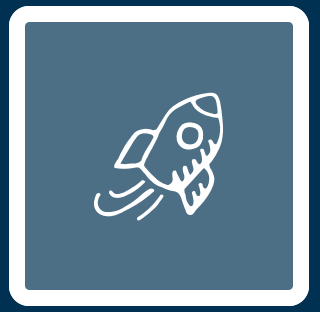
- ✓ **Sind Entscheidungszuständigkeiten klar benannt und auf Rechtmäßigkeit geprüft?**
  Geschäftsleiter tragen das Irrtumsrisiko für eine Fehleinschätzung.
- ✓ **Sind Organe der Gesellschaft dokumentiert und an den erforderlichen Stellen eingebunden?**
  Regelmäßig sind Vollmachten ratsam, um Gesellschafterversammlungen zu ermöglichen.
- ✓ **Sind rechtliche Fragestellungen klar identifiziert und werden durch einen Rechtsanwalt beantwortet?**
  Auch die Einbindung eines Syndikusrechtsanwalts ist ausreichend.
- ✓ **Sind Risiken angemessen identifiziert?**
  Verlassen Sie sich NICHT auf Zertifikate von Dienstleistern und Zulieferern sondern prüfen Maßnahmen selbst auf Angemessenheit?
- ✓ **Ist das Reporting von IT-Sicherheitsrisiken und -maßnahmen ausreichend und dokumentiert?**
  Ansonsten steht infrage, ob auf angemessener Informationsgrundlage entschieden wurde.

Was ausdrücklich nicht erforderlich ist:

"IT-Sicherheit"

Aus einem Sicherheitsvorfall kann nicht auf unzureichende Sicherheitsmaßnahmen geschlossen werden (*EuGH, Urt. v. 25.01.2024, Az. C 687/21 Rz. 40*).

Erforderlich sind sorgfältige Prozesse, welche auf Wirksamkeit überprüft werden (EuGH, Urt. v. 14.12.2023 – Az. C 340/21 Rz. 43, 46).



"Stand der Technik"

Unternehmen sind nicht verpflichtet, stets den Stand der Technik zu erreichen. Erforderlich ist eine ganzheitliche Risikobetrachtung.

Der Stand der Technik darf unterschritten werden, wenn das Risiko akzeptabel ist oder organisatorisch mitigiert wird.

"Zero Trust"

Dieser Begriff ist selbst in der Sicherheitsbranche nicht einheitlich verwendet.

Die Rechtsprechung fordert stichprobenartige Kontrollen - erteilt damit aber auch bloßen Audits eine Absage!

Eine saubere Arbeit im Bereich der IT-Sicherheit hilft allen Beteiligten.

Sie profitieren.

Jede Person, welche auf korrekte und rechtmäßige Prozesse drängt, schützt sich selbst vor rechtlichen Vorwürfen.

Ihr Unternehmen profitiert.

Auch das eigene Unternehmen profitiert jedoch von einem weiteren Haftungsträger: Der D&O-Versicherung.

Die D&O-Versicherung kann eine bedeutende Versicherungslücke schließen.

- **Haftungsprozesse gegen Geschäftsleiter werden oft gescheut, weil sie mit persönlichen Vorwürfen einhergehen.**

  Denn sie sind grundsätzlich im Haftungsverhältnis zu führen und das Organ trägt das Risiko von Deckungsausschlüssen - zum Beispiel grober Fahrlässigkeit oder Vorsatz.

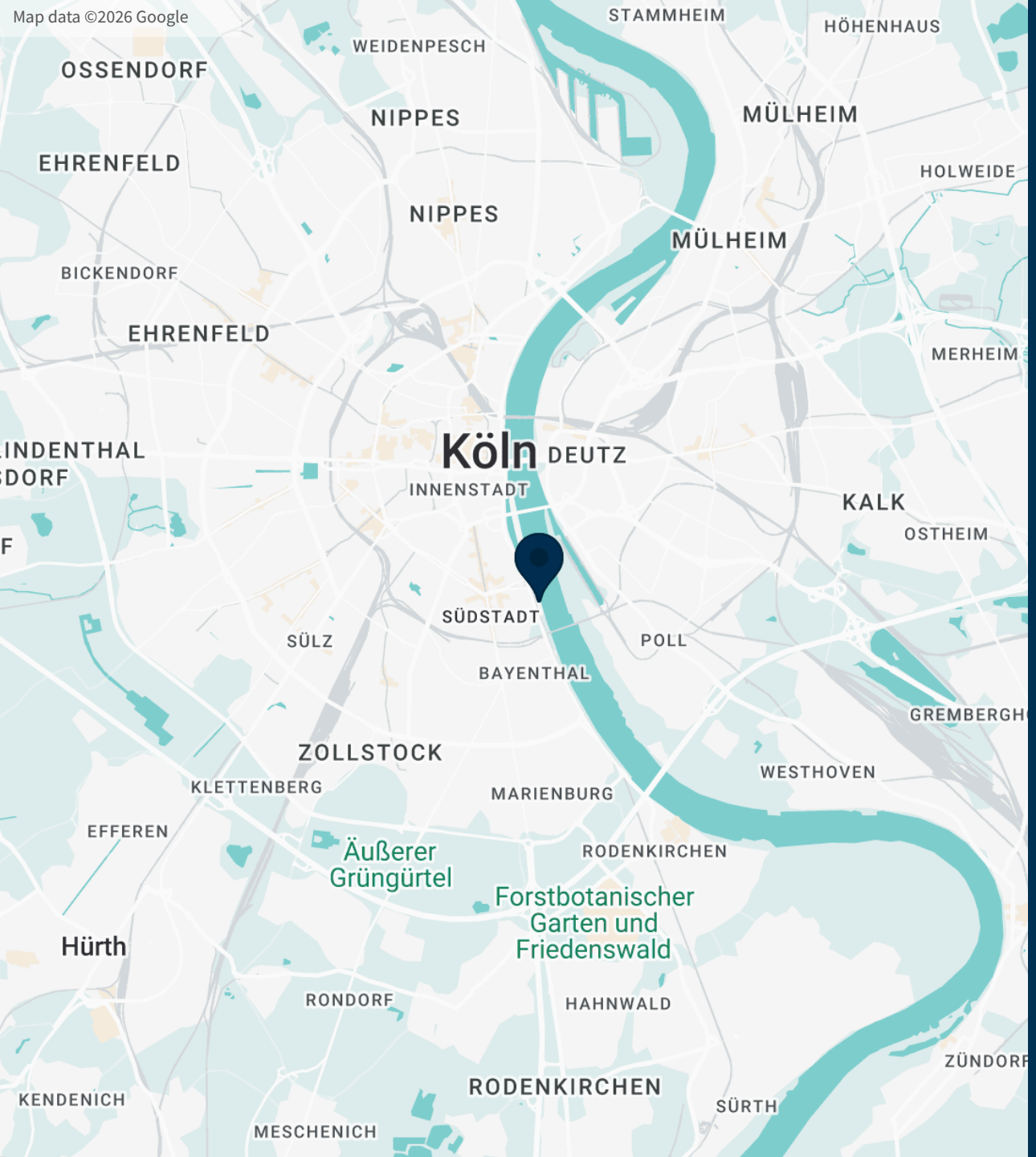
- **Cyberrisiken sind jedoch sehr schwer zu versichern.**

  Obliegenheiten in Cyberrisk-Policen gehen oft deutlich über regulatorische Anforderungen hinaus.

- **Mit der D&O-Versicherung besteht im Fall der Fälle oft jedoch sowieso ein Haftungsträger.**

  Die Rechtsprechung lässt bei sorgfältiger Gestaltung auch einen Direktprozess gegen den D&O-Versicherer aus abgetretenem Recht zu (BGH, Urt. v. 13.04.2016 – IV ZR 304/13, zitiert nach BeckRS 2016, 8173). Hierdurch kann eine Schadlosstellung erfolgen ohne einen Prozess gegen den betroffenen Geschäftsleiter führen zu müssen.

Hier ist Platz für Gedanken und Fragen.



Schnell erreichbar:

Agrippinawerft 24, 50678 Köln

+ 49 221 2080 7420

Notfall: +49 152 54122535

julian.zaudig@fgvw.de

Notfall: ra@zaudig.com

Dr. Julian Zaudig

www.fgvw.de