

# Der Cyberausschluss in der Berufshaftpflichtversicherung

---

*Hermann Wilhelmer\**

## I. Einleitung

Rechts- und wirtschaftsberatende Berufsträger sind besonders interessante Targets für Hacker. Sie verfügen über alles, woran Hacker interessiert sind: sensible Daten und Vermögenswerte.<sup>1</sup> Rechtsanwälte (Strafverteidiger) bzw Steuerberater (im Rahmen der Lohnverrechnung bzw der Beratung/Betreuung zum Sozialversicherungsrecht) über sensible personenbezogene Daten, Rechtsanwälte und Notare als Vertrags- bzw Urkundenerrichter im Zuge von M&A-Transaktionen über sensible Wirtschaftsdaten,<sup>2</sup> Patentanwälte bei der Begründung bzw Durchsetzung/Verteidigung von Patentrechten über hoch sensitive Geschäftsgeheimnisse ihrer Mandanten.

Auch die Organisation von Geldflüssen ist Teil der Dienstleistung von rechts- und wirtschaftsberatenden Berufsträgern. Rechtsanwälte und Notare verfügen als Treuhänder über nicht unerhebliches Mandantengeld. Erfolgreich

---

\* Dr. *Hermann Wilhelmer* ist Haftpflicht- und Versicherungsspezialist für rechts- und wirtschaftsberatende Berufe und Geschäftsführer der von Lauff und Bolz Versicherungsmakler GmbH.

1 *Garrie/Spemow*, Law Firm Cybersecurity (2017) 2. Dass es Hackern in erster Linie darum geht, mit ihren Angriffen Geld zu verdienen, zeigt auch der Zeitungsbericht „Hackerangriffe: Warum Anwaltskanzleien oft Lösegeld bezahlen“, <https://www.derstandard.at/story/2000140653714/hackerangriffe-warum-anwaltskanzleien-oft-loesegeld-bezahlen> (abgerufen am 24.7.2024); siehe ebenfalls *Rothmann/Segger*, Cyber-Erpressung und Cyber-Versicherung in der Praxis, d Anwaltblatt 2/2024, 152 ff.

2 Hacker können Anwaltsdaten erbeuten und für Aktiendeals nutzen, vgl dazu den Bericht in der Süddeutschen Zeitung v 30.12.2016.

vor Gericht erstrittene Geldbeträge sind von Rechtsanwälten an Mandanten weiterzuleiten. Steuerberater organisieren die Rücküberweisung von Steuerguthaben, die dem Mandanten gegenüber der Finanzverwaltung zustehen. Der Austausch über Überweisungsvorgänge, Bankdaten etc findet zum Teil per E-Mail statt, oftmals nur transport-, nicht Ende-zu-Ende-verschlüsselt.<sup>3</sup> Damit geht ein nicht unerhebliches Risiko einher, dass Hacker nach unbefugtem Zugang auf die IT von rechts- und wirtschaftsberatenden Kanzleien sich durch weitere Täuschungshandlungen Zugriff auf die vom jeweiligen Berufsträger verwahrten bzw treuhändig gehaltenen Vermögenswerte verschaffen.

Kommt es durch hacker-bedingte Täuschungshandlungen (etwa durch einen erfolgreichen Man-in-the-Middle-Angriff)<sup>4</sup> zum Abfluss von Daten oder von Mandantengelder,<sup>5</sup> werden die Rechte Dritter (des Mandanten) beeinträchtigt. Ist der erfolgreiche Hackerangriff durch ein fahrlässiges Verhalten des rechts- und wirtschaftsberatenden Berufsträgers mitverursacht, stellen sich in der Folge auch Haftungsfragen.<sup>6</sup> Gerade bei großen M&A-Deals kann ein Datenleak dazu führen, dass der Mandant in seinen Rechten, Rechtspositionen bzw in seinen Geschäftschancen geschädigt wird. (Hohe) Haftpflichtansprüche gegen den Berufsträger drohen.

Welche Dritthaftungsschadensszenarien für rechts- und wirtschaftsberatende Berufsträger denkbar sind, wird im Folgenden anhand von sechs Fallkonstel-

---

3 Zur Unterscheidung von Transport- und Ende-zu-Ende-Verschlüsselung in der elektronischen Kommunikation siehe ua *Schöttle/Ludwig*, Anwaltliche Kommunikation per E-Mail – nur noch mit Ende-zu-Ende-Verschlüsselung?, BRAK-Mitt 2020, 308 ff.

4 *Malek/Schütz*, Cyberversicherung – Überblick und aktuelle Probleme, PHi 5/2018, 174 ff (175).

5 Mandantengelder (bzw Gelder finanzierender Banken) werden von Rechtsanwälten oder Notaren vor allem im Zuge von Abwicklungstreuhandschaften übernommen, siehe dazu aus österreichischer Sicht *Wilhelmer*, Aktuelle Rechtsfragen der Treuhänderdeckung, ö AnwBl 2019, 757 ff (759–761); zur eingeschränkten Übernahme von Geldtreuhandschaften bei Immobilientransaktionen aus deutscher Sicht siehe *Haug/Zimmermann*, Die Amtshaftung des Notars<sup>4</sup> (2018) Rz 682 ff; *Sänger/Scheuch*, Wandel im Berufsbild: Mittelverwendungskontrolle als anwaltliche Tätigkeit? d AnwBl 6/2012, 497 ff. Auf diese Vermögenswerte können Hacker durch entsprechende Täuschungshandlungen ebenso „zugreifen“ wie auf Vermögenswerte der Berufsausübungsgesellschaft.

6 *Thesling*, EuGH erhöht Haftungsrisiken für Kanzleien bei Cyber-Risiken, d Anwaltblatt 2/2024, 157 ff; *Malek/Spittka*, Datenschutzrechtliche Haftungsrisiken nach Cyber-Vorfällen im Spiegel aktueller EuGH-Rechtsprechung, *VersicherungsPraxis* 2/2024, 3–6.

lationen beschrieben. Es stellt sich sodann die Folgefrage, ob diese Haftungsszenarien in der Berufshaftpflichtversicherung versichert sind.<sup>7</sup>

Sofern die Berufshaftpflichtversicherung cyberbedingte Haftpflichtrisiken deckt, was, wie unter III. ausgeführt, weitgehend der Fall ist, ist die Schlussfolgerung der Versicherer nachliegend, über die Einführung eines Cyber-Ausschlusses – wie in anderen Versicherungssparten – (auch) in der Berufshaftpflichtversicherung nachzudenken.<sup>8</sup> Am österreichischen Versicherungsmarkt gibt es bereits Versicherer, die einen Cyber-Ausschluss in die Berufshaftpflichtversicherung aufnehmen (wollen). Der überwiegende österreichische wie auch deutsche Versicherungsmarkt wartet mit der Aufnahme eines Cyber-Ausschlusses in die Berufshaftpflichtversicherung hingegen noch ab. Der englische Versicherungsmarkt geht ebenfalls einen interessanten Weg. Mittels einer „Cyber-Crime-Clause“ wird das cyberbedingte Drittschadensrisiko ausdrücklich als versichert erklärt/bestätigt (Deckung für „third-party-losses“), ausgeschlossen wird (deklaratorisch) nur der cyber-incident-bedingte Eigenschaden des Versicherungsnehmers (keine Deckung für „first-party-losses“) (siehe dazu näheres unten unter VI.A).

In diesem Beitrag wird sodann auf die Textierung sowie auf die Regelungsziele des Cyber-Ausschlusses eingegangen, wie er exemplarisch in Art 8 Ziffer 18 der ABHV 2023<sup>9</sup> eines großen österreichischen Versicherers in der Berufshaftpflichtversicherung am Markt seit 2023/2024 etabliert wird. Dieser Cyber-Ausschluss wird einer Interpretation unterzogen, um den Anwendungsbereich des Cyber-Ausschlusses festzustellen und eine Angemessenheitsprüfung vor-

7 Zur Beurteilung der Deckung von Cyber-Risiken in der Haftpflichtversicherung, insbesondere Berufshaftpflichtversicherung s *Scheuba*, Cyberversicherung als Haftpflichtversicherung, in *Promok*, Cyberversicherung (2023) 99 (101 ff); *Kath*, Die Cyber-Versicherung, *ZVers* 2019, 107 ff; *Keltner*, Versicherbarkeit von Cyber Risiken und ausgewählte Abgrenzungsfragen der Sparten Cyber-, Vertrauensschaden-, D&O- und Betriebshaftpflichtversicherung, in *Berisha/Gisch/Koban*, Haftpflicht-, Rechtsschutz- und Cyberversicherung (2018) 127–128; für Deutschland ähnlich *Riebert*, Versicherungsschutz rund um Cyber, *d AnwBl* 2018, 356–357; s dazu auch *Bertsch/Fortmann*, Silent-Cyber-Risiken in konventionellen Unternehmensversicherungen (Teil 2), *r+s* 2021, 549 (552–554) (dort zum Verhältnis Silent-Cyber und D&O-Versicherung); siehe dazu auch *Wilhelmer*, Berufshaftpflichtversicherung Rz 136.

8 Die Identifizierung bzw Vermeidung von Silent-Cyber-Cover in Versicherungssparten, die Cyber-Risiken nicht ausdrücklich als mitversichert benennen, ist allgemeine Strategie der Versicherungswirtschaft, siehe dazu *Bertsch/Fortmann*, *r+s* 2021, 549 ff; *Bertsch*, Silent Cyber – Darstellung und Bewältigung einer neuen Herausforderung (2021).

9 Generell zum ABHV-Deckungsstandard siehe *Wilhelmer*, Berufshaftpflichtversicherung Rz 339–440.

zunehmen. In diesem Zusammenhang findet auch eine kritische Beleuchtung des Cyber-Ausschlusses statt.

Abschließend wird der Frage nachgegangen, ob bzw in welchem Ausmaß ein Cyber-Ausschluss in der Berufshaftpflichtversicherung per se rechtswirksam vereinbart werden kann. Hierbei wird der Cyber-Ausschluss anhand der Maßstäbe, wie sie im Pflichthaftpflichtversicherungsrecht<sup>10</sup> sowie im freiwilligen Haftpflichtversicherungsrecht gegeben sind, einer Überprüfung und Bewertung unterzogen.

## II. Cyber-Haftungsszenarien für rechts- und wirtschaftsberatende Berufe

Werden rechts- und wirtschaftsberatende Berufsträger und deren Kanzlei-strukturen in einen Cyber-Angriff involviert, sind eine Vielzahl an Haftungs- bzw Schädigungsszenarien gegenüber dem Mandanten bzw sonstigen Dritten denkbar. Die nachfolgende Aufzählung an Haftungs- und Schadensszenarien erfolgt beispielhaft.

### A. Fall 1 – Datenverschlüsselung, Versäumnis prozessualer Fristen

In Folge einer erfolgreichen Phishing-Attacke<sup>11</sup> oder durch Übersendung eines mit Ransomware<sup>12</sup> infizierten Anhangs per E-Mail erlangen Hacker Zugriff

---

10 Zum Pflichtpflichtversicherungsrecht grundlegend für Österreich siehe *Fenyves*, Versicherungsvertragsrechtliche Grundfragen der Pflichthaftpflichtversicherung, VR 2005, 70 ff; *Rubin* in *Fenyves/Perner/Riedler*, VersVG § 158b Rz 1 ff. Für Deutschland siehe *Dallwig*, Pflichtversicherung (2014).

11 Eine Phishing-Attacke ist darauf gerichtet, durch Täuschungs-E-Mails Zugangsdaten des Empfängers herauszulocken. Phishing-Attacken stellen ein großes Cyber-Risiko dar, weil Mitarbeiter des Unternehmens durch Manipulation bzw Vortäuschen falscher Tatsachen dazu verleitet werden Zugangsdaten bzw anderweitige Unternehmensinformationen preiszugeben, siehe *Rother*, Cyber-Risiken: Risikomanagement und Versicherung, in *Berisha/Gisch/Koban*, Haftpflicht-, Rechtsschutzversicherung und Versicherungsvertriebsrecht 2019 (2020) 87 (99 f).

12 Eine besonders hohes Cyber-Angriffsrisiko repräsentieren Ransomware-Attacken. Ransomware ist eine Schadsoftware, die gezielt oder zufällig (etwa durch Anklicken eines Links) in IT-Systeme eingespielt wird und die alle auf einem Computer bzw IT-Netzwerk befindlichen Daten verschlüsselt, worauf Hacker eine Entschlüsselung der Daten gegen Zahlung eines Lösegelds anbieten, siehe *Eggen*, Die Cyberversicherung (2023) 39 f; *Kipker*, Cybersecurity<sup>2</sup> (2023) Kap 3 Rz 177. Angriffe durch Ransomware führen nicht zur Verschlüsselung von Daten, sondern auch zu Datenkopien, um auf dieser Basis mit einer Veröffentlichung der Daten zu drohen.

auf das IT-System und schließlich auf die Daten eines Rechtsanwalts. Die Daten werden in der Folge kopiert, exfiltriert und durch eine Ransomware verschlüsselt. Die Rechtsanwaltskanzlei kann in der Folge Arbeitsvorgänge nicht mehr ausführen. Es kommt ua zum Versäumnis prozessualer Fristen. Die dem Mandanten an sich berechtigt zustehende Forderung gegenüber einem Dritten „verfristet“ und eine Wiedereinsetzung in den vorherigen Stand wird infolge eines Verschuldens des Mitarbeiters der Anwaltskanzlei nicht genehmigt. Insofern ist die Forderung des Mandanten gegen den Dritten nicht mehr durchsetzbar und ein (reiner) Vermögensschaden tritt ein.<sup>13</sup>

## **B. Fall 2 – Man-in-the-Middle, umgeleitetes Steuerguthaben auf „Fake-Konto“**

Durch eine erfolgreiche Phishing-Attacke oder durch Übersendung eines mit Ransomware infizierten Dokumentes gelangen die Hacker in das IT-System eines Steuerberaters. Die Hacker lesen in der Folge als „Man-in-the-Middle“<sup>14</sup> die (nicht Ende-zu-Ende-verschlüsselte) Korrespondenz zwischen dem Steuerberater und dem Mandanten mit. Als es zur Rücküberweisung eines Steuerguthabens durch das Finanzamt an den Mandanten kommt, durchbricht der Hacker die Kommunikation zwischen dem Steuerberater und Mandanten, indem er in beide Richtungen die tatsächlich verfassten E-Mails abfängt und anstatt dessen gefälschte E-Mails versendet. Dadurch täuscht er sowohl den Steuerberater als auch den Mandanten über die Kontodaten des Mandanten. In der Folge überweist das Finanzamt das Steuerguthaben auf das „Fake-Konto“ der Hacker. Als der Betrug auffällt, ist das Geld vom Fake-Konto bereits abgebucht und damit verloren.

Der Mandant erleidet in Höhe des fehlgeleiteten Geldbetrages einen Vermögensschaden. Gegenüber dem Steuerberater wird in der Folge der Vorwurf erhoben, zum einen durch eine nicht erkannte Phishing-Attacke den Zugang zu den eigenen IT-System ermöglicht zu haben, zum anderen den weiteren Verlauf eines Man-in-the-Middle-Angriffs nicht bemerkt zu haben, was auch

---

Dies wiederum mit der Verbindung der Forderung nach Zahlung von Lösegeld zur Abwendung der Datenveröffentlichung.

13 Zum Forderungsverlust als reinen Vermögensschaden siehe *Wilbelmer*, Berufshaftpflichtversicherung Rz 1568.

14 *Malek/Schütz*, PHi 5/2018, 174 (175).

aufgrund der geringfügig veränderten E-Mail-Adresse, die von den Hackern verwendet wurde, möglich gewesen wäre.<sup>15</sup>

### C. Fall 3 – Datenleak, Verlust von Gewinnchancen

Aufgrund eines Datenleaks durch Veröffentlichung kopierter Daten, der auf einen Hackerangriff auf das IT-System eines Rechtsanwalts/Notars zurückgeht, kommt es zur Veröffentlichung wertvoller Daten und Geschäftsgeheimnisse des Mandanten. Darauf scheidet ein M&A-Deal oder kann dieser aus Sicht des Mandanten nur zu nachteiligeren Konditionen abgeschlossen werden. Der durch den Datenleak verursachte entgangene Geschäftsgewinn<sup>16</sup> oder die verschlechterte Verhandlungs- und daraus folgende Vermögenssituation wird als Schaden geltend gemacht.<sup>17</sup>

### D. Fall 4 – Veröffentlichung personenbezogener Daten

Die persönlichen Daten eines prominenten Mandanten (zB eines Fußballprofis) werden durch einen Hackerangriff in der Rechtsanwaltskanzlei gestohlen und im Darknet veröffentlicht. Der Mandant behauptet in der Folge einen aus der Datenveröffentlichung resultierenden Gefühlsschaden gem Art 82 DSGVO wegen erheblicher Furcht über die Verbreitung persönlichen Informationen (zB wegen Berichterstattung über seine sexuelle Orientierung).<sup>18</sup> In der Folge kommt es (auch) zu einem Reputationsverlust des Mandanten und dadurch zu einem berufsbedingten Verdienstentgang.<sup>19</sup>

---

15 Zur (potenziellen) (Organ-)Haftung im Fall manipulierter E-Mail-Adressen siehe *O. Lange*, Organhaftung und Phishing – oder: Wo versteckt man am besten ein Blatt? *r+s* 2023, 641 ff (647).

16 Ist das Vermögen im Sinne eines Gesamtvermögensvergleiches vermindert, tritt ein positiver Schaden ein, der bei leichtem Verschulden vom Haftpflichtigen zu ersetzen ist, siehe *Welser/Zöchling-Jud*, Bürgerliches Recht II<sup>14</sup> Rz 1433.

17 Tritt die Vermögensbeeinträchtigung dadurch ein, dass eine Gewinnchance nicht genutzt werden kann, ist der Schaden entgangener Gewinn, der nur bei grobem Verschulden vom Haftpflichtigen zu ersetzen ist, siehe *Welser/Zöchling-Jud*, Bürgerliches Recht II<sup>14</sup> Rz 1435.

18 Zum Schadenersatz, sofern er sich auf Art 82 DSGVO gründet, siehe *Spitzer*, Schadenersatz für Datenschutzverletzungen, *ÖJZ* 2019, 79 ff; *Malek*, Cyberversicherung: Datenschutzklagen und Schadenersatz wegen DSGVO-Verstößen, *PHI* 2020, 160 ff; *Malek/Spittka*, *VersicherungsPraxis* 2/2024, 3–6.

19 Zum Verdienstentgang als Schaden siehe *Welser/Zöchling-Jud*, Bürgerliches Recht II<sup>14</sup> Rz 1480 ff.