LG Kiel (5. Zivilkammer), Urteil vom 23.05.2024 – 5 O 128/21

ECLI:DE:LGKIEL:2024:0523.5O128.21.0A

Tenor:
Die Klage wird abgewiesen.
Die Klägerin trägt die Kosten des Rechtsstreits.
Das Urteil ist gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand:
1 Die Klägerin macht gegen die Beklagte Ansprüche aus einer Cyber-Versicherung geltend.
2 Die Klägerin betreibt in Norddeutschland an 16 Standorten einen Holzgroßhandel mit der Möglichkeit einer Online-Bestellung für ihre ausschließlich gewerblichen Kunden. Mit Wirkung ab 12.03.2020 schloss die Klägerin unter Vermittlung der ... eine Cyber-Versicherung bei der Beklagten ab, welche hierbei von der ... als Assekuradeurin vertreten wurde. Die Angaben des auf Seiten der Klägerin tätigen Mitarbeiters der Maklerin, des Zeugen ..., erfolgten in Zusammenarbeit und nach Rücksprache mit dem Zeugen ..., der die IT-Abteilung der Klägerin leitet. Grundlage des Vertrages ist der Versicherungsschein gemäß Anlage WH 1. Es gelten die allgemeinen Versicherungsbedingungen der Beklagten gemäß den Anlagen WH 2 und B 1. Zusätzlich finden die Sondervereinbarungen der Beklagten für durch die ... vermittelten Verträge gemäß den Anlagen WH 3 und WH 3a Anwendung. Diese sehen unter anderem Folgendes vor:

„Der Versicherer erkennt an, dass ihm bei Abschluss des Versicherungsvertrages alle Gefahrumstände, die für seinen Entschluss, den Vertrag mit dem vereinbarten Inhalt zu schließen, erheblich waren, bekannt geworden sind. Dieses Anerkenntnis gilt jedoch nicht für Gefahrumstände, die durch den Versicherungsnehmer arglistig verschwiegen wurden…“

3 Der Vertragsschluss erfolgte elektronisch über ein Onlineportal, bei dem für den Vertragsschluss gemäß der Anlage WH 11 einzelne Felder am Bildschirm ausgefüllt und bestätigt werden müssen. Unter dem Schritt 5 werden Risikofragen gestellt, die der für die Klägerin tätige Makler wie folgt beantwortete:

„A 5.4 Risikofragen
1. Die IT des Unternehmens wird durch mindestens einen IT-Spezialisten betreut:
Ja
2. Es werden regelmäßig (mindestens wöchentlich) Datensicherungen durchgeführt:
Ja
3. Alle stationären und mobilen Arbeitsrechner sind mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet:
Ja
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 v.a. Betriebssysteme, Virenscanner, Firewall, Router, NAS-Systeme):
Ja
5. Es existieren Regelungen zum Umgang mit IT-Zugangsdaten im Unternehmen, deren Umsetzung überwacht wird:
Ja
6. Es werden Hard- und Software (wie Firewalls) zum Schutz des Unternehmensnetzwerks eingesetzt:
Ja

7. Mitarbeiter dürfen private Geräte für dienstliche Zwecke verwenden:

Ja

8. Gab es in den letzten drei Jahren einen Cyber-Schaden oder einen Datenschutzvorfall im Unternehmen?: Nein“

4 Im Unternehmen der Klägerin wurde zum Betrieb ihres Webshops ein Web SQL-Server mit dem Windows-Betriebssystem 2008 eingesetzt, für den seit Januar 2020 kein Software- und Sicherheitsupdate mehr bereitgestellt wurde. Der Support und damit die Zusatzfunktionen für dieses Programm endeten bereits 2015. Einen vom Hersteller angebotenen erweiterten Support- und Updatevertrag hatte die Klägerin für diesen Rechner nicht abgeschlossen. Jedenfalls zum Zeitpunkt des Schadensfalls bestand über diesen Server eine Zugriffsmöglichkeit auf das IT-System der Klägerin, ohne durch eine Firewall zusätzlich geschützt zu sein. Der Web SQL-Server verfügte auch nicht über einen Virenscanner oder eine Antiviren-Software. Außerdem wurden neben einem Fax-Server mit Windows 2003 Betriebssystem zwei weitere Rechner mit dem Betriebssystem Windows 2003 als Speicherplatz im Unternehmen der Klägerin eingesetzt, auf die Arbeitsplatzrechner im Betrieb der Klägerin zugreifen konnten. Diese drei Windows 2003 Server verfügten ebenfalls nicht über einen Virenscanner. Einer der beiden im Unternehmen eingesetzten Domain-Controller, der DC 09, befand sich im Auslieferungszustand von März 2019, das heißt seit diesem Zeitraum waren keine Aktualisierung oder Sicherheitsupdates an diesem durchgeführt worden. Auf einem der rund 399 im Betrieb der Klägerin eingesetzten Rechner war das SMB1 Protokoll aktiv, bei dem seit 2017 Schwachstellen bekannt waren und dessen Deaktivierung auf allen Systemen empfohlen worden war. Der Domain-Controller diente als Bereichssteuerung der zentralen Authentifizierung von Computern und Benutzern des gesamten Rechnernetzes der Klägerin. Im Netz der Klägerin existierte eine hohe Anzahl von Benutzerkonten mit administrativer Zugangsberechtigung, nämlich insgesamt 77 Nutzer. Bei der Begutachtung des Schadensfalls durch eine von der Beklagten beauftragte Sachverständige wurden im IT-System der Klägerin Passwörter wie ..., ..., ... oder ... festgestellt.
5 Seit mindestens dem 18.09.2020 hatte ein externer Angreifer Zugriff auf das IT-System der Klägerin. Am Samstag, den 10.10.2020 um 21:30 Uhr erfolgte durch den Mitarbeiter der Klägerin ... bei der ... eine Schadensmeldung. Zuvor war dem Mitarbeiter eines externen Dienstleisters der Klägerin, dem Zeugen ..., der mit dem Umbau der Firewall beauftragt worden war, aufgefallen, dass es zu einem hohen unüblichen Datenfluss bzw. Zugriffsversuche aus dem eigenen Netz gekommen war. Die Ursache hierfür war eine durch einen Hackerangriff über den als Webserver genutzten Windows 08 Rechner eingeschleuste Schadsoftware. Das IT-System der Klägerin wurde heruntergefahren, sodass der Betrieb zunächst stillstand.
6 Die Beklagte ließ ein Gutachten mit forensischer Analyse durch die Diplom-Informatikerin ... einholen, welches am 16.10.2020 vorlag. Wegen des Inhaltes wird auf die Anlage ... Bezug genommen. Danach sei durch die eingeschleuste Schadsoftware DoublePulsar und Eternal Group in das IT-System die Rechnerkapazität der Klägerin für Bitcoin Mining benutzt worden. Auf dem SQL-Server sei das Vorliegen von Schadsoftware bestätigt worden.
7 Mit Schreiben vom 20.10.2020 erklärte die ... für die Beklagte gemäß § 19 Abs. 2 VVG den Rücktritt vom Vertrag (Anlage WH 5) und die Leistungsfreiheit für den geltend gemachten Schadensfall. Mit der Klagerwiderung vom 18.08.2021 hat die Beklagte zudem die Anfechtung wegen arglistiger Täuschung erklärt.
8 Mit Schreiben vom 21.12.2020 forderte die Klägerin die Beklagte zur Leistung auf (Anlage WH 7).
9 Die Klägerin ist der Ansicht, dass, da der Vertrag nur über ein Onlineportal per Anklicken geschlossen worden sei, die streitgegenständlichen Risikofragen der Klägerin bzw. der von ihr beauftragten Maklerfirma nicht in Textform gemäß § 126b BGB gestellt worden seien. Auch

liege keine Belehrung gemäß § 19 Abs. 5 VVG in Textform vor. Die vor dem Vertragsschluss abgegebene Erklärung werde nicht als PDF übermittelt oder ausgedruckt. Nach dem Anklicken des Buttons „Invitatio-Anfragen“ erhalte der Nutzer eine E-Mail seitens der ... mit – unstreitig – dem folgenden Wortlaut: „Vielen Dank für ihre Invitatio-Anfrage zu dem oben genannten Kunden. Gerne bestätigen wir ihnen die Annahmen der Anfrage. Die Quotierung wurde in ein Invitatio (Angebot) umgewandelt und steht ihnen unter der oben genannten Vorgangsnummer im System zur Verfügung. Sie können die Invitatio dort ab sofort exportieren (Download oder Druck) oder durch Videoklicks in einen gültigen Versicherungsvertrag umwandeln“ (s. Anlage WH 11). Es sei nicht erforderlich die Invitatio abzurufen, um einen gültigen Vertragsschluss herbeizuführen, sondern es könne stets direkt ein gültiger Versicherungsvertrag generiert werden, der dann erst mit der Policen-Version und der Prämienrechnung als PDF-Anhänge übermittelt werde.

10 Die Klägerin habe die Risikofragen nicht falsch beantwortet, jedenfalls habe der insoweit tätige Zeuge ... nicht vorsätzlich oder arglistig gehandelt. Der Windows 08 Rechner sei als Web-SQL-Server genutzt worden und gehöre zu einem sogenannten Portalserver. Dort seien ausschließlich Daten gespeichert worden, die nicht hätten portiert werden können und nur als „Lagerfläche“ gedient hätten. Der Rechner habe als „Mittler“ zwischen dem Web-Shop der Klägerin und ihrem Warenwirtschaftssystem gedient. Er habe sich bei Antragsstellung in einer sogenannten demilitarisierten Zone (DMZ) befunden, das heißt sei durch eine externe und eine interne Firewall der deutschen T. geschützt gewesen, sodass nach Auffassung des Zeugen ... von diesem kein Sicherheitsrisiko ausgegangen sei. Im Vorfeld des Cyberschadens habe die Klägerin im August 2020 ihren Web-Shop nicht mehr betreiben können, weil ein Rechenzentrum der T. ausgefallen sei. Auf Vorschlag des externen Dienstleisters ..., eines Mitarbeiters der Firma ... IT Solutions, sei eine zweite Datenleitung für den Web-Shop genutzt worden und hierbei der zum Zeitpunkt der Antragstellung in einer DMZ befindliche Windows 08 Server bei Umbau der Firewall ungeschützt ins Netz gestellt worden. Hierüber habe der Zeuge ... die Klägerin nicht informiert.

11 Für die Sicherheitsupdates und Windows-Patches sei der inzwischen verstorbene Mitarbeiter der Klägerin ... zuständig gewesen. Der Zeuge ... sei davon ausgegangen, dass durch den Mitarbeiter ... sowie den nach der Erkrankung des Zeugen ... verstärkt hinzugezogenen externen Dienstleister ... die erforderlichen Aktualisierungen und Updates erfolgt seien. Ein Rechner mit Windows 2003 Betriebssystem sei als Fax-Server zwar angeschlossen, aber nicht mehr benutzt worden. Die weiteren zwei Rechner mit Windows 2003 Betriebssystem seien ausschließlich als Speicherplatz zur Datenablage genutzt worden. Man habe sich auf diesen nicht anmelden können. Bei Beantwortung der Risikofragen habe der Zeuge ... nicht an diese Rechner gedacht.

12 Im Übrigen ist die Klägerin der Ansicht, dass unter den Begriff des Arbeitsrechners in der Frage zu Ziffer 3) die als Speicher genutzten Windows Server 2003, der Web-Server mit dem Betriebssystem 2008 sowie der Domain Controller nicht zu fassen seien. Auch die Frage 4) sei nicht falsch beantwortet worden, da für den Windows 2008 Rechner der Hersteller gegen Entgelt noch Sicherheitsupdates bereitgestellt habe.

13 Die Frage zu Ziffer 5) sei ebenfalls nicht fehlerhaft beantwortet worden. Es gebe im Unternehmen eine klare Kennwortrichtlinie. Allein den Lagerarbeitern seien wegen der Handscanner und der Arbeit mit Handschuhen einfachere Kennwörter erlaubt. Das Passwort für den Domain-Administrator „...“ sei vor Einführung der Richtlinie eingerichtet und nicht mehr geändert worden. Dies sei dem Zeugen ... nicht bekanntgewesen. Eine Falschbeantwortung der Risikofragen sei jedenfalls schuldlos erfolgt.

14 Im Übrigen bestreitet die Klägerin, dass die Beklagte den Versicherungsvertrag in Kenntnis aller tatsächlichen Umstände nicht oder nicht so geschlossen hätte.

15 Nach Bemerken der Infizierung mit Schadsoftware habe die Klägerin den Schaden der ... gemeldet und das weitere Vorgehen mit dieser abgestimmt. Eine Bezifferung des Schadens sei der Klägerin zunächst nicht möglich gewesen, sodass sie zunächst einen

Feststellungsantrag gestellt habe. Es sei letztlich erforderlich gewesen, die gesamte Infrastruktur neu aufzubauen, da es aussichtslos gewesen sei, die Schadsoftware restlos zu beseitigen. Zur Schadensbeseitigung habe die Klägerin die Firma ... IT GmbH beauftragt, die ihre Leistungen mit insgesamt 130.190,88 € sowie weiteren 239.160,09 € abgerechnet habe. Zudem seien EDV-Kosten in Höhe von insgesamt 55.634,55 € entstanden. Wegen der Zusammensetzung der einzelnen Kosten wird auf die Anlagen WH 12, WH 13 und WH 14 Bezug genommen.

16 Die Klägerin hatte mit der Klage zunächst beantragt festzustellen,

1. dass die Beklagte verpflichtet ist, der Klägerin aus dem Versicherungsvertrag DE ... Versicherungsschutz für den Schadenfall vom 10.10.2020, Schadenfallnummer ... zu gewähren sowie
2. die Beklagte zu verpflichten, der Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 2.810,19 € nebst 5% Zinsen über dem Basiszinssatz seit Rechtshängigkeit zu zahlen.

17 Mit Schriftsatz vom 05.02.2024 hat die Klägerin ihre Klage erweitert und beantragt nunmehr neben dem aufrechterhaltenen Antrag zu Ziffer 2)

1. a) die Beklagte zu verurteilen, an die Klägerin 687.952,23 € nebst Zinsen in Höhe von 5% über dem Basiszinssatz seit Zustellung dieses Schriftsatzes zu zahlen sowie

b) festzustellen, dass die Beklagte verpflichtet ist, der Klägerin auch darüber hinaus aus dem Versicherungsvertrag DE ... Versicherungsschutz für den Schadenfall vom 10.10.2020, Schadenfallnummer ... zu gewähren.

18 Zuletzt hat die Klägerin unter Verweis auf einen Additionsfehler in ihrer Excel-Tabelle beantragt,

1. a) die Beklagte wird verurteilt, an die Klägerin 424.985,52 € nebst Zinsen in Höhe von 5% über dem Basiszinssatz seit Zustellung dieses Schriftsatzes zu zahlen sowie

b) festzustellen, dass die Beklagte verpflichtet ist, der Klägerin auch darüber hinaus aus dem Versicherungsvertrag DE ... Versicherungsschutz für den Schadenfall vom 10.10.2020, Schadenfallnummer ... zu gewähren und

2. die Beklagte zu verpflichten, der Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 2.810,19 € nebst 5% Zinsen über dem Basiszinssatz seit Rechtshängigkeit zu zahlen.

19 Die Beklagte beantragt, die Klage abzuweisen.
20 Die Beklagte trägt vor, dass der Versicherungsvertrag nach einem Invitatiomodell abgeschlossen worden sei. Bevor der Button „Annahmeprozess invitatio starten“ gedrückt werde, könne auf das individuelle Angebot, welches als wichtige Angebotsunterlage gemäß Anlage ... zugesandt worden sei, zugegriffen und dieses noch einmal bearbeitet werden.
21 Erfolgte Änderungen müssten nochmals bestätigt werden.
22 Die mit der ... vereinbarten Sondervereinbarungen würden erst mit Vertragsschluss Vertragsbestandteil. In dem hier erfolgten Abschluss des Vertrages im Invitatiomodell erfolge die Beantwortung der Risikofragen durch die Klägerin noch vor dem Angebot der Beklagten und der Abgabe der Invitatio an die Beklagte. Diese fertige erst daraufhin das Vertragsangebot. Der Vertrag komme danach erst durch die Annahme durch die Klägerin zustande. Im Übrigen finde die in der Sondervereinbarung enthaltene Anerkennungsklausel bei der Falschbeantwortung ausdrücklich gestellter Fragen keine Anwendung.

23 Die Beklagte behauptet, dass der Zustand der IT der Klägerin katastrophal gewesen sei. In Kenntnis der Unzulänglichkeiten des IT-Systems, insbesondere der Nutzung von Rechnern mit fehlendem aktiven Sicherheitsupdate wäre der Versicherungsvertrag niemals geschlossen worden, da dies das Schadensrisiko um ein Vielfaches erhöhen würde. In dem IT-System der Klägerin seien „End to life“ Systeme mit unzureichenden Patches genutzt worden. Die Firewall der T. sei unzureichend gewesen. Es habe zudem an klaren Verantwortungsabgrenzungen zwischen den Zeugen ... und ... sowie dem externen Dienstleister ... und an Kontrollmechanismen gefehlt.
24 Die Klägerin bzw. deren Wissensvertreter ... und ... hätten vorsätzlich und arglistig gehandelt. Bei einem Auslesen der Patches und Supportlevels hätte die Klägerin die gefahrerhöhenden Umstände erkennen können. Sie treffe eine Erkundungspflicht. Falls bei dem Vertragsschluss Angaben ohne eigene Erkenntnis „ins Blaue hinein“ erfolgt seien, so sei dies arglistig. Der für die IT-Leitung zuständige Zeuge ... verfüge nicht über das entsprechende Fachwissen, sodass auch die Frage 1) fehlerhaft beantwortet worden sei.
25 Die Beklagte ist der Ansicht, dass sie jedenfalls gemäß den §§ 23 ff. VVG wegen Gefahrerhöhung bzw. gemäß § 81 Abs. 2 VVG wegen grob fahrlässiger Herbeiführung des Versicherungsfalls leistungsfrei geworden sei. Es liege auch nach dem Klägervortrag jedenfalls eine nachträgliche Gefahrerhöhung durch den Einsatz des Windows 2008 Servers ohne Firewall-Schutz vor.
26 Das Gericht hat im Termin vom 09.11.2022 den Geschäftsführer der Klägerin, Herrn Dr. ..., persönlich angehört. Diesbezüglich wird Bezug genommen auf das Sitzungsprotokoll vom 09.11.2022 (Bl. 181 ff. d. A.). Zudem wurde der Zeuge ... zur IT-Ausstattung der Klägerin und zur Durchführung des Vertragsschlusses in Zusammenarbeit mit der ... und der Information des dort tätigen Mitarbeiters ... vernommen. Die Vernehmung erfolgte in Anwesenheit des IT-Sachverständigen ... , der im Termin zusätzlich Stellungnahmen zum IT-System der Klägerin und der Risiken eines Schadenseintritts abgegeben hat. Wegen des Ergebnisses der Beweisaufnahme wird Bezug genommen auf das Sitzungsprotokoll vom 28.02.2024 (Bl. 385 ff. d. A.).

Entscheidungsgründe:
27 Die Klage ist nicht begründet.
28 Der Klägerin steht gegen die Beklagte kein Anspruch auf Zahlung von Versicherungsleistungen aus dem zwischen den Parteien geschlossenen Versicherungsvertrag zu, da der Vertrag aufgrund der von der Beklagten erklärten Anfechtung wegen arglistiger Täuschung nichtig ist (§§ 20, 22 VVG i.V.m. §§ 123 Abs. 1, 142 Abs. 1 BGB).
29 Die Beklagte hat mit der Klagerwiderung vom 18.08.2021 und damit noch binnen der Jahresfrist des § 124 BGB die Anfechtung des Vertrages wegen arglistiger Täuschung erklärt.
30 Die Klägerin hat die Beklagte bei Vertragsschluss über vertragsrelevante Risiken arglistig getäuscht, indem sie nach Überzeugung der Kammer jedenfalls die im Rahmen der Invitatio gestellten Risikofragen zu Ziffer 3) und 4) durch ihren beauftragten Verhandlungsgehilfen, den Zeugen ..., falsch beantworten ließ, der seine Angaben im Bewusstsein seiner Unkenntnis ins Blaue hinein machte. Zwischen den Parteien ist unstreitig, dass, wie sich auch aus der von der Klägerin vorgelegten Anlage WH 11 ergibt, dem Abschluss des Versicherungsvertrages zunächst eine sogenannte Invitatio vorausgeht, bei der der künftige Versicherungsnehmer, also hier die Klägerin über ihren Makler, nicht nur allgemeine Angaben zu ihrem Unternehmen und den Umfang des gewünschten Versicherungsschutzes über ein Onlineportal eingibt, sondern auch die dort abgefragten Risikofragen entweder mit ja oder nein beantworten muss, um im Anschluss die Invitatio starten zu können, das heißt die Beklagte als Versicherung zur Abgabe eines Angebotes auf Abschluss eines Versicherungsvertrages einzuladen. Es handelt sich also nicht um den von der Klägerseite angeführten Fall einer Täuschung über nicht erfragte Umstände. Unerheblich ist in diesem Zusammenhang, ob die über das Onlineportal gestellten Risikofragen im weiteren Verlauf der Vertragsverhandlung und des Abschlusses des

Vertrages auch in Textform gemäß § 126b BGB, wie im Fall des § 19 Abs. 1 VVG gefordert, gestellt worden sind. Eine arglistige Täuschung liegt selbst dann vor, wenn vor dem Vertragsschluss gestellte mündliche Fragen objektiv falsch beantwortet worden sind. Dies gilt damit erst recht, wenn die über ein Onlineportal auf dem Bildschirm sichtbaren Fragen falsch beantwortet werden (OLG Celle VersR 2020, 830; OLG Hamm BeckRS 2019, 37498; Langheid/WandtBußmann Münchener Komm. z. VVG § 22 R. 19; Piontek r+s 2019 S. 1 ff (4)). Anzumerken ist in diesem Zusammenhang jedoch, dass der Zeuge ..., der zum Vertragsschluss und den dortigen Angaben vernommen worden ist von sich auch erklärte, dass er die dortigen Angaben und Erklärungen für sich nochmals ausgedruckt habe, da er noch ein Anhänger der Papierform sei, was gegen die Darstellung der Klägerseite spricht, die gestellten Risikofragen hätten vor Vertragsschluss nicht in Textform im Sinne des § 126b BGB vorgelegen.

31 Jedenfalls die hier gestellten Risikofragen zu Ziffer 3) und 4) wurden bezogen auf den als Speicherplatz genutzten Windows 2003 Rechner, den für den Betrieb des WEB-Shops eingesetzten Windows 2008 SQL-Server und den noch im Auslieferungszustand von 2019 befindlichen Domain-Controller DC09 objektiv falsch beantwortet, so dass dahin gestellt bleiben kann, inwieweit auch weitere Fragen falsch beantwortet worden sind. Die Frage zu 3), ob „alle stationären und mobilen Arbeitsrechner mit aktueller Software zur Erkennung und Vermeidung von Schadsoftware ausgestattet“ sind, wurde mit „ja“ beantwortet. Ebenso wurde die Frage zu Ziffer 4) nach der Durchführung verfügbarer Sicherheitsupdates ohne schuldhaftes Zögern und dem Einsatz von Produkten für die Software für Betriebssysteme, Virenscanner, Firewall, Router, NAS-Systeme usw., für die vom Hersteller Sicherheitsupdates bereitgestellt werden, bejaht. Tatsächlich war unstreitig auf dem Windows 2003 Rechner kein Virenschutzprogramm installiert und Sicherheitsupdates des Herstellers für die Klägerin nicht verfügbar. Das gilt auch für den zum Betrieb des WEB-Shops als Verbindung zum Warenwirtschaftssystem der Klägerin eingesetzten Windows 2008 Rechner. Auch hier war vor dem Vertragsschluss im Januar 2020 das von dem Hersteller bereit gestellte Sicherheitsupdate ausgelaufen. Einen erweiterten Supportvertrag, über den weiterhin Sicherheitsupdates hätten abgerufen werden können, hatte die Klägerin unstreitig für diesen Rechner nicht abgeschlossen. Zudem bestätigte der Zeuge ..., dass, wie sich auch aus der von der Beklagten beauftragten forensischen Analyse durch die Diplom-Informatikerin ... ergibt, der Microsoft Windows 2008 R2 Rechner, der als WEB-SQL Server genutzt worden ist, nicht über einen Virenscanner verfügte. Schließlich befand sich auch der Domaincontroller DC 09 noch im Auslieferungszustand von 2019, dass heißt weder waren Sicherheitsupdates und Aktualisierung erfolgt noch ein Virenschutz installiert. Die Fragen zu Ziffer 3) und 4) sind damit objektiv falsch beantwortet worden.

32 Die Klägerin kann nicht damit gehört werden, dass unter den Begriff des Arbeitsrechners in Frage 3) lediglich die Arbeitsplatzrechner, auf denen ein Virenscanner installiert war, nicht jedoch die im Netzwerk der Klägerin installierten Server, insbesondere nicht der – nach dem Klägervortrag – bei Vertragsschluss in einer demilitarisierten Zone (DMZ) befindliche SQLServer, erfasst sei.

33 Nach ständiger Rechtsprechung des Bundesgerichtshofs ist für die Auslegung von allgemeinen Versicherungsbedingungen wie auch für Erklärungen des Versicherers und damit den hier gestellten Risikofragen auf den durchschnittlichen, um Verständnis bemühten Versicherungsnehmer ohne versicherungsrechtliche Spezialkenntnisse abzustellen. In erster Linie ist bei der Auslegung vom Wortlaut auszugehen. Zudem ist der verfolgte Zweck und der Sinnzusammenhang zu berücksichtigen (BGH Urteil vom 23.06.1993 – IV ZR 135/92). Der Versicherungsnehmer, der eine Cyberversicherung zur Absicherung seines betrieblichen IT-Netzwerkes vor Schäden durch Hackerangriffe oder Ähnlichem absichern möchte, wird hierbei ohne weiteres erkennen, dass die vor dem Versicherungsvertragsschluss erfolgende Risikobewertung durch den Versicherer maßgeblich von verfügbaren Schutzmaßnahmen gegen IT-Angriffe von außen, wie installierten Virenschutzprogrammen und vom Hersteller

bereitgestellten und auch abgerufenen Sicherheitsupdates abhängt. Gerade wenn die in der Verfügungsgewalt des Versicherungsnehmers stehenden Rechner in einem Netzwerk verbunden sind, ist ohne weiteres ersichtlich, dass die Gesamtheit des Netzes nur so sicher sein kann, wie deren schwächsten Glieder. Er wird daher den Begriff des Arbeitsrechners weiter verstehen als den des bloßen Arbeitsplatzrechners und hierunter alle Computersysteme verstehen, die in dem Betrieb Funktionen, sei es als Eingabegerät oder als Server wahrnehmen, weil bereits durch den Zugriff auf einzelne Komponenten mit Malware das gesamte Netzwerk Schaden nehmen kann. Er wird aus der Formulierung in Frage 4), in der nach „durchgeführten“ Sicherheitsupdates gefragt wird, des Weiteren erkennen, dass der Versicherer sich hier nach tatsächlich verfügbaren und von dem Anfragenden genutzte Sicherheitsupdates des Herstellers erkundigt.
34 Die Klägerin kann auch nicht damit gehört werden, dass ein ausreichender Virenschutz über die mit den Windows 2003 verbundenen mobilen Arbeitsplatzrechner gewährt worden sei oder der Windows 2008 SQL Rechner zum Zeitpunkt des Vertragsschlusses sich in einer sogenannten DMZ befunden habe und es sich hierbei nicht um einen Arbeitsrechner handele. Damit blieben weiterhin die im Netzwerk eingebundenen, als Speicherplatz genutzten Server mit dem Windows 2003 Betriebssystem sowie der WEB-SQL-Server mit dem Windows 2008 System ohne aktuellen Virenschutz und Sicherheitsupdates. Sie waren dennoch, wie der Sachverständige ... im Rahmen der Erörterung in der mündlichen Verhandlung erklärte, über die angeschlossenen Arbeitsplatzrechner mit dem Internet verbunden. Die älteren Rechner verfügten über allgemein bekannte Sicherheitsmängel, wie zum Beispiel das aktive SMB1 Protokoll, die von externen Angreifern zur Kompromittierung des gesamten Netzsystems genutzt werden konnten. Es steht der Klägerin als Versicherungsnehmerin nicht zu, an Stelle des Versicherers und ohne dies offen zu legen, die Risikobewertung selbst vorzunehmen. Dies ist vergleichbar mit dem Fall, in dem im Rahmen einer Berufsunfähigkeits- oder Lebensversicherung die Gesundheitsfrage nach einem Bluthochdruck von dem Versicherungsnehmer verneint wird, weil dieser durch die Einnahmen von Medikamenten gut eingestellt ist. Auch wenn daneben weitere Schutzmaßnahmen vor einem Schadangriff getroffen worden sein sollten, bleibt es dabei, dass die Fragen zu Ziffer 3) und 4) objektiv falsch beantwortet worden sind.

35 Der Zeuge ... hat die zu Ziffer 3) und 4) gestellten Fragen ins Blaue hinein unrichtig beantwortet und damit arglistig getäuscht.
36 Die Klägerin 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 Klägerin 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. Das überzeugt die Kammer nicht. Hinsichtlich der Falschbeantwortung der Risikofragen zu 3) und 4) zu den oben genannten Rechnern liegt kein Fall der bloß fahrlässigen Unkenntnis vor, sondern der „bewussten Unkenntnis“ in dem Sinne des „na wenn schon“, was den Tatbestand der arglistigen Täuschung erfüllt.
37 Der Zeuge ... gab im Rahmen seiner Vernehmung an, dass die als Speicherplatz genutzten Rechner mit Windows 2003 Betriebssystem bei Beantwortung der Risikofragen „geflissentlich übersehen“ worden seien. Zu berücksichtigen ist weiter, dass es sich bei den oben genannten drei Rechnersystemen nicht um im Betrieb funktionell untergeordnete Rechner handelte, wie beispielsweise der ebenfalls mit einem Windows 2003 System ausgestattete, nach Angaben des Zeugen ... nicht mehr genutzte, gleichwohl im Netz angeschlossene Fax-Server an dem

Standort .... Vielmehr hatten sowohl die Windows 2003 und 2008 Rechner als auch der Domain Controller 09 entscheidende und zentrale Funktionen im Betrieb der Klägerin, sodass es nicht vorstellbar ist, dass diese Rechner „einfach vergessen“ worden sind. So dienten die Windows 2003 Rechner als zentraler Speicherplatz für Vertragsunterlagen, Rechnungen oder sonstige Dokumente des Unternehmens, waren über die angeschlossenen Arbeitsplatzrechner erreichbar und auf diese Weise mit dem IT-Netz verbunden. Die Rechner wurden, wie es der Zeuge ... angab, als „riesiger USB-Stick“ genutzt.

38 Ebenso hatte der als WEB-SQL-Server genutzte, mit dem Windows 2008 Betriebssystem ausgestattete Rechner, der schließlich das Einfallstor für den Hackerangriff bot, eine zentrale Rolle im Unternehmen der Klägerin. Er diente zum Betrieb des Herzstückes des Unternehmens, nämlich dem Betrieb des WEB-Shops, indem er eine Verbindung zu dem Warenwirtschaftssystem der Klägerin herstellte. Hierdurch erhielt der bestellende Kunde eine Rückmeldung, inwieweit der von ihm angefragte Artikel auf Lager und verfügbar war. Hierbei war man sich im Unternehmen der Klägerin durchaus der Risiken eines Schadangriffes auf diesen Server bewusst, da dieser, nach ihrem Vortrag, durch eine doppelte Firewall abgesichert gewesen sei und sich in einer sogenannten DMZ befunden habe. Es ist nicht vorstellbar, dass dieser so gesondert gesicherte Server bei den ausdrücklich gestellten Risikofragen nach Software zum Erkennen und Vermeiden von Schadsoftware und Sicherheitsupdates von dem Zeugen ... als Leiter der IT-Abteilung einfach vergessen worden ist.

39 Schließlich kam auch dem Domain-Controller DC09 eine zentrale Funktion im Unternehmen zu. Der Domain-Controller, der von der Beklagten als „Schatztruhe mit den Schlüsseln zum Königreich“ bezeichnet worden ist, wurde von dem Zeugen ... weniger poetisch als „Telefonbuch des Unternehmens“ bezeichnet. Die Funktion des Domain-Controller sei so wichtig, wie der Zeuge ... weiter anmerkte, dass im Unternehmen deshalb zwei davon zur Verfügung stünden, da bei einem Ausfall eines Domain-Controllers bei der Klägerin praktisch niemand mehr arbeiten könne. Der Domain-Controller ist ein Server zur zentralen Authentifizierung von Computern und Rechner in einem Rechnernetz, also von zentraler Bedeutung für die Funktionsweise des gesamten, 400 Rechner umfassenden Rechnernetzes der Klägerin.

40 Hinzu kommt, dass, wie der Sachverständige ... im Termin vom 28.02.2024 erläuterte, der Sicherheitszustand des IT-Netzwerkes von dem Zeugen ... vor Beantwortung der Risikofragen relativ leicht durch einen Blick hätte überprüft werden können. So gibt es in der Regel eine zentrale Konsole, über die der Virenschutz verwaltet wird und die nach den Angaben des Sachverständigen eigentlich auch täglich angeschaut werden müsste, um den Sicherheitszustand des IT-Systems zu prüfen. Hierdurch wäre für den Zeugen ... leicht erkennbar gewesen, inwieweit der Virenschutz im Netzwerk vollständig vorliegt und aktualisiert ist und ob hiervon alle Rechner, wie angegeben, erfasst sind. Gleiches gilt für die durchgeführten, vom Hersteller angebotenen Sicherheitsupdates. Diese hätten über das im Betrieb der Klägerin genutzte WSUS-System sofort erfasst werden können und hier wären dann die nicht aktualisierten Windows-Rechner und der Domain-Controller in der Gruppe der Rechner aufgefallen, bei denen kein Update erfolgt war. Eine Kontrolle dieser Systeme hatte der Zeuge ... nach eigenen Angaben nicht vorgenommen, so dass er seine Antworten ins Blaue hinein abgegeben hat. Er hat, jedenfalls nach der ersten Antwort auf die Frage, welche Erkundigungen er vor Beantwortung der Risikofragen eingeholt habe, bekundet, dass er sich heute nicht daran erinnere, bezüglich der Risikofragen Rücksprache mit Herrn ... gehalten zu haben. Er hatte vor Beantwortung der Risikofragen auch keine Systemüberprüfung durchgeführt, obgleich, wie oben geschildert, dies durch einen einfachen Blick möglich gewesen wäre. Die nach seinen Vorgaben dem Mitarbeiter des Maklers, dem Zeugen ..., mitgeteilten Antworten auf die Risikofragen waren danach ungeprüft mitgeteilt worden. Der Zeuge ... hielt es daher jedenfalls für möglich, dass die von ihm auf die Risikofragen der Beklagten abgegebenen Antworten falsch waren. Auch Verhaltensweisen, die auf bedingten

Vorsatz im Sinne eines „Fürmöglichhalten“ reduziert sind, sind von der Arglist im Sinne des § 123 BGB umfasst. Die Kammer ist nach Wertung aller Gesamtumstände zudem davon überzeugt, dass der Zeuge ... es jedenfalls für möglich hielt, dass die Beklagte durch seine Antworten zum Vertragsschluss bestimmt wird und den Vertrag jedenfalls bei der wahrheitsgemäßen Beantwortung der Fragen diesen nicht oder zu anderen Bedingungen geschlossen hätte.

41 Das Verhalten des Zeugen ... muss sich die Klägerin zurechnen lassen. Sie hat sich des Zeugen als Verhandlungsgehilfen bei Abschluss des Versicherungsvertrages bezüglich der Beantwortung der Risikofragen bedient. Er ist daher nicht Dritter im Sinne des § 123 Abs. 2 Satz 1 BGB (Münchener Kommentar Langheid/Wandt/Bußmann VVG § 22 Rn. 37).

42 Schließlich war die Falschbeantwortung der Risikofragen und damit die erfolgte Täuschung auch kausal für den Vertragsschluss. Dies ist bereits dann der Fall, wenn der Vertrag nicht in der erfolgten Weise abgeschlossen worden wäre. Es versteht sich ohne weiteres, dass die Frage der Absicherung des IT-Netzwerkes durch verfügbare Virenscanner oder auch Sicherheitsupdates entscheidend ist für die Frage eines möglichen zukünftigen Schadenseintritts und damit geeignet ist, die Entscheidung der Beklagten zur Übernahme dieses Risikos und zum Abschluss des Versicherungsvertrages zu beeinflussen. Jedenfalls auf die Höhe der zu entrichtenden Prämie hat die Beantwortung der Risikofragen, wie sich aus der eingereichten Anlage WH 11 unmittelbar ergibt, Einfluss. Der Eindeckungsprozess erfolgt danach in einzelnen Schritten, wie sie in der Anlage WH 11 anhand von Screenshots dargestellt ist. Nach der Eingabe allgemeiner Unternehmensdaten und der Auswahl des Versicherungsschutzes wird zunächst eine sogenannte Indikationsprämie, also eine vorläufige Prämie angegeben. Dann erfolgt unter Schritt 5 die Beantwortung der im Tatbestand dargestellten Risikofragen, indem der Anfragende die neben den Fragen befindlichen Button entweder bei ja oder nein festlegen kann. Im Anschluss erfolgt unter Schritt 6 eine neue Prämienübersicht, in der nun die endgültig ausgewiesene individuelle Prämie angegeben wird.

43 Damit steht fest, dass jedenfalls die Höhe der Versicherungsprämie durch die Falschbeantwortung der Risikofragen beeinflusst wird.

44 Nach alledem ist der Versicherungsvertrag aufgrund der begründeten Anfechtung des Vertrages wegen arglistiger Täuschung nichtig. Die Beklagte ist zur Erbringung der vereinbarten Versicherungsleistungen nicht verpflichtet. Angesichts der arglistigen Täuschung kommt es auf die Regelung in der Anerkenntnisklausel in der Sondervereinbarung der ... nicht an. Die Klage ist daher insgesamt, das heißt auch bezüglich des geltend gemachten Feststellungsantrages und der als Nebenforderungen beantragten vorgerichtlichen Rechtsanwaltskosten abzuweisen.

45 Die prozessualen Nebenentscheidungen folgen aus den §§ 91 Abs. 1, 269 Abs. 3, 709 ZPO. Die Klägerin hat den mit der Klageerweiterung vom 05.02.2024 (Bl. 342 d. A.) gestellten Zahlungsantrag in Höhe von dort noch 687.952,23 € im Termin vom 28.02.2024 teilweise zurückgenommen, indem dort nur noch ein Zahlbetrag in Höhe von 424.985,52 € beantragt worden ist