49. Jahrgang
datenschutz-berater.de
DSB 03/2025

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Prof. Dr. Ronald Petrlic und Johannes Zwerschke

OLG Schleswig: Ende-zu-Ende-Verschlüsselung ist nach der DSGVO im Geschäftsverkehr regelmäßig erforderlich

OLG Schleswig, Urt. v. 18.12.2024 – 12 U 9/24

Die Gerichtsentscheidung in Kürze

Das schleswig-holsteinische Oberlandesgericht entschied, dass die Zahlung einer wegen eines Hackerangriffs manipulierten Rechnung auf ein fremdes Konto keine Erfüllung der Werklohnforderung darstellt. Die irrtümlich zahlende Kundin könne jedoch wegen des dolo-agit-Einwands nach § 242 BGB einen Schadensersatzanspruch gegen das Unternehmen aus Art. 82 DSGVO geltend machen, wenn dieses den Versand der Rechnung per E-Mail nicht ausreichend abgesichert hat. Das Gericht betonte, dass eine bloße Transportverschlüsselung bei geschäftlichen E-Mails mit personenbezogenen Daten nicht ausreicht. Vielmehr sei eine Ende-zu-Ende-Verschlüsselung notwendig, um ein angemessenes Schutzniveau zu gewährleisten. Zudem treffe die Kundin auch kein Mitverschulden, da es ihr nicht zuzumuten sei, die Feinheiten einer manipulierten Rechnung zu entdecken.

Der Fall

Die Klägerin, ein Werkunternehmer, stellte der Beklagten, einer privaten Kundin, eine Schlussrechnung über 15.385,78 EUR per E-Mail zu. Diese Rechnung wurde durch einen unbekannten Dritten manipuliert, sodass die Beklagte den Betrag auf ein falsches Konto überwies. Streitig blieb dabei, ob die Manipulation der Rechnung aufgrund eines Hacks eines E-Mail-Kontos schon bei der Klägerin oder aber erst auf dem Versandweg an die Beklagte erfolgte. Die Klägerin forderte daraufhin die Zahlung des Werklohns erneut. Die Beklagte berief sich darauf, dass sie die Rechnung wie erhalten beglichen habe, und machte geltend, dass die Manipulation im Verantwortungsbereich der Klägerin liege.

Bewertung des Urteils aus rechtlicher Perspektive

Das Berufungsgericht hat sich zunächst mit der Frage befasst, ob durch die Zahlung des Werklohns auf das Konto des unbekannten Dritten eine Erfüllungswirkung i. S. v. § 362 Abs. 2 BGB eingetreten ist. Dies wird vom OLG Schleswig deshalb abgelehnt, weil die Leistung an einen Dritten gemäß §§ 362 Abs. 2, 185 BGB nur dann erfüllende Wirkung entfalten könne, wenn der nicht empfangsbefugte Dritte die Leistung entsprechend den Weisungen des Schuldners an den Gläubiger weiterleitet oder der Gläubiger die Leistungserbringung an den Dritten ausdrücklich oder schlüssig genehmigt, was beides hier nicht der Fall ist. Es sei demnach also keine Erfüllung eingetreten.

In einem weiteren Schritt urteilt das Gericht aber, dass der Beklagten, die wegen der manipulierten Rechnung auf das Konto eines unberechtigten Dritten überwiesen hatte, gegen den Kläger gemäß § 242 BGB (dolo-agit-Einwand) ein Anspruch auf Schadensersatz in Höhe der geltend gemachten Forderung zustehe. Dem Grunde nach stützt das OLG Schleswig diesen Schadensersatzanspruch auf Art. 82 Abs. 1 DSGVO, obwohl sich die Beklagte nach den Urteilsgründen nicht einmal ausdrücklich auf Art. 82 Abs. 1 DSGVO berufen zu haben scheint.

Im streitgegenständlichen Fall leitet das Gericht den Verstoß aus den Art. 5, 24 und 32 DSGVO her. Denn es sei von der Klägerin (bestritten) lediglich eine Transportverschlüsselung verwendet worden und sie habe es versäumt, nachzuweisen, dass diese tatbestandlich hinreichend geeignet sei. Dies könne aber nach Meinung des Gerichts schon deshalb dahinstehen bleiben, weil eine Transportverschlüsselung hier nicht geeignet sei, um die Anforderungen nach Art. 32 DSGVO zu erfüllen. Dabei erkennt das Gericht an, dass die DSGVO keine harten Vorgaben zur Verschlüsselung macht und eine solche nicht einmal zwingend vorgeschrieben ist. Deshalb stützt sich das Gericht für seine weitere Argumentation auf die Einschätzungen der Datenschutzkonferenz und des Bundesamtes für Sicherheit in der Informationstechnik (siehe unter Rn. 75 und 79 ff. des Urteils). Für die Frage der geeigneten Verschlüsselung stellt das Gericht zunächst darauf ab, dass ein verschlüsselungsloser E-Mail-Versand nicht möglich sei. Es erwähnt in diesem Zusammenhang auch die vorstehend genannten behördlichen Einschätzungen. Das Gericht schlussfolgert weiter aus den genannten Behördeneinschätzungen, dass eine Transportverschlüsselung für E-Mails ebenfalls nicht geeignet sei, um die Anforderungen insbesondere aus Art. 32 Abs. 1 DSGVO zu gewährleisten. Denn beim Versand von geschäftlichen E-Mails mit personenbezogenen Daten zwischen Unternehmer und Kunden drohe ein hohes finanzielles Risiko durch Verfälschung der angehängten Rechnung. Das Gericht stellt dabei auf die allgemeine Bekanntheit und hohe Schadensträchtigkeit von Hackerangriffen ab. Dass ein solcher Angriff bei der Klägerin in der Vergangenheit bisher nicht vorkam, ist für das Gericht nicht maßgeblich. Trotz der Tatsache, dass in dem Rechtsstreit streitig ist, ob der Hackerangriff in den IT-Systemen der Klägerin stattfand, könnte dies darauf hinweisen, dass das Gericht von einem Hackerangriff in den Systemen der Klägerin ausgeht. Ebenso lässt das Ge-

richt den Einwand der Klägerin nicht gelten, dass die Implementierung einer Ende-zu-Ende-Verschlüsselung mit (finanziellen) Aufwänden verbunden sei und dass die Verwendung einer solchen Verschlüsselung (nach Darstellung der Klägerin) im Geschäftsverkehr unüblich sei. Das Gericht geht im Rahmen der Verschuldensvermutung (Art. 82 Abs. 3 DSGVO) sogar so weit, dass selbst die Empfehlung eines IT-Beraters für die Verwendung einer Transportverschlüsselung unbeachtlich sei, da es Sache der Klägerin sei, zu entscheiden, welche Verschlüsselung letztlich verwendet wird. „Gekrönt" wird die Entscheidung dadurch, dass auch kein Mitverschulden gemäß § 254 BGB zulasten der Beklagten anzunehmen sei. Denn es sei ihr nicht zuzumuten, geringfügige Änderungen der manipulierten Rechnung zu entdecken.

Rechtliche Schlussfolgerungen aus dem Urteil

Die hiesige Entscheidung stellt aus rechtlicher Sicht einen starken Kontrast zur Entscheidung des OLG Karlsruhe (Urt. v. 27.7.2023 – 19 U 83/22) dar, da sie den Verschuldensschwerpunkt im Fall von manipulierten Rechnungen und den daraus resultierenden Schäden eher beim Versender als beim Empfänger verortet. Gleichwohl gilt es zu beachten, dass das OLG Karlsruhe den Schwerpunkt seiner Entscheidung anders als das OLG Schleswig nicht auf Fragen zur DSGVO gelegt hat. Beiden vorgenannten Entscheidungen dürfte dennoch gemein sein, dass der vollständige Verzicht auf die Verwendung irgendeiner E-Mail-Verschlüsselung immer schwerer zu vertreten ist (in diese Richtung auch VG Mainz, Urt. v. 17.12.2020 – 1 K 778/19.MZ; a. A. LG Rostock, Urt. v. 20.11.2024 – 2 O 450/24, Rn. 19, das bemerkenswerterweise und unter Verweis auf das vorstehend zitierte Urteil des OLG Karlsruhe die Existenz jeglicher (gesetzlicher) Vorgaben für Sicherheitsvorkehrungen beim E-Mail-Versand ablehnt.).

Die Erwägungen des OLG Schleswig sind teils kritisch zu bewerten. So konstatierte das Gericht ein hohes finanzielles Risiko. Hier ging es um einen Betrag von ca. 15.000 EUR. Daraus stellt sich allerdings die Frage, ob beim Versand von E-Mails mit kleinen Rechnungen (z. B. 100 EUR) ein kleines tatbestandliches Risiko vorläge und in der Folge dann eine Transportverschlüsselung ausreichen würde. Bemerkenswert ist in diesem Zusammenhang zudem, dass das Gericht zuerst auf das Risiko der Verfälschung angehängter Rechnungen abstellt, dann aber die Gefahr von Hackerangriffen auf Unternehmen zugrunde legt. Unklar bleibt also, ob das tatbestandliche Risiko nach Art. 32 Abs. 1 DSGVO im Risiko der Veränderbarkeit von „nur" transportverschlüsselten E-Mails im Rahmen des Versands liegt oder aber darin, dass Unternehmen mit hoher Wahrscheinlichkeit gehackt werden und hieraus das Risiko der Veränderung von E-Mails sowie ein finanzieller Schaden resultiert.

Würde man darauf abstellen, dass sich das Risiko hier aufgrund des Hacks der IT-Infrastruktur der Klägerin realisiert hat, was nach dem Urteil ungeklärt bleibt, so könnte der E-Mail-Empfänger zudem Schadensersatzansprüche aus § 19 Abs. 4 TDDDG geltend machen. Denn der Versender von E-Mails ist auch zum Schutz der von ihm betriebenen E-Mail-Infrastruktur verpflichtet. Bemerkenswerterweise wurde § 19 Abs. 4 TDDDG in vergleichbaren Verfahren bisher nicht näher thematisiert (am Rande unter Bezug auf die Vorgängernorm, § 13 Abs. 7 TMG: OLG Frankfurt a. M., Urt. v. 6.12.2023 – 3 U 3/23, Rn. 29).

Aus dem Vorstehenden ergibt sich außerdem die Frage, ob Rechnungen per E-Mail versendende Verantwortliche mit ihren empfangenden betroffenen Personen eine Absenkung des Schutzniveaus vereinbaren dürfen. Denn im Schadensfall könnte sich der Versender im Zweifel auf die Absenkung des Schutzniveaus berufen und so dem Empfänger ggf. ein Mitverschulden zuweisen. Die in der Rechtsprechung und bei den Aufsichtsbehörden wohl vorherrschende Ansicht bejaht die Möglichkeit der Absenkung des Schutzniveaus von Art. 32 DSGVO (OLG Düsseldorf, Urt. v. 28.10.2021 – 16 U 275/20, Rn. 55 ff.; SG Hamburg, Urt. v. 30.6.2023, Rn. 94 ff.; Datenschutzkonferenz, Beschl. v. 24.11.2021).

Für die rechtliche Bewertung stellt sich schließlich in faktischer Hinsicht die Frage, ob der Empfänger überhaupt dazu in der Lage wäre, eine Ende-zu-Ende-verschlüsselte E-Mail zu empfangen. Denn nicht zuletzt unter diesem Aspekt dürfte die Frage im Rahmen des Mitverschuldens nach § 254 BGB zu diskutieren sein, ob der E-Mail-Empfänger überhaupt in der Lage ist, E-Mails dergestalt verschlüsselt zu empfangen.

Neben diesen rein datenschutzrechtlichen Aspekten dürften aber auch eher zivilrechtliche Fragen im Rahmen der hiesigen Problematik zum Tragen kommen. Denn gemäß § 130 Abs. 1 Satz 1 BGB wird eine Willenserklärung in dem Zeitpunkt wirksam, in dem sie einem anderen zugeht. Eine Rechnung, die per E-Mail versandt wird, ist als rechtsgeschäftsähnliche Erklärung und damit als Willenserklärung zu qualifizieren. Daraus folgt, dass der Absender der Willenserklärung sämtliche Verfälschungen zu vertreten hat, die bis zum Zugang beim Empfänger eintreten. Der BGH hat sich zwar bereits mit dem Zugang von E-Mails als Willenserklärungen auseinandergesetzt (Urt. v. 6.10.2022 – VII ZR 895/21). Ersichtlich wurde die Frage der Verfälschung vor Zugang im Fall von E-Mails mit Blick auf § 130 BGB in der Rechtsprechung aber bisher noch nicht entschieden.

Bewertung des Urteils aus technischer Perspektive

Im rechtlichen Abschnitt wurde bereits die Frage aufgeworfen, ob der Empfänger überhaupt dazu in der Lage wä-

re, eine Ende-zu-Ende-verschlüsselte E-Mail zu empfangen. Aus technischer Sicht lässt sich hierzu sagen, dass mit S/MIME und PGP zwar Verfahren zur E-Mail-Verschlüsselung existieren, diese in der Praxis – gerade bei Endkunden – allerdings so gut wie nicht zur Anwendung kommen. Die wenigsten Nutzer sind in der Lage, Ende-zu-Ende-verschlüsselte E-Mails zu empfangen, da sie weder über die nötige Software verfügen noch die entsprechenden Schlüssel vorab generiert haben. Im geschäftlichen Umfeld ist S/MIME eher üblich als PGP, wodurch S/MIME in der B2B-Kommunikation in einigen Fällen zur Anwendung kommt. In einer Studie (Stransky, et al.: „27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University", 2022 IEEE Symposium on Security and Privacy) aus dem Jahr 2022 kommen Forscher aus Deutschland, die mehr als 87 Millionen E-Mails von mehr als 37.000 Nutzern einer großen Universität (mit über 30.000 Studenten und 5.000 Mitarbeitern) über einen Zeitraum von 27 Jahren analysiert haben, zu dem Schluss, dass lediglich 0,06 % aller E-Mails Ende-zu-Ende-verschlüsselt waren (und 2,8 % signiert), wobei S/MIME 6-mal so häufig verwendet wurde wie PGP. Hierzu sei noch anzumerken, dass an deutschen Universitäten kostenfreie S/MIME-Zertifikate für Nutzer bereitgestellt werden, wodurch die Nutzung eher noch häufiger ist als in der "normalen Praxis", in der solche Zertifikate kostenpflichtig sind. Aus dem Urteil geht nicht hervor, ob die Beklagte überhaupt in der Lage war, Ende-zu-Ende-verschlüsselte E-Mails in Empfang zu nehmen. Aus der Praxiserfahrung heraus ist es als höchst unwahrscheinlich einzuschätzen, dass dies der Fall war. Falls dies doch der Fall gewesen ist, hätte die Beklagte ihren öffentlichen Schlüssel (bzw. ihr E-Mail-Zertifikat) vorab der Klägerin zukommen lassen müssen, damit diese in die Lage versetzt worden wäre, ihr Ende-zu-Ende-verschlüsselte E-Mails zu senden.

Ein weiterer spannender Aspekt aus technischer Sicht bezieht sich auf die Art der Transportverschlüsselung. In dem Urteil werden hierzu bedauerlicherweise keine Details genannt – wie dies auch schon im Urteil vom VG Mainz (Urteil vom 17.12.2020, 1 K 778/19.MZ) aus dem Jahr 2020 der Fall war (siehe auch Petrlic, DSB 2021, 88). Neben der in der Praxis typischerweise vorherrschenden opportunistischen Transportverschlüsselung gibt es noch die obligatorische Transportverschlüsselung, sowie die in der Orientierungshilfe genannte "qualifizierte" Transportverschlüsselung, bei der es sich aus technischer Sicht um die Verwendung von DANE handelt. Aus der Orientierungshilfe geht hervor, dass beim Versand von E-Mails mit hohem Risiko „regelmäßig" eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung zu nutzen sind. Behördenvertreter haben allerdings bestätigt, dass anstatt einer Ende-zu-Ende-Verschlüsselung in vielen Fällen auch eine qualifizierte Transportverschlüsselung ausreichend ist – was aus technischer Sicht sehr sinnvoll ist. Darüber hinaus muss darauf hingewiesen werden, dass nach der Orientierungshilfe auch Empfänger von E-Mails mit hohem Risiko Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung anbieten müssen. Leider geht aus dem Urteil nicht hervor, ob die Beklagte Maßnahmen ergriffen hat (d. h. insbesondere DANE auf dem Mail-Server eingerichtet hat), damit eine qualifizierte Transportverschlüsselung ermöglicht wurde. Sollte dies der Fall gewesen sein, so wäre eine zusätzliche Ende-zu-Ende-Verschlüsselung selbst aus Sicht der strengen Vorgaben der Datenschutzaufsichtsbehörden gar nicht nötig gewesen, da ein "Aufbrechen" der Transportverschlüsselung durch einen Angreifer aufgrund der Nutzung von DANE als äußert unwahrscheinlich betrachtet werden kann. Eine Studie des Co-Autors dieses Beitrags zeigt allerdings, dass qualifizierte Transportverschlüsselungen in der Praxis bedauerlicherweise zu selten genutzt werden. In einer Studie (Lange, et al.: "An Email a Day Could Give Your Health Data Away", DPM 2022) werden seit dem Jahr 2022 jeden Monat rund 4.000 Gesundheitseinrichtungen in Deutschland auf die Einhaltung der Vorgaben aus der Orientierungshilfe hin geprüft. Lediglich bei 1 % der untersuchten E-Mail-Server der Verantwortlichen kommt DANE zum Einsatz. Die Ergebnisse der monatlichen Untersuchung können unter https://mail-sicherheit.jetzt/test-der-e-mail-server-deutscher-gesundheitseinrichtungen/ abgerufen werden.

Aus technischer Sicht ist es äußerst unwahrscheinlich, dass die Rechnung in der E-Mail tatsächlich auf dem Transportweg manipuliert wurde. Laut Zahlen von Google (https://transparencyreport.google.com/safer-email/overview?hl=en) werden – Stand Februar 2025 – weltweit 99 % aller E-Mails von und zu Google Mail (Gmail) transportverschlüsselt übermittelt. Selbst wenn es sich dabei „nur" um die opportunistische Transportverschlüsselung handelt, würde ein derartiger Angriff ein gewisses Maß an Aufwand erzeugen. Aus der Praxis sind (abgesehen von in einer Studie (Durumeric, et al.: „Neither Snow Nor Rain Nor MITM…: An Empirical Analysis of Email Delivery Security", IMC 15) aus dem Jahr 2015 aufgezeigten systematischen Angriffen auf die Transportverschlüsselung in Ländern wie Tunesien) dem Co-Autor keine Fälle bekannt, bei dem Angriffe dadurch stattgefunden haben, dass die Transportverschlüsselung „aufgebrochen" wurde. Vielmehr werden in den meisten Fällen die E-Mail-Konten der Nutzer „gehackt", was einen deutlich geringeren Aufwand darstellt, da hierfür in den meisten Fällen lediglich schwache Passwörter erraten werden müssen bzw. im Rahmen von Phishing-Angriffen diese Passwörter (leicht) erbeutet werden können. Auch wenn hierzu keine Details aus dem Urteil hervorgehen, ist die Übernahme eines E-Mail-Kontos – sei es aufseiten der Klägerin bzw. aufseiten der Beklagten – als viel wahrscheinlicher anzusehen. Eine Ende-zu-Ende-Verschlüsselung hätte hier also mit großer Wahrscheinlichkeit keine Wirkung erzielt.

Ein weiterer Schwachpunkt des Urteils aus technischer Sicht ist darin zu sehen, dass das Gericht durch die Forderung von Ende-zu-Ende-Verschlüsselung auf das Schutzziel „Vertraulichkeit“ abstellt. Vielmehr geht es in dem Fall allerdings um die Schutzziele „Integrität“ und „Authentizität“ – und diese werden eben nicht durch die Nutzung einer Ende-zu-Ende-Verschlüsselung gewährleistet (siehe hierzu auch Petrlic, DuD 2017, 41), sondern durch die Nutzung einer digitalen Signatur. Konsequenterweise hätte das Gericht anstatt der Ende-zu-Ende-Verschlüsselung eine digitale Signatur der E-Mail (mit S/MIME) durch die Klägerin einfordern müssen.

Zuletzt entschied das Gericht noch: „Soweit dieser zu erwartende hohe Standard zum Schutz der personenbezogenen Daten beim Versand von Emails mit angehängten Rechnungen nicht sichergestellt werden kann, bleibt für ein Unternehmen – ohne dass hierfür größerer technischer und/oder finanzieller Aufwand betrieben werden müsste – wie eh und je der Versand von Rechnungen per Post das Mittel der Wahl.“ Dies ist weder wünschenswert – vor allem auch im Hinblick auf die E-Rechnung, noch wäre ausgeschlossen, dass falsche Rechnungen auf dem Postweg versandt werden könnten. Unternehmensgründer machen die Erfahrung, dass der erste Brief nach der Gründung eine Fake-Rechnung enthält, die zur Zahlung von vermeintlichen Gebühren an das Handelsregister auffordert.

Handlungsanweisung für die Praxis/Fazit

Zusammenfassend lässt sich festhalten, dass das Urteil des OLG Schleswig aus rechtlicher und technischer Sicht als äußerst problematisch anzusehen ist und die potenziellen Konsequenzen in Bezug auf die E-Mail-Kommunikation enorm sind. Noch ist unklar, ob das Urteil Bestand haben wird oder ob eine der Parteien des Rechtsstreits in Revision geht.

Auch wenn man zu dem Schluss kommt, dass eine Ende-zu-Ende-Verschlüsselung in diesem Fall (und ähnlich gelagerten Fällen in der Praxis) nicht zwingend notwendig ist, so sollten sich Verantwortliche – spätestens nach diesem Urteil – trotzdem mit dem Thema E-Mail-Sicherheit auseinandersetzen. Es gibt Alternativen zur Ende-zu-Ende-Verschlüsselung – diese müssen nur konsequent umgesetzt und gut dokumentiert werden.

Autoren:

Prof. Dr. Ronald Petrlic ist Professor für Informationssicherheit an der TH Nürnberg und Geschäftsführer der Petrlic Consulting GmbH.

Johannes Zwerschke ist Rechtsanwalt bei der Kanzlei Piltz Legal in Berlin und spezialisiert im Fachgebiet Datenschutz- und IT- und IT-Sicherheitsrecht.