Landgericht Hagen, 9 O 258/23

Datum:	15.10.2024
Gericht:	Landgericht Hagen
Spruchkörper:	9. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	9 O 258/23
ECLI:	ECLI:DE:LGHA:2024:1015.9O258.23.00

Tenor:

Die Klage wird abgewiesen.

Die Kosten des Rechtsstreits trägt die Klägerin.

Das Urteil ist gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand: 1

Die Klägerin macht gegen die Beklagte einen Ersatzanspruch aus einem Cyber-Versicherungsvertrag geltend. 2

Zwischen den Parteien besteht unter der Versicherungsschein-Nr. H. eine Cyber-Versicherung. Die Versicherung wurde zum 11.05.2020 abgeschlossen mit einer ursprünglichen Versicherungsdauer bis zum 01.01.2022 und stillschweigend jährlich verlängert. Der Versicherung liegen die Allgemeinen Versicherungsbedingungen für die Versicherung von Cyber-Risiken, Stand: 4.2019 (im Folgenden „AVB“) zugrunde. Der Versicherungsumfang erstreckt sich auch auf den Versicherungsschutz für den Baustein „Cyber-Vertrauensschäden“ im Sinne von Teil D der AVB. Nach Umfirmierung der Klägerin wurde ein entsprechender Nachtrag zum Versicherungsschein gefertigt (Anlage K2). 3

Die Versicherungsbedingungen regeln in Teil A auszugsweise: 4

3. Informationssicherheitsverletzung 5

Informationssicherheitsverletzungen im Sinne dieser Bedingungen sind: 6

3.1. Verletzung datenschutzrechtlicher Bestimmungen 7

8

Nach der Datenschutz-Grundverordnung (DS-GVO), dem Bundesdatenschutzgesetz (BDSG) oder anderen Regelungen zum Datenschutz unzulässige oder unrichtige Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten Dritter durch Versicherte; dies gilt auch bei Verletzungen vergleichbarer ausländischer Rechtsnormen.

3.2. Vertraulichkeitsverletzung 9

Verletzungen der Vertraulichkeit Daten Dritter durch den Versicherungsnehmer, die sich im Verfügungsbereich des Versicherungsnehmers befinden. Dazu gehören insbesondere Betriebs- und Geschäftsgeheimnisse Dritter. 10

3.3. Netzwerksicherheitsverletzungen 11

Netzwerke im Sinne dieser Vertragsbedingungen sind Telekommunikations-, Daten- und Rechnernetzwerke des Versicherungsnehmers. Netzwerksicherheitsverletzungen sind Beeinträchtigungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des Versicherungsnehmers. 12

[…] 13

4. Versicherungsfall und Serienschäden 14

Versicherungsschutz besteht für alle im Zeitraum zwischen Versicherungsbeginn und Versicherungsende vom Versicherungsnehmer entdeckten Informationssicherheitsverletzungen. Die Informationssicherheitsverletzung gilt mit dem Zeitpunkt der ersten nachprüfbaren Feststellung durch den Versicherungsnehmer als entdeckt (Versicherungsfall). 15

Unter Teil A 3.3.1. der AVB sind zudem positive und negative Beispiele für Netzwerksicherheitsverletzungen aufgeführt. Im Übrigen wird wegen der Einzelheiten und des Inhalts des Versicherungsscheins und der Versicherungsbedingungen auf die Anlagen K1 – K3 (Bl. 13 ff. d.A.) Bezug genommen. 16

Die Klägerin steht in einer regelmäßigen Geschäftsbeziehung zu einem polnischen Lieferanten, der Fa. Y. Sp.z.o.o (Lieferant). Mit dem Lieferanten kommunizierte die Klägerin in der Regel per E-Mail. Kontaktperson der Klägerin bei dem Lieferanten war Herr G. F.. Per E-Mail wurde mit diesem unter anderem die Bezahlung offener Rechnungsbeträge besprochen. Herr F. verwendete die E-Mailadresse *R..pl*. Zum Jahreswechsel 2022/2023 hatte die Klägerin gegenüber dem Lieferanten aufgrund erfolgter Lieferungen Rechnungen im unteren sechsstelligen Bereich zu begleichen. 17

Am 25.01.2023 erhielt die Klägerin eine E-Mail, mit welcher der vermeintliche Lieferant eine geplante Änderung seiner Bankmitteilung kommunizierte und dies damit begründete, dass die Kontoführungsgebühren der üblichen Bankverbindung zu hoch seien. Dabei verwendete der Absender die E-Mail-Adresse *L..plR..pl*. Der Domänenteil des Lieferanten "@L..pl." wurde weiterhin verwendet. Die Signatur des Lieferanten und der Name „G. F." wurden ebenfalls weiterhin verwendet. 18

Später wurde die Klägerin erneut über diese E-Mail kontaktiert und erörterte - wie aus der Kommunikation mit der Lieferantin gewohnt - Bestellungen und offene Rechnungen. Insbesondere wurden der Klägerin, wie am 25.01.2023 angekündigt, neue Bankdaten mitgeteilt. Zahlungen der Klägerin an die Lieferantin sollten danach auf das Konto IBAN N02, X., N03 S., W. erfolgen. 19

Auf Grund dieser Nachricht änderte die Klägerin die bei ihr für den Lieferanten hinterlegten Kontodaten. Die nun folgenden Rechnungen über insgesamt 85.000,00 € zahlte die Klägerin mit insgesamt vier Überweisungen auf das ihr neu mitgeteilte Bankkonto bei der X. in W.. 20

Die Zahlungen an das fremde Konto setzten sich wie folgt zusammen: 21

Datum	Betrag
09.02.2023	15.000,00 €
13.02.2023	40.000,00 €
16.02.2023	10.000,00 €
27.02.2023	20.000,00 €
	85.000,00 €

22

Im Nachhinein stellte sich heraus, dass diese E-Mails nicht von dem eigentlichen Lieferanten kamen, sondern Fälschungen waren und auch das Konto, auf welches die Zahlungen geflossen sind, kein Konto des Lieferanten war. 23

Anfang März hatten der Lieferant und die Klägerin telefonisch Kontakt. In diesem Zusammenhang wies der Lieferant darauf hin, trotz weiterhin offener Rechnungspositionen keine Zahlungen der Klägerin erhalten zu haben und erklärte auch, seine Bankverbindung nicht geändert zu haben. Die Klägerin übersandte sodann den vorausgegangenen E-Mail-Verkehr samt der Überweisungsträger an den Lieferanten per WhatsApp zur weitergehenden Erläuterung. 24

Die Klägerin erstatte ferner unter dem 02.03.2023 Strafanzeige. Zudem nahm die Klägerin am 02.03.2023 Kontakt mit der J. auf, um eine Rücküberweisung des Geldtransfers zu erreichen. Die Rücküberweisung des von dort überwiesenen und umgeleiteten Betrages in Höhe von 20.000,00 € war jedoch nicht mehr möglich. Außerdem setzte sich die Klägerin am 02.03.2023 mit der D., Essen in Verbindung und stellte dort unter Erläuterung des Sachverhaltes einen telefonischen Antrag auf Rücküberweisung des von dort überwiesenen Betrages in Höhe von 20.000,00 €. Auch diesem Kreditinstitut war die Rückbuchung nicht möglich. 25

Anschließend meldete die Klägerin den Schaden am 02.03.2023 der Beklagten. Die Beklagte führte den Sachverhalt sodann unter der Schadennummer N04. 26

Der Vorfall wurde im Auftrag der Klägerin durch die K. GmbH geprüft. Die K. GmbH kam in ihrer abschließenden Stellungnahme dazu, dass der Exchange Server des Lieferanten der Klägerin vermutlich „gehackt" worden sei, da die betrügerische Mail vom Exchange Server des Kunden verschickt worden sei. 27

Die Beklagte lehnte mit E-Mail vom 07.03.2023 die Regulierung des Schadens ab. Daraufhin wandten sich die jetzigen Prozessbevollmächtigten der Klägerin an die Beklagte und forderten diese unter dem 25.05.2023 erfolglos zur Schadensregulierung auf 28

29

Die Klägerin ist der Ansicht, der Eingriff des Schädigers in den laufenden E-Mailverkehr und den über ein Online-Banking-System abgewickelten Zahlungsverkehr zwischen ihr und ihrem Lieferanten sei ein Eingriff in ihr Telekommunikationsnetzwerk. Ihr Telekommunikationsnetzwerk sei deshalb „gehackt“ worden. Auch ist sie der Ansicht, es läge kein Angriff mittels nachgebildeter E-Mail-Adresse vor. Denn der Dritte habe keine E-Mail-Adresse nachgebildet, sondern das E-Mail-Postfach des Lieferanten direkt verwendet. Schließlich meint sie, die AVB seien als allgemeine Geschäftsbedingungen zu überprüfen und nach einer Inhaltskontrolle unwirksam.

Die Klägerin beantragt, 30

die Beklagte zu verurteilen, an sie 85.000,00 € nebst Zinsen in Höhe von 9 % über dem jeweiligen Basiszinssatz seit dem 07.03.2023 zu zahlen sowie sie von den vorgerichtlichen Anwaltskosten in Höhe von 2.049,30 € freizustellen. 31

Die Beklagte beantragt, 32

die Klage abzuweisen. 33

Sie ist der Auffassung, die Netzwerke und Computersysteme der Klägerin seien weder angegriffen noch technisch kompromittiert worden. Vielmehr mache die Klägerin mit ihrer Klage einen reinen Täuschungsschaden geltend. Der Erhalt einer betrügerischen Phishing-E-Mail reiche nicht aus, um den Versicherungsschutz unter der abgeschlossenen Cyberversicherung auszulösen. Der Angriff auf den E-Mail-Account des Lieferanten führe nicht dazu, dass auch das Telekommunikationsnetz der Klägerin selbst „gehackt“ worden sei. 34

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze nebst deren Anlagen Bezug genommen. 35

Entscheidungsgründe: 36

Die zulässige Klage ist unbegründet. 37

I. 38

Die Klägerin hat keinen Anspruch auf Zahlung in Höhe von 85.000,00 € gegen die Beklagte aus dem zwischen den Parteien bestehenden Versicherungsvertrag über eine Cyber-Versicherung in Verbindung mit § 1 VVG. 39

1. 40

Es liegt kein Versicherungsfall vor, weil es an einer Informationssicherheitsverletzung im Sinne des Teil A Ziff. 4 der AVB fehlt. Weder liegt eine Verletzung datenschutzrechtlicher Bestimmungen (Teil A Ziffer 3.1 AVB) noch eine Vertraulichkeitsverletzung (Teil A Ziffer 3.2 AVB) noch eine Netzwerksicherheitsverletzung (Teil A Ziffer 3.3 AVB) vor. 41

a) 42

Eine Verletzung datenschutzrechtlicher Bestimmungen liegt schon deshalb nicht vor, weil die Klägerin als Versicherungsnehmerin keinen Verstoß gegen datenschutzrechtliche Bestimmungen begangen hat. 43

44

Für eine Vertraulichkeitsverletzung im Sinne der AVB fehlt es an einer Verletzung der Vertraulichkeit Daten Dritter durch die Klägerin.

b) 45

Auch eine Netzwerksicherheitsverletzung liegt nicht vor. Dies ergibt die Auslegung der zugrundeliegenden AVB, hier Teil A Ziffer 3.3. der AVB. 46

Allgemeine Versicherungsbedingungen sind so auszulegen, wie ein durchschnittlicher, um Verständnis bemühter Versicherungsnehmer sie bei verständiger Würdigung, aufmerksamer Durchsicht und unter Berücksichtigung des erkennbaren Sinnzusammenhangs versteht. Dabei kommt es auf die Verständnismöglichkeiten eines Versicherungsnehmers ohne versicherungsrechtliche Spezialkenntnisse und damit auch auf seine Interessen an. In erster Linie ist vom Bedingungswortlaut auszugehen. Der mit dem Bedingungswerk verfolgte Zweck und der Sinnzusammenhang der Klauseln sind zusätzlich zu berücksichtigen, soweit sie für den Versicherungsnehmer erkennbar sind (BGH r+s 2020, 163 Rn. 9, beck-online m.w.N.). 47

Ein solcher Versicherungsnehmer wird die entsprechende Klausel dahin verstehen, dass es zu einer Verletzung der Sicherheit des Netzwerkes der Klägerin gekommen sein muss und eine derartige Verletzung bei dem Empfang von E-Mails, die von einem anderen als dem in den E-Mails angegebenen Absender stammen, nicht gegeben ist. Allein der Umstand, dass aufgrund der unautorisierten Verwendung des E-Mail Exchange Servers des Lieferanten möglicherweise eine nicht zu erkennende Täuschung vorgelegen hat, stellt keinen direkten Angriff auf die Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme der Klägerin dar. Die informationstechnischen Systeme – auch das E-Mail System der Klägerin – und letztlich auch das Netzwerk der Klägerin funktionierten wie vorgesehen. Mails konnten auf normale Weise und unverändert empfangen und gesendet werden. Betroffen von dem Cyber-Angriff war lediglich ein Netzwerk eines Dritten. 48

Berücksichtigt werden müssen bei einer Auslegung der Versicherungsbedingungen weiterhin die – nicht abschließenden – Regelbeispiele aus Teil A Ziff. 3.3.1., in denen es auszugsweise heißt: 49

Keine Netzwerksicherheitsverletzung liegt vor, wenn 50

(3) Beeinträchtigungen der oben genannten Art in Netzwerken Dritter stattfinden, die Auswirkungen jedoch auch beim Versicherungsnehmer auftreten (z. B. man-in-the-middle Angriff bei Zulieferer); 51

(4) kein Eingriff in das Netzwerk des Versicherungsnehmers stattgefunden hat (z. B. fake president Angriffe mittels nachgebildeter E-Mail-Adresse). 52

Aus diesen Regelbeispielen kann ein durchschnittlicher und verständiger Versicherungsnehmer erkennen, dass der vorliegende Fall, der zu den eben genannten Regelbeispielen Ähnlichkeiten aufweist, nicht zu den versicherten Risiken zählt. Voraussetzung des Versicherungsschutzes bleibt eine Netzwerksicherheitsverletzung bei dem Versicherungsnehmer selbst, die nicht vorliegt. Beeinträchtigungen bei Dritten sind keine Netzwerksicherheitsverletzung bei der Klägerin. In Abgrenzung zu einem Cyber-Angriff handelt es sich im vorliegenden Fall einer dem „normalen“ Betrug nahen Tat. 53

Auch im Übrigen ist dieses Verständnis der AVB sachgerecht. Denn im vorliegenden Fall ist die Klägerin auf eine betrügerische E-Mail hereingefallen. Dieses Risiko ist heute 54

allgegenwärtig und nichts, was notwendigerweise durch eine Cyber-Versicherung abzusichern wäre. Andernfalls wäre jedweder E-Mail-Verkehr mit Spam- oder Phishing-Mails eine Netzwerksicherheitsverletzung bei dem Versicherungsnehmer. Das versicherte Risiko würde sich auf den weltweiten E-Mail-Verkehr ausweiten.

c) 55

Auch liegt kein Versicherungsfall nach der Vertrauensschadenversicherung nach Teil D. Ziff. 1 AVB vor. Der Versicherungsfall ist ergänzend in der Vertrauensschadenversicherung zunächst unter Teil D. Ziff.1 wie folgt definiert: 56

Versicherungsschutz besteht für den Versicherungsnehmer wegen eines Versicherungsfalles im Sinne von Teil A Ziffer 4, wenn die Informationssicherheitsverletzung vorsätzlich und rechtswidrig erfolgte und nach den gesetzlichen Bestimmungen über unerlaubte Handlungen zum Schadenersatz verpflichtet und der Versicherungsnehmer unmittelbar dadurch einen Vermögensschaden erleidet. Es ist dabei unerheblich, ob die Informationssicherheitsverletzung von Mitarbeitern des Versicherungsnehmers oder von Dritten erfolgte. 57

Weiterhin besteht Versicherungsschutz auch für einen eingetretenen „Täuschungsschaden“ (Teil D. Ziff. 1.2.): 58

Versicherungsschutz besteht für den mittelbar entstandenen Vermögensschaden, wenn ein Mitarbeiter des Versicherungsnehmers auf Grund einer Informationssicherheitsverletzung gemäß Teil A Ziffer 3, welche einen Straftatbestand im Sinne des Strafgesetzbuches erfüllt, dazu verleitet wurde, Zahlungen / Überweisungen zu veranlassen. 59

Zwar umfasst der Versicherungsschutz des Teil D der AVB dem Wortlaut und auch dem Sinn und Zweck nach betrügerische Handlungen die das Vertrauen des Versicherungsnehmers ausnutzen. Die Vertrauensschadenversicherung bietet – je nach Ausgestaltung – gerade auch Versicherungsschutz für vorsätzliche Eingriffe in informationsverarbeitende Systeme des Versicherungsnehmers, durch eine Vertrauensperson oder Dritte, und dadurch unmittelbar verursachte Schäden (Schilbach, r+s 2024, 581 Rn. 49, beck-online). 60

Da allerdings immer auch eine Informationssicherheitsverletzung erforderlich ist, ist der Anwendungsbereich der Vertrauensschadenversicherung nicht eröffnet. 61

2. 62

Entgegen der Auffassung der Klägerin sind die streitgegenständlichen AVB in den relevanten Auszügen nicht gem. § 307 BGB unwirksam. 63

a) 64

Zum einen stellen sowohl Teil A. Ziff. 4 AVB, als auch Teil D Ziff. 1.2 Leistungsbeschreibungen des versicherten Risikos dar und unterliegen gem. § 307 Abs. 3 S. 1 BGB nicht der Inhaltskontrolle im Hinblick auf das Kriterium der unangemessenen Benachteiligung. Die Formulierungen in Teil A Ziff. 3 und Teil D Ziff. 1 AVB stellen keine Einschränkungen des zuvor festgelegten Versicherungsumfangs dar, sondern legen erst die vom Versicherer geschuldete Leistung fest (vgl. auch BGH NJW 2023, 208). 65

b) 66

67

Die Leistungsbeschreibungen verstoßen auch nicht gegen das – sich gem. § 307 Abs. 3 S. 2 BGB auch auf das Hauptleistungsversprechen erstreckende (vgl. BGH VersR 2014, 625) – Transparenzgebot des § 307 Abs. 1 S. 2 BGB.

aa) 68

Nach dem Transparenzgebot ist der Verwender allgemeiner Geschäftsbedingungen gehalten, Rechte und Pflichten seines Vertragspartners möglichst klar und durchschaubar darzustellen. Dabei kommt es nicht nur darauf an, dass die Klausel in ihrer Formulierung für den durchschnittlichen Versicherungsnehmer verständlich ist. Vielmehr gebieten Treu und Glauben, dass die Klausel die wirtschaftlichen Nachteile und Belastungen soweit erkennen lässt, wie dies nach den Umständen gefordert werden kann. Dem Versicherungsnehmer soll bereits im Zeitpunkt des Vertragsschlusses vor Augen geführt werden, in welchem Umfang er Versicherungsschutz erlangt und welche Umstände seinen Versicherungsschutz gefährden. Nur dann kann er die Entscheidung treffen, ob er den angebotenen Versicherungsschutz nimmt oder nicht (vgl. BGH NJW 2023, 208). Maßgebend sind die Verständnismöglichkeiten des typischerweise bei Verträgen der geregelten Art zu erwartenden Durchschnittskunden. Insoweit gilt kein anderer Maßstab als derjenige, der auch bei der Auslegung von Versicherungsbedingungen zu beachten ist (BGH aaO.). 69

bb) 70

Nach diesen Grundsätzen sind die Leistungsbeschreibungen der AVB nicht intransparent. Denn für eine Cyber-Versicherung ist typisch und für den Durchschnittskunden erkennbar, dass nur das Risiko der eigenen IT-Systeme geschützt werden soll und nicht weltweite Hacker-Angriffe, die in mittelbarer Weise Auswirkungen gegenüber dem Versicherungsnehmer haben können. Andernfalls wäre bereits die Teilnahme am E-Mail-Verkehr an sich ein großes Risiko, da niemand vor – auch gut gefälschten – Phishing Mails geschützt ist. Die Versicherungsbedingungen sind insoweit klar und verständlich formuliert, dass im Rahmen der Netzwerksicherheitsverletzung gerade eine Beeinträchtigung der eigenen Netzwerke vorliegen muss. 71

II. 72

Die Zinsforderung und der Anspruch auf Erstattung der vorgerichtlichen Anwaltskosten teilen das Schicksal der Hauptforderung und bestehen nicht. 73

III. 74

Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit hat ihre Rechtsgrundlage in § 709 S. 1, S. 2 ZPO. 75

IV. 76

Der Streitwert wird auf 85.000,00 € festgesetzt. 77

P.	M.	C.

78

Verkündet am 15.10.2024 79

V., Justizbeschäftigte 80


Justiz NRW
Rechtsprechungsdatenbank ONLINE