Dr. Martin Bahr

Bei Rechnungsversand von E-Mails Ende-zu-Ende-Verschlüsselung Pflicht?

Ein aktuelles Urteil des Oberlandesgerichts Schleswig (OLG Schleswig) sorgt derzeit für erhebliche Unsicherheit bei Unternehmen, die ihre Rechnungen per E-Mail versenden. Nach der Entscheidung des Gerichts ist nicht nur eine Transportverschlüsselung, sondern auch eine Ende-zu-Ende-Verschlüsselung erforderlich. Ist dies nicht der Fall, stellt dies einen Datenschutzverstoß dar, der den Empfänger der Nachricht zu Schadensersatz in Höhe des Rechnungsbetrags verpflichtet.
Der aktuelle Artikel stellt dieses Urteil vor, beleuchtet zwei weitere Entscheidungen und ordnet ein, wie sich Unternehmen in Zukunft am besten verhalten sollten.

1. Der Ursprung des Problems: Urteil des OLG Schleswig

Hintergrund ist eine Entscheidung des OLG Schleswig von Ende Dezember 2024. [1]

Das klagende Unternehmen installierte bei dem verklagten Verbraucher eine Heizungsanlage. Die Schlussrechnung wurde dem Kunden per E-Mail übermittelt, wobei lediglich eine Transportverschlüsselung verwendet wurde.

Unbemerkt von beiden Parteien manipulierten Dritte die E-Mail und änderten die Bankverbindung, sodass der Beklagte den Rechnungsbetrag in Höhe von 15.000 Euro auf ein Konto der Betrüger überwies.

Als die Klägerin später die Zahlung verlangte, verweigerte der Kunde die Zahlung.

Diese Auffassung hat das OLG Schleswig nun in seinem Urteil bestätigt.

Die Beklagte schulde der Klägerin daher keine weitere Zahlung.

Zwar sei die ursprüngliche Zahlungspflicht durch die Überweisung auf das falsche Konto nicht erfüllt worden, da keine Anweisung zur Zahlung an einen Dritten vorgelegen habe.

Dem Kunden stehe jedoch ein Schadensersatzanspruch nach der Datenschutz-Grundverordnung (DSGVO) zu, den er der Forderung entgegenhalten könne.

Das klagende Unternehmen hätte beim Versand sensibler Daten – wie einer Rechnung mit Kundendaten – höhere Schutzmaßnahmen ergreifen müssen. Die eingesetzte Transportverschlüsselung war nicht ausreichend, erforderlich wäre eine Ende-zu-Ende-Verschlüsselung gewesen, um Manipulationen auszuschließen.

Da das Unternehmen gegen die datenschutzrechtliche Pflicht zum Schutz personenbezogener Daten verstoßen habe, müsse es für den entstandenen Schaden einstehen.

DER AUTOR

Die **Kanzlei Dr. Bahr** (www.Dr-Bahr.com) ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter Suchmaschinen-und-Recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

[1] OLG Schleswig, Urt. v. 18.12.2024 – Az.: 12 U 9/24.

> "Nach Ansicht des Senats ist danach eine reine Transportverschlüsselung beim Versand von geschäftlichen Emails mit personenbezogenen Daten zwischen Unternehmer und Kunden jedenfalls bei dem hier bestehenden hohen finanziellen Risiko durch Verfälschung der angehängten Rechnung der Klägerin für den Kunden nicht ausreichend und kann keinen „geeigneten" Schutz im Sinne der DSGVO darstellen. Vielmehr ist die End-to-End-Verschlüsselung zurzeit das Mittel der Wahl."

Auch der Umstand, dass die letzte E-Mail in Gestaltung und Farbgebung von den vorherigen abweiche, begründe kein Mitverschulden des Beklagten, so die Richter.

> „Anders als das Landgericht meint, oblag der Beklagten bzw. dem Zeugen A., dessen Verschulden ihr möglicherweise gem. § 278 BGB zuzurechnen wäre, nach Ansicht des Senats keine genaue Überprüfung der letztlich auf dem Computer des Zeugen verfälscht, da hinsichtlich der Kontoverbindung manipuliert vorliegenden Rechnung. Die von der Klägerin aufgezeigten Unterschiede zu früheren (Abschlags-)Rechnungen betreffend die Farbe, Angaben zum Geschäftsführer, fehlenden QR-Code der Bankverbindung und fehlendes Siegel stellen geringfügige äußere Abweichungen dar, die weder der Beklagten noch dem Zeugen A. bei oberflächlicher Betrachtung auffallen mussten.
> Etwas anderes folgt auch nicht daraus, dass die Beklagte erkannt hat, dass die Kontoverbindung verändert war. Angesichts der Tatsache, dass im Geschäftsleben die Kontoverbindung eines Unternehmens aus diversen Gründen geändert wird, kann einer privaten Kundin wie der Beklagten nicht vorgeworfen werden, dass sie vor der Überweisung des offenen Werklohns keine Rücksprache mit der Klägerin genommen hat."

Die Auffassung des OLG Schleswig hat zu erheblicher Verwirrung und Unsicherheit bei den Unternehmen geführt. Es ist daher wichtig, die Entscheidung in den Gesamtkontext der bisherigen Rechtsprechung einzuordnen.

Deutlich weniger Aufmerksamkeit haben zwei sehr ähnliche Entscheidungen aus den Jahren 2023 und 2024 gefunden. Sie wurden in der bisherigen Diskussion kaum wahrgenommen.

2. OLG Karlsruhe: Kein SFP-Eintrag bei Rechnungsversand per E-Mail

An erster Stelle ist hier die Entscheidung des OLG Karlsruhe aus dem Jahr 2023 zu nennen. [2]

Die Karlsruher Richter kamen zu dem Ergebnis, dass Unternehmen rechtlich nicht verpflichtet sind, einen SPF-Eintrag (Sender Policy Framework) zu verwenden.

Dem Rechtsstreit lag folgender Fall zugrunde: Die Klägerin verlangte von der Beklagten die Zahlung des Kaufpreises für einen Gebrauchtwagen. Beide Parteien handelten als Unternehmer.

Nach Vertragsschluss erhielt die Beklagte eine E-Mail mit einer Bankverbindung, auf die sie den Kaufpreis überwies.

Später stellte sich heraus, dass ein Dritter, der sich unbefugt Zugang verschafft hatte, die Nachricht versandt und die Kontodaten manipuliert hatte. Die Zahlung erfolgte daher auf ein Konto, das nicht der Klägerin gehörte.

Die Klägerin hielt an ihrer Forderung fest und verlangte die Zahlung des Kaufpreises. Die Beklagte verteidigte sich mit dem Einwand, bereits Zahlung geleistet zu haben.

Das OLG gab der Klägerin Recht.

> „Es liegt keine Nebenpflichtverletzung der Klägerin dergestalt vor, dass sie schuldhaft eine Ursache dafür gesetzt hätte (...). Für den dadurch verursachten Schaden, der darin besteht, dass die Beklagte durch Überweisung auf ein nicht der Klägerin zugeordnetes Konto die Forderung der Klägerin nicht zum Erlöschen bringen konnte (...), schuldet die Klägerin der Beklagten deshalb keinen Schadensersatz."

Die Beklagte argumentierte, die Klägerin habe gegen die erforderlichen technischen Schutzmaßnahmen verstoßen, da sie keinen SPF-Eintrag für ihre E-Mail-Konten eingerichtet habe.

> „Die Beklagte behauptet, es sei zum Versand (...) der (...) E-Mail an sie durch einen Dritten dadurch gekommen, dass auf das E-Mail-Konto der Klägerin eine Hacking-Attacke ausgeführt worden sei, die das Ausspionieren der Geschäftsbeziehung der Parteien und der Rechnungs-E-Mail ermöglicht habe.
> Dies sei durch mangelnde Vorsichtsmaßnahmen der Klägerin ermöglicht worden, wofür ein Anscheinsbeweis spreche; konkret nennt die Beklagte insoweit die nicht erfolgte Verwendung des ‚sender policy framework (SPF)' bei der Kommunikation sowie eine unterlassene Verschlüsselung der pdf-Datei."

Die Richter erteilten diesem Standpunkt jedoch eine klare Absage:

[2] OLG Karlsruhe, Urt. v. 27.07.2023 – Az.: 19 U 83/22.

> „Konkrete gesetzliche Vorgaben für Sicherheitsvorkehrungen beim Versand von E-Mails im geschäftlichen Verkehr gibt es nicht; insbesondere ist der sachliche Anwendungsbereich der Datenschutz-Grundverordnung im Streitfall nicht eröffnet, da diese nur für die Verarbeitung von Informationen gilt, die sich auf eine natürliche Person beziehen (...).
> Selbst wenn man in einem der vorstehend behandelten Umstände eine Pflichtverletzung der Klägerin sehen wollte, fehlte es am Nachweis der Kausalität dieser Pflichtverletzung für den eingetretenen Schaden."

3. LG Rostock: Zahlungspflichtiger trägt Risiko bei Fehlüberweisung durch Phishing-Mail Zahlungspflichtiger

Der zweite Fall betrifft eine Entscheidung des LG Rostock. [3]

Die Klägerin, ein Bauunternehmen, hatte mit der Beklagten, ebenfalls einem Bauunternehmen, einen Vertrag über Maler- und Trockenbauarbeiten geschlossen. Im Laufe der Arbeiten stellte die Klägerin der Beklagten Abschlagsrechnungen aus. Eine dieser Rechnungen belief sich auf knapp 38.000 Euro und wurde der Beklagten ordnungsgemäß übermittelt.

Kurze Zeit später erhielt die Beklagte eine weitere E-Mail mit einer nahezu identischen Rechnung, die jedoch eine andere Bankverbindung enthielt. Die Umstände ließen darauf schließen, dass diese Nachricht von Dritten manipuliert worden war.

Die Beklagte überwies daraufhin den Rechnungsbetrag auf das falsche Konto.

Als die Klägerin die Zahlung anmahnte, verweigerte die Beklagte die Zahlung mit der Begründung, sie habe die Forderung bereits beglichen.

Zu Unrecht, so die Richter. Die Zahlungspflicht sei nicht erloschen:

> „Gegen die Verletzung einer Schutzpflicht spricht vorliegend schon die Überlegung, dass es dem beiderseitigen Parteiwillen entsprochen haben dürfte, für die Kommunikation zur Abwicklung des Vertrages E-Mails zu benutzen.
> Dass E-Mails ein unsicherer Übertragungsweg und anfällig für externe Angriffe sind, ist seit Jahren allgemein bekannt. Wird E-Mail-Verkehr zwischen den Parteien genutzt, existieren grundsätzlich keine Vorgaben für Sicherheitsvorkehrungen insoweit.
> Zudem ist fraglich, ob es überhaupt in der Macht der Klägerin stand, ihr System weiter abzusichern und selbst, wenn das möglich gewesen sein sollte, ob nicht gleichwohl ein Angriff durch etwa Abfangen der E-Mail hätte erfolgreich durchgeführt werden können."

4. Resümee: Was gilt nun? Zahlungspflichtiger

Auf den ersten Blick scheinen sich die drei genannten Entscheidungen zu widersprechen. Auf der einen Seite steht die Auffassung des OLG Schleswig, auf der anderen die des OLG Karlsruhe und des LG Rostock.

Bei näherer Betrachtung zeigt sich jedoch ein wichtiger Unterschied: Im Fall des OLG Schleswig ging es um eine Rechnung an einen Verbraucher (B2C), während die beiden anderen Urteile Rechnungen an Unternehmer (B2B) betrafen.

Das bedeutet: Auch nach Auffassung des OLG Schleswig besteht keine Pflicht zur Ende-zu-Ende-Verschlüsselung, wenn der Rechnungsempfänger ein Unternehmer ist.

Aber auch für die Konstellation, dass der Kunde ein Verbraucher ist, kann die Entscheidung des OLG Schleswig nur als absolutes Fehlurteil bezeichnet werden. Sie ist in mehrfacher Hinsicht geradezu grotesk und völlig unverständlich.

Die Forderung, dass Rechnungen ab einer Größenordnung von ca. 15.000 Euro zwingend nicht nur transport-, sondern auch inhaltsverschlüsselt übermittelt werden müssen, ist realitätsfern und in der Praxis kaum umsetzbar.

Man muss sich fragen: Wie soll das im täglichen Geschäftsverkehr, insbesondere mit Verbrauchern, funktionieren?

Seien wir ehrlich: Die überwiegende Mehrheit der Verbraucher verfügt weder über das notwendige technische Wissen noch über die erforderliche Infrastruktur, um inhaltsverschlüsselte E-Mails problemlos entschlüsseln und verarbeiten zu können. Verschlüsselungsverfahren wie PGP oder S/MIME sind für die Masse der Endnutzer schlicht nicht praktikabel. Derartige Forderungen mögen zwar theoretisch denkbar sein, entbehren aber jeglicher Realitätsnähe.

Die Absurdität der gerichtlichen Argumentation wird noch deutlicher, wenn man den Sachverhalt auf ein anderes Medium überträgt. Wäre die Rechnung klassisch per Post versandt und unterwegs von einem Dritten geöffnet und manipuliert worden? Würde dann ernsthaft jemand auf die Idee kommen, das versendende Unternehmen für diese Manipulation haftbar zu machen? Eine solche Forderung wäre abwegig und würde vom gesunden Menschenverstand sofort zurückgewiesen. Warum soll dann für eine E-Mail ein anderer Maßstab gelten?

Hinzu kommt, dass sich das Gericht unreflektiert auf die DSGVO beruft. Selbst wenn man eine Pflichtverletzung unterstellt, fehlt es offensichtlich an

einem adäquaten Kausalzusammenhang zwischen einer etwaigen Verletzung datenschutzrechtlicher Pflichten und dem eingetretenen Schaden. Die Anforderungen der DSGVO dürfen nicht so weit überdehnt werden, dass sie zu einer pauschalen Haftung für kriminelle Handlungen Dritter führen.

Besonders unverständlich und lebensfremd ist zudem, dass das Gericht dem Empfänger der manipulierten E-Mail nicht einmal ein Mitverschulden anlastet. Ihm hätte auffallen müssen, dass die betrügerische Nachricht in Gestaltung, Aufbau und äußeren Merkmalen deutlich von den bisherigen Rechnungen abweicht. Gerade bei Rechnungen über erhebliche Beträge wäre eine erhöhte Aufmerksamkeit des Empfängers zu erwarten gewesen.

Insgesamt offenbart die Entscheidung des Gerichts eine eklatante Loslösung von den tatsächlichen Gegebenheiten des elektronischen Geschäftsverkehrs. Die hier aufgestellten Anforderungen sind weder praxistauglich noch rechtlich überzeugend. Sie verlagern das Risiko einseitig auf den Absender, ohne der berechtigten Eigenverantwortung des Empfängers auch nur ansatzweise Rechnung zu tragen.

5. Ergebnis:

Für den **B2B-Bereich** ist das OLG Schleswig nicht relevant, d. h., Sie können weiterhin Rechnungen ohne inhaltliche Verschlüsselung per E-Mail versenden.

Versenden Sie hingegen elektronische Rechnungen im B2C-Bereich, empfehlen wir Ihnen Folgendes:

Wenn Sie rechtlich zu 100 % auf der sicheren Seite sein wollen, prüfen Sie, ob Sie ohne größeren Aufwand auf eine andere Versandform umstellen können, zum Beispiel indem Sie die Rechnung in einem Log-in-Bereich Ihrer Website zur Verfügung stellen und nicht per E-Mail versenden. Dies wird in der Regel nicht ohne größeren Aufwand möglich sein (Programmierung der Webseite, Kunde muss sich extra einloggen etc.).

Wenn ein gewisses rechtliches Restrisiko für Sie akzeptabel ist, ignorieren Sie das Urteil einfach und versenden Sie Ihre Rechnungen weiterhin wie bisher. Wie gesagt, wir halten das Urteil des OLG Schleswig für ein absolutes Fehlurteil. Aber so ist die Welt.

Wenn Sie eine differenzierte Vorgehensweise bevorzugen und das Risiko von Einnahmeverlusten reduzieren wollen, können Sie auch eine gesplittete Vorgehensweise wählen. Bis zu einem Betrag X, dessen Ausfall Sie im Zweifelsfall für vertretbar halten, versenden Sie die Rechnung weiterhin per E-Mail. Bei höheren Beträgen, deren Ausfall für Sie wirtschaftlich schmerzhaft wäre, wählen Sie eine andere Versandform, zum Beispiel per Brief. ¶

Herausgeber & Chefredakteur (verantwortlich):
Mario Fischer
E-Mail: redaktion@websiteboosting.com

Autoren dieser Ausgabe:
Tobias Aubele, Dr. Martin Bahr, Felix Beilharz, Dr. Torsten Beyer, Stephan Czysch, Wolfgang Jung, Beatrice Köhler, Hanns Kronenberg, Markus Laue, Matthäus Michalik, Rebecca Schwarz, Eico Schweins, Hendrik Unger, Sarah Weitnauer, Theresa Zanker

Anzeigenleitung:
Markus Lutz
E-Mail: anzeigenleitung@websiteboosting.com

Art Direction, Layout/Produktion:
Kai Neugebauer

Lektorat:
Bärbel Philipp, textperlen.de

Fotos & Illustrationen:
Website Boosting / GettyImages

Druck:
Schleunungdruck GmbH, Eltertstraße 27
97828 Marktheidenfeld

Vertrieb:
PressUp GmbH, Postfach 70 13 11
22013 Hamburg
E-Mail: websiteboosting@pressup.de

Abonnement:
Website Boosting Aboservice
PressUp GmbH, Postfach 70 13 11
22013 Hamburg
Tel. 040 / 38 6666 – 342
E-Mail: websiteboosting@pressup.de

Erscheinungsweise: 6 x jährlich
Bezugspreis: Einzelheft: 11,80€
Bezugspreis Inland jährlich 62,00€ inkl. Versand
Bezugspreis Ausland jährlich 70,80€ inkl. Versand

Studenten im Inland erhalten gegen Vorlage einer Immatrikulationsbescheinigung einen Preisvorteil – Details finden Sie auf der Website.

Verlagsleitung:
Michael Müßig
Tel: +49 931 / 26 038 04,
verlag@websiteboosting.com

Anschrift des Verlages
Hotspot Verlag GmbH
Obere Landwehr 4a, 97204 Höchberg
Tel: + 49 931 / 26 038 04
E-Mail: verlag@hotspotverlag.de
www.hotspotverlag.de

Geschäftsführung:
Kai Neugebauer

ISSN: 2191-6241