

Arglistanfechtung in der Cyberversicherung

16 U 63/24

5 O 128/21 Landgericht Kiel



Schleswig-Holsteinisches Oberlandesgericht

Beschluss

In dem Rechtsstreit

Agenda:

- 1. Deutsches Cyberurteil (LG Tübingen)
- 2. Deutsches Cyberurteil (LG Kiel)
- **NEU:** OLG Schleswig, Beschl. v. **14.10.2024** – 16 U 63/24

hat der 16. Zivilsenat des Schleswig-Holsteinischen Oberlandesgerichts in Schleswig durch den Vorsitzenden Richter am Oberlandesgericht Dr. Diercks, den Richter am Oberlandesgericht Dr. Biermann und den Richter am Oberlandesgericht Althoff am 14.10.2024 beschlossen:

1.

Der Senat beabsichtigt, die Berufung der Klägerin gegen das Urteil der 5. Zivilkammer des Landgerichts Kiel vom 23. Mai 2024 gemäß § 522 Abs. 2 ZPO zurückzuweisen, weil er einstimmig der Auffassung ist, dass die Berufung offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache auch keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts durch Urteil erfordert und auch die Durchführung einer mündlichen Verhandlung über die Berufung nicht geboten ist.

LG Tübingen

I. LG Tübingen (Urt. v. 26.5.2023 – 4 O 193/21)

FALL:

- Die Kl. interessierte sich für eine Cyberversicherung
- Am **13.2.2020** fand eine Veranstaltung in den Räumen der Kl. statt, an dem ein Vertreter des Assekuradeurs teilnahm und im Rahmen dessen der Versicherungsschutz bei der Bekl. vorgestellt sowie eine veraltete IT offengelegt wurde
- Am **3.4.2020** übersandte die Bekl. der Kl. auf eine invitatio hin ein Angebot, welches am 6.4.2020 angenommen wurde
- Bestandteil des Angebots sind vorab im Rahmen eines sog. Quotierungsprozesses gestellte und von der Kl. beantwortete Risikofragen

I. LG Tübingen (Urt. v. 26.5.2023 – 4 O 193/21)

FALL:

Die Bekl. stellte insgesamt acht Risikofragen, wobei die Kl. nur die letzte Frage mit „Nein“ und alle übrigen Fragen – **objektiv falsch** – mit „Ja“ beantwortete. Die Fragen haben u.a. folgenden Wortlaut:

3. Alle stationären und mobilen Arbeitsrechner sind mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet.

4. Verfügbare Sicherheitsupdates werden ohne schuldhaftes Zögern durchgeführt, und für die Software, die für den Betrieb des IT-Systems erforderlich ist, werden lediglich Produkte eingesetzt, für die vom Hersteller Sicherheitsupdates bereitgestellt werden (dies betrifft va Betriebssysteme, Virens Scanner, Firewall, Router, NAS-Systeme).

I. LG Tübingen (Urt. v. 26.5.2023 – 4 O 193/21)

FALL:

- am **29./30.5.2020** kam es zu einem Ransomware-Angriff inkl. der Verschlüsselung von Daten
- nach IT-forensischen Untersuchungen hat die Bekl. am **4.6.2020** den Rücktritt vom Versicherungsvertrag wegen arglistiger Falschangaben erklärt

I. LG Tübingen (Urt. v. 26.5.2023 – 4 O 193/21)

LÖSUNG: Arglist verneint

- Trotz des Einsatzes von zumindest 11 veralteten Servern ist allenfalls die Frage 4 bei der Antragstellung im April 2020 falsch beantwortet worden.
- Der Kl. ist zuzugeben, dass die Risikofrage 3 sich auf stationäre und mobile Arbeitsrechner und eben nicht auf Server bezieht.
- Auch bezüglich der Risikofrage 4 ist jedoch nicht von einer vorsätzlich und erst recht nicht von einer arglistig falschen Beantwortung auszugehen. Unabhängig von der rechtlichen Einordnung der Veranstaltung am 13.2.2020 und der genauen Rolle des Zeugen B hat die **Beweisaufnahme ergeben, dass für die Mitarbeiter der Kl. durch diese Veranstaltung übereinstimmend der Eindruck entstanden ist, dass seitens der Bekl. keine hohen Anforderungen hinsichtlich der IT-Sicherheit gestellt werden. (...)**

LG Kiel

II. LG Kiel (v. 23.5.2024 – 5 O 128/21)

Arglistanfechtung bei einer im Invitatio-Modell abgeschlossenen Cyberversicherung

1. Täuscht der VN den VN arglistig über im Rahmen der Erstellung einer Invitatio ad offerendum des VN über ein Online-Portal des VR erfragte Risikoumstände, so kann der VR den Vertrag auch dann nach § 20, § 22 VVG, § 123 Abs. 1 BGB anfechten, wenn er die entsprechenden Risikofragen nicht in Textform nach § 126b BGB gestellt und den VN nicht iSv § 19 Abs. 5 VVG hingewiesen hat.

2. Fragt der VR im Rahmen der Vertragsverhandlungen über den Abschluss einer Cyberversicherung danach, ob „Arbeitsrechner“ mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet seien, so beschränkt sich die Frage aus Sicht eines durchschnittlichen VN nicht auf Arbeitsplatzrechner, sondern schließt auch die im Netzwerk des VN installierten Server mit ein.

3. Ein VN (oder eine für diese handelnde Person) beantwortet eine von VR im Rahmen der Vertragsverhandlungen über den Abschluss einer Cyberversicherung gestellte Risikofrage danach, ob verfügbare Sicherheitsupdates ohne schuldhaftes Zögern durchgeführt werden, „ins Blaue hinein“ und damit bewusst unrichtig, wenn er sich lediglich darauf verlässt, dass die hiermit generell beauftragten Mitarbeiter die Sicherheitsupdates durchgeführt haben, insbes. dann, wenn ihm eine entsprechende Kontrolle jederzeit unschwer möglich gewesen wäre.

OLG Schleswig

In Anlegung dieser Maßstäbe ist es berufsrechtlich nicht zu beanstanden, dass das Landgericht dazu gefunden hat, dass der Zeuge ■■■ arglistig gehandelt habe; der Senat

16 U 63/24

Seite 15

teilt diese Beurteilung, §§ 286, 529 ZPO.

FALL:

- VN betreibt Holzgroßhandel
- Zum Betrieb eines Webshops wurde ein Web-SQL-Server mit dem Betriebssystem Windows 2008 eingesetzt, für den seit Januar 2020 kein Software- und Sicherheitsupdate mehr bereitgestellt wurde
- Der Support des Herstellers endete bereits 2015
- Ein erweiterter Support-/Update-Vertrag wurde nicht abgeschlossen
- Der Server verfügte nicht über Antiviren-Software
- Außerdem wurden mit Windows 2003-Betriebssystem neben einem Fax-Server zwei weitere Rechner als Speicherplatz für Kundendaten eingesetzt; diese Rechner verfügten ebenso wenig über Antivirenschutz
- Der Domain-Controller befand sich im Auslieferungszustand März 2019 (war also seit jeher „ungepatcht“).

FALL:

- Am 12.03.2020 schloss die Kl. bei der Bekl. eine Cyberversicherung ab
- U.a. wurden folgende Risikofragen gestellt und vom IT-Leiter der Kl. mit „Ja“ beantwortet:
 - 3. alle stationären und mobilen Arbeitsrechner sind mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet.
 - 4. verfügbare Sicherheit Updates werden ohne schuldhaftes Zögern durchgeführt, und für die Software, die für den Betrieb des IT-Systems erforderlich ist, werden lediglich Produkte eingesetzt, für die vom Hersteller Sicherheitsupdates bereitgestellt werden (dies betrifft v.a. Betriebssysteme, Virens Scanner, Firewall, Router, NAS-Systeme).
- Am 10.10.2020 erlangte ein externer Angreifer Zugang zu dem Computersystem der Kl. und missbrauchte dieses insbesondere zum Bitcoin Mining (Daten- & BU-Schaden).

FALL:

- Am 18.08.2021 erklärte die Bekl. Rücktritt (§ 19 VVG) und Anfechtung (§ 123 BGB)

LÖSUNG:

Arglistanfechtung gem. § 22 VVG i.V.m. § 123 BGB greift durch.

FRAGEN DES VR IN TEXTFORM

Für die Anfechtbarkeit kommt es – mit dem Landgericht (U 11) und entgegen der Berufung – nicht darauf an, ob die Risikofragen der Klägerin im Sinne von §§ 19 Abs. 1 Satz 1 VVG, 126 b BGB förmlich in Textform gestellt worden sind. Schon unerfragt gemachte falsche Angaben vermögen eine arglistige Täuschung zu begründen (vgl. nur Langheid/*Wandt-Bußmann*, VVG, Kommentar, 3. Auflage, § 22 Rn. 18 m.w.N.). Erst recht kann die Falschbeantwortung nur mündlicher, aber tatsächlich gestellter Fragen eine arglistige Täuschung auslösen (Langheid/*Wandt-Bußmann*, ebd. Rn. 19 m.w.N.). Das muss entsprechend umso mehr gelten, wenn die Fragen wie hier nicht nur mündlich, sondern genau ausformuliert in einer lesbaren Form gestellt worden sind.

OBJEKTIVE FALSCHBEANTWORTUNG:

- Risikofrage 3), ob alle stationären und mobilen Arbeitsrechner mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet sind, wurde objektiv falsch beantwortet.
- Server = Arbeitsrechner, die vom Arbeitsplatzrechner abzugrenzen seien
- Erkennbar seien IT-gefahrenspezifisch alle Rechner gemeint, die im Netzwerk miteinander verbunden sind
- Verteilung über einen Management-Rechner unmaßgeblich, weil nach „*allen*“ Rechnern gefragt wird
- Risikofrage 4) wurden ebenso objektiv falsch beantwortet
- „Unverzüglich“ updaten meine erkennbar ohne schuldhaftes Zögern
- Die Frage 4) beziehe sich eindeutig auf alle Rechner

ARGLIST: (+)

Die VN hat sich wie folgt verteidigt:

- Die KI. hat sich dahingehend eingelassen, dass der Zeuge ... bei der Beantwortung der Risikofragen weder an den Windows 2003 Server und Speicherplatz, noch an den als SQL-Server für den Betrieb des WEB-Shops genutzten Windows 2008 Rechner **gedacht** habe. Auch sei ihm **unbekannt** gewesen, dass der Domain-Controller DC09 seit März 2019 kein Update oder Virenschutz erhalten hatte und sich noch im Auslieferungszustand befunden habe.
- Der Zeuge ... bestätigte diesen Vortrag der KI. im Rahmen seiner Vernehmung und gab an, er habe sich **darauf verlassen, dass die von ihm hierzu beauftragten Mitarbeiter**, wie der inzwischen verstorbene Angestellte ... sowie der externe Dienstleister ..., die ihnen übertragenen Aufgaben zur Absicherung des Netzwerkes korrekt wahrgenommen hätten.

ARGLIST: (+)

Arglist (allgemein)

Die bewusste Falsch- oder Nichtbeantwortung von Fragen genügt für sich genommen nicht für Arglist. Vielmehr muss in subjektiver Hinsicht hinzukommen, dass der VN auf die **Entschließung des VR Einfluss nehmen will und sich daher bewusst ist, dass der VR möglicherweise (bedingter Vorsatz genügt) seinen Antrag nicht** oder nur unter erschwerten Bedingungen annehmen werde, wenn er die Wahrheit sage (BGH NJW 2007, 2041; VersR 2011, 337 Rn. 19; OLG Koblenz VersR 2013, 1113 (1114); OLG Karlsruhe NJW 2014, 3733; OLG Hamm VersR 2018, 282 (283); VersR 2020, 538 (539)).

Eine **Vermögensschädigung / Bereicherungsabsicht braucht aber nicht** geplant zu sein (RGZ 96, 345 (346); BGH VersR 1957, 351 (352); VersR 2007, 785 Rn. 8; VersR 2008, 809 Rn. 8; OGH Österreich VersR 1978, 954).

Unkenntnis entlastet den VN nicht, wenn er im Bewusstsein seiner Unkenntnis „**ins Blaue hinein**“ Angaben macht (OLG Hamm VersR 1990, 765; OLG München VersR 2000, 711 (712); OLG Koblenz VersR 2004, 849 (851); KG VersR 2007, 381 (382); OLG Frankfurt a. M. ZfS 2009, 269; OLG Saarbrücken VersR 2020, 91 Ls. Rn. 35; OLG Hamm VersR 2020, 538 (539)).

Dasselbe gilt, wenn er sich sehenden Auges der Kenntnis verschließt (BGH VersR 1993, 170 (171)).

Dass Arglist vorgelegen hat, muss der Versicherer darlegen und beweisen (BeckOK VVG/Spuhl, 18. Ed. 1.2.2023, VVG § 21 Rn. 55).

ARGLIST: (+)

- Den Cyber-VN treffen **besondere Sorgfaltspflichten** (400 AN, 143,5 Mio € Umsatz)
- Es geht um Angaben zum **aktuellen Status** der IT-Sicherheit und nicht um in der Vergangenheit liegende Informationen
- VN verfügt über IT-Abteilung und damit über **Fachkompetenz**
- Es gab kein IT-Management-Konzept
- IT-Zuständigkeiten waren nicht klar geregelt
- Delegierte Aufgaben wurden nicht kontrolliert
- Der AN, der für AN die Risikofragen beantwortete, hatte **den IT-Zustand nicht verifiziert und auch keine Rückfragen bei Kollegen gehalten** (= Erkundigungspflicht)
- IT-Sicherheitsstatus wäre leicht ermittelbar gewesen
- Heißt: der VN hatte keine genaue Kenntnis von der IT-Sicherheit und beantwortete die Risikofragen damit „**ins Blaue hinein**“
- Ein „Irrtum“ liege nicht vor, weil der betreffende AN wusste, dass er keine genaue Faktenkenntnis habe („**bewusste Unkenntnis**“)