Kommunikation & Recht

K&R
9 | September 2023
26. Jahrgang
Seiten 553 - 632

www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

13 500 EUR wegen der Verletzung von IT-Sicherheitspflichten verhilft ihrer Rechtsverteidigung ebenfalls nicht zum Erfolg. Ein entsprechender Schadensersatzanspruch der Klägerin besteht nicht, auf die vorstehenden Ausführungen unter 2. wird zur Vermeidung von Wiederholungen Bezug genommen.

5. Die Klägerin hat gem. § 280 Abs. 2, § 286 BGB einen Anspruch auf Erstattung vorgerichtlicher Rechtsanwaltskosten in Höhe von 953,40 EUR entsprechend einer 1,3-Gebühr gem. Nr. 2300 VV RVG aus einem Gegenstandswert von 13 500 EUR zuzüglich Auslagenpauschale. Sie hat – von der Beklagten unbestritten – vorgetragen, dass deren Geschäftsführer am 19. 10. 2021 die Zahlung des Kaufpreises abgelehnt hat, so dass die Beklagte gem. § 286 Abs. 2 Nr. 3 BGB in Verzug geraten ist. […]

Nils Wiedemann und Prof. Dr. Christoph Sorge*

Kommentar

I. Das Problem

Die Entscheidung des OLG Karlsruhe behandelt die Frage, welche Sicherheitsvorkehrungen beim Versand von E-Mails im Geschäftsverkehr vom Empfänger berechtigterweise erwartet werden dürfen.

II. Die Entscheidung

Die Käuferin eines Gebrauchtwagens hatte per E-Mail zunächst die korrekte, kurz darauf aber von der gleichen Absenderadresse eine durch einen Dritten veränderte Rechnung erhalten. Sie überwies den Kaufpreis daraufhin auf das in der zweiten E-Mail angegebene Konto des Dritten. Auch andere Kunden waren betroffen. Die Verkäuferin klagte auf „nochmalige“ Zahlung; die Käuferin machte geltend, dass die Klägerin unzureichende Sicherheitsvorkehrungen für den E-Mail-Versand getroffen habe. Das LG Mosbach nahm eine Erfüllung gemäß § 362 BGB an und wies die Klage ab. Das OLG Karlsruhe hob die Entscheidung auf und verurteilte die Beklagte zur Zahlung des Kaufpreises. Aus dem Vortrag ergebe sich keine Pflichtverletzung der Klägerin.

III. Bewertung

Die konkrete Ausgestaltung der Leitsätze des Urteils des OLG Karlsruhe überzeugen, das Ergebnis und die Begründung sind teils zu kritisieren.

1. OH der DSK und Anwendbarkeit DSGVO

Die vom LG herangezogene Orientierungshilfe der DSK (OH)[1] definiert u. a. Anforderungen an die verwendeten Verfahren der Transportverschlüsselung. Nach dem OLG ist die OH hier aber nicht maßgeblich, da die DSGVO sachlich nicht anwendbar sei. Diese Ansicht überzeugt nicht. Mangels einer weitergehenden Begründung kann nur angenommen werden, dass das OLG fälschlicherweise davon ausgeht, weil es sich bei den Parteien um juristische Personen handelt. Ein Personenbezug ist jedoch bereits zu bejahen, wenn eine natürliche Person indirekt identifiziert werden kann, etwa weil Angaben zu einer juristischen Person sich indirekt auf eine natürliche Person beziehen. Es erscheint auch im Geschäftsverkehr fernliegend, dass E-Mails keine personenbezogenen Daten (wie etwa Namen) enthalten. Die DSGVO ist dann anwendbar, die OH dürfte grundsätzlich herangezogen werden.

2. Transportverschlüsselung

E-Mails werden üblicherweise vom Computer des Absenders zunächst an einen E-Mail-Server bei seinem Provider und von dort an den für die Domain des Empfängers zuständigen E-Mail-Server übermittelt, wo der Empfänger sie schließlich abruft. Es finden folglich mindestens drei einzelne Übertragungen der E-Mail statt. Diese können jeweils verschlüsselt sein; ein Großteil der E-Mail-Server unterstützt eine solche Transportverschlüsselung.[2]

Transportverschlüsselung kann opportunistisch oder obligatorisch ausgestaltet sein. Bei einer obligatorischen Transportverschlüsselung wird die E-Mail nur versendet, wenn sie verschlüsselt übertragen werden kann.[3] Die OH sieht eine solche Verschlüsselung beim E-Mail-Versand von personenbezogenen Daten vor, wenn der Bruch der Vertraulichkeit ein Risiko für natürliche Personen darstellen kann. Diese Anforderungen der OH an eine Transportverschlüsselung sind aus technischer Sicht auch sinnvoll und erfordern lediglich die Umsetzung etablierter technischer Standards sowie explizit den Verzicht auf die Unterstützung älterer Verfahren mit geringerem Sicherheitsniveau. Allerdings werden diese Anforderungen in der Praxis von vielen E-Mail-Servern nicht erfüllt.[4] Das VG Mainz entschied kürzlich, dass beim E-Mail-Versand von personenbezogenen Daten auch bei Berufsgeheimnisträgern die Verwendung einer „(obligatorischen) Transportverschlüsselung“ datenschutzrechtlich ausreichend ist, sofern nicht aufgrund besonderer Umstände ein erhöhter Schutzbedarf besteht.[5] Jedoch ließ das VG Mainz offen, welche Art von Transportverschlüsselung in der Praxis erforderlich ist.[6]

Letztlich wird dies auch durch das OLG nicht beantwortet. So lehnt es bereits aufgrund des fehlenden Vortrags der Beklagten eine Pflichtverletzung ab und geht nicht weiter darauf ein, ob die vom Anbieter der Klägerin verwendete Transportverschlüsselung ausreichend war. Anders als beim VG Mainz ist in einem Zwei-Personen-Verhältnis die Unterscheidung, ob opportunistische oder obligatorische Transportverschlüsselung verwendet wurde, nicht von Belang, da – wie das OLG zutreffend feststellt – der Empfänger eine solche ermöglichen müsste. Daher wäre im Geschäftsverkehr grundsätzlich nur eine Pflichtverletzung gegeben, wenn der Absender eine veraltete oder überhaupt keine Transportverschlüsselung verwendet.

Eine Transportverschlüsselung schützt jedoch nicht die Echtheit der Absenderangabe (Authentizität) einer E-Mail, sondern nur die Vertraulichkeit der Kommunikationsinhalte. Grundsätzlich kann jeder Absender einer E-Mail die angegebene Absenderadresse frei wählen. Deshalb wird das Fehlen einer Transportverschlüsselung nur kausal für einen entstandenen Schaden sein, wenn der Angriff gerade durch ein Abfangen der Kommunikation ermöglicht wurde.

---

* Mehr über die Autoren erfahren Sie am Ende des Kommentars.

1 DSK, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Stand: 13. 3. 2020.

2 *Tatang/Flume/Holz*, DIMVA 2021, 368.

3 *Petrlic*, DSB 2021, 88, 89.

4 *Wambach*, INFORMATIK 2022, S. 628, 632.

5 VG Mainz, 17. 12. 2020 – 1 K 778/19.MZ.

6 *Petrlic*, DSB 2021, 88, 90.

3. Ende-zu-Ende-Verschlüsselung der E-Mail oder PDF-Datei

Verschlüsselung schützt grundsätzlich nur die Vertraulichkeit des Inhalts, nicht die Authentizität. Dies gilt sowohl für Ende-zu-Ende-verschlüsselte E-Mails als auch für die Verschlüsselung von (PDF-)Dateien. Sowohl der Absender als auch der Empfänger müssen das entsprechende Verfahren[7] verwenden. Das OLG stellt zutreffend fest, dass sich eine Ende-zu-Ende-Verschlüsselung beim Versand von E-Mails in der Praxis bislang nicht durchgesetzt hat und deshalb auch im Geschäftsverkehr nicht ohne weiteres vom Absender erwartet werden kann. Auch die OH sieht eine solche nur im Falle eines hohen Risikos bei der Übermittlung personenbezogener Daten per E-Mail vor. Zuzustimmen ist dem OLG, dass der Versand von verschlüsselten PDF-Dateien außerhalb eines Austauschs besonders sensibler Daten vom Absender in der Praxis üblicherweise nicht erwartet werden kann, sofern nicht eine entsprechende Vereinbarung getroffen wurde.

4. SPF und DKIM

Das „Sender Policy Frameworks (SPF)“[8] oder auch „DomainKeys Identified Mail (DKIM)“[9] sind – technisch unterschiedliche – Verfahren, die dem Empfänger einer Nachricht die Prüfung ermöglichen, ob der vom Absender verwendete E-Mail-Server zum Versand von E-Mails für die verwendete Domain autorisiert ist. Ist er es nicht, kann die E-Mail etwa als Spam markiert oder verworfen werden. Zutreffend ist, dass Kunden eines Anbieters grundsätzlich keinen Einfluss darauf haben, ob für die Domain des Anbieters ein solches Verfahren verwendet wird. Allerdings können die Kunden durch die Auswahl eines Anbieters, der ein solches Verfahren anbietet, durchaus beeinflussen, ob für ihren geschäftlichen Verkehr ein solches Verfahren angewendet wird. Untersuchungen zeigen, dass ca. 65 % der Top500-Domains aus 139 Ländern im Jahr 2021 SPF verwenden.[10] Auch hier ist aber erforderlich, dass der Empfänger per Konfiguration oder Auswahl des Anbieters die Verwendung von Verfahren wie SPF dem Absender ermöglicht.

Allerdings können weder SPF noch DKIM einen Schutz gewähren, wenn ein Angreifer, z. B. aufgrund eines erratenen Passworts, Zugriff auf den E-Mail-Server des Absenders erhält. Welcher Server für den E-Mail-Versand genutzt wurde, lässt sich mit wenig Aufwand durch einen Blick in die Kopfzeilen (Header) der E-Mail verifizieren. Sollte dies der E-Mail-Server des vorgeblichen Absenders (oder seines Diensteanbieters) sein, liegt es nahe, die Ursache für das Sicherheitsproblem in der Sphäre des vorgeblichen Absenders zu suchen. In einem solchen Fall wäre – selbst wenn der Nichtgebrauch von SPF eine Pflichtverletzung des Absenders darstellt – diese wohl nicht kausal für den Schaden, da dieser auch bei Verwendung der Verfahren eintreten könnte.

5. Digitale Signaturen

Die zuverlässigste – aber im Urteil nicht behandelte – Möglichkeit zum Schutz der Authentizität und Integrität einer Nachricht wäre die Verwendung einer digitalen Signatur.[11] Diese werden mittels eines kryptographischen Verfahrens durch den Inhaber eines (geheimzuhaltenden) privaten Schlüssels erstellt und können durch jeden Inhaber des zugehörigen öffentlichen Schlüssels überprüft werden. Die Identität des Schlüsselpaar-Inhabers kann durch eine vertrauenswürdige Stelle bestätigt werden. Gängige E-Mail-Programme sind in der Lage, digitale Signaturen nach dem S/MIME-Standard zu prüfen. Eine Signatur kann daneben auch in ein PDF-Dokument eingebettet und dann durch gängige PDF-Betrachter überprüft werden.

6. Allgemeine Sicherheitsvorkehrungen in der Sphäre des Absenders

Ein Indiz für Sicherheitsprobleme in der Sphäre des vorgeblichen Absenders kann in der Verwendung von Informationen liegen, die lediglich dort vorliegen – insbesondere, wenn gleich mehrere Empfänger gefälschte E-Mails erhalten. Plausibel sind etwa erratene Passwörter, die Ausnutzung von Sicherheitslücken in Software, die der vorgebliche Absender einsetzt, sowie Angriffe durch Schadsoftware (die aufgrund der erwähnten Sicherheitslücken oder durch menschliches Fehlverhalten installiert werden kann). Auch die Mitwirkung von Beschäftigten des vorgeblichen Absenders ist als Möglichkeit zu erwägen. Die Wahl hinreichend komplexer Passwörter, die zeitnahe Installation von Softwareupdates und auch die Nutzung von Virenscannern können zur Reduktion von Angriffsflächen beitragen. Dennoch bietet keine dieser Maßnahmen einen hundertprozentigen Schutz. Insoweit ist dem OLG zuzustimmen, dass die Klägerin keine Pflicht zum Ausschluss jeglichen Missbrauchs trifft. Sie trifft jedoch die Pflicht, ausreichende Sicherheitsvorkehrungen zu treffen. Es drängt sich der Verdacht auf, dass diese nicht ausreichend waren, wenn der vorgebliche Absender Informationen aus der Sphäre der Klägerin hat. Zudem wird durch die Vornahme der genannten Sicherheitsmaßnahmen eine Pflicht der Klägerin zur Information der Beklagten oder zum Ergreifen von Gegenmaßnahmen nicht ausgeschlossen, wenn aufgrund des Zugriffs eines erfolgreichen Angreifers mehrfach veränderte E-Mails versendet werden. Insgesamt greift die Ablehnung einer Pflichtverletzung der Klägerin zu kurz. Zudem lässt das OLG offen, wodurch der Versand der zweiten E-Mail (mit Informationen aus der Originalrechnung) denn sonst, wenn nicht durch einen erfolgreichen Angriff auf die Klägerin ermöglicht worden sein könnte. Insofern erscheint ein Beweis ersten Anscheins nicht völlig abwegig und die Ablehnung hätte zumindest einer weiteren Begründung bedurft. Daher können die Ausführungen insoweit nicht überzeugen und es ist nicht auszuschließen, dass das OLG eine kausale Pflichtverletzung der Klägerin und somit einen (gekürzten) Schadensersatzanspruch der Beklagten hätte annehmen müssen.

Nils Wiedemann

Studium an der Universität Konstanz und am University College Cork, Irland; Referendariat am LG Karlsruhe; LL.M. in IP and IT Law am Trinity College Dublin, Irland. Seit 2022 wiss. Mitarbeiter am Lehrstuhl von Prof. Dr. Sorge an der Universität des Saarlandes. Schwerpunkt: IT-Recht.

© Foto: Oliver Dietze

Christoph Sorge

Promotion in Informatik 2007 am KIT; 2008 - 2010 Research Scientist, NEC Laboratories Europe; 2010 - 2014 Juniorprofessor für Sicherheit in Netzwerken, Universität Paderborn. Seit 2014 Professor an der Universität des Saarlandes. Schwerpunkt: Rechtsinformatik, insb. Datenschutz und IT-Sicherheit.

7 PGP (RfC 4880) oder S/MIME (RfC 8551).
8 RfC 7208.
9 RfC 6376.
10 *Maroofi/Korczynski/Hölzel/Duda*, IEEE TNSM 2021, 3184, 3195.
11 *Sorge*, in: Ory/Weth (Hrsg.), jurisPK-ERV Band 1, 2. Aufl. 2022, Kapitel 3 Rn. 2 ff.