von Rechtsanwalt **Phil Salewski**

OLG Karlsruhe: Besondere Verschlüsselungsmechanismen für E-Mails zwischen Unternehmen nicht erforderlich

Die Kommunikation via E-Mail ist ein beliebtes Ziel von Phishing und Scamming. Durch die Vorspiegelung eines seriösen Ursprungs können über betrügerische E-Mails sensible Daten des Empfängers abgegriffen und missbraucht werden. Zur Gegenwehr kommen besondere Verschlüsselungsmechanismen zum Einsatz, welche die Vertraulichkeit und Vertrauenswürdigkeit der Kommunikation gewährleisten sollen. Ob und inwieweit Unternehmen im geschäftlichen Mailverkehr zur Ergreifung derartiger Verschlüsselungsmaßnahmen verpflichtet sind, klärte jüngst das OLG Karlsruhe.

I. Der Sachverhalt

Zwei GmbHs schlossen einen Kaufvertrag über einen gebrauchten Mercedes zum Preis von 13.500€.

Die beiden Geschäftsführer vereinbarten, dass der Verkäufer dem Käufer noch am selben Tag eine E-Mail schicken sollte. Im Anhang dieser E-Mails sendete der Verkäufer dem Käufer die Rechnung zu.

Zwei Minuten später bekam der Käufer eine zweite E-Mail, die eine manipulierte Zahlungsaufforderung enthielt, in der eine andere Bank als in der ersten E-Mail genannt wurde. Zudem war die E-Mail in der Sie-Form gehalten, obwohl die beiden Geschäftsmänner per Du miteinander kommunizierten. Am Ende der E-Mail befand sich ein unverständlicher Satz, der sich auf eine ganz andere Ware bezog.

Trotz all dieser Auffälligkeiten überwies der Käufer den Kaufpreis in Höhe von 13.500€ unter Nutzung der zuletzt erhaltenen Bankdaten.

Nach elf Tagen forderte der Verkäufer schließlich vom Käufer Zahlung des fälligen Betrags, was dieser jedoch mit der Begründung ablehnte, er habe seine Pflichten aus dem Kaufvertrag bereits erfüllt. Daraufhin klagte der Verkäufer.

In der ersten Instanz entschied das LG Mosbach zugunsten des Käufers und stellte fest, der Verkäufer habe „zu wenig“ für die Datensicherheit getan und so den Hackerangriff überhaupt erst ermöglicht. Der Verkäufer habe Sicherheitsvorkehrungen, etwa eine Anwendung des „Sender Policy Framework“-Verfahrens, eine Verschlüsselung des PDF-Anhangs, eine End-zu-End-Verschlüsselung oder eine Transportverschlüsselung, treffen müssen.

Gegen diese Entscheidung legte der Verkäufer sodann Berufung zum OLG Karlsruhe ein.

II. Die Entscheidung

Das OLG Karlsruhe hob als Berufungsgericht mit Urteil vom 27.07.2023 (Az: 19 U 83/22) die erstinstanzliche Entscheidung auf.

Anders als das LG Mosbach verurteilte das OLG Karlsruhe den Käufer zur Zahlung des vereinbarten Kaufpreises nebst Zinsen und Prozesskosten. Eine Revision wurde nicht zugelassen.

Konkrete gesetzliche Vorgaben für Sicherheitsvorkehrungen beim Versand von E-Mails im geschäftlichen Verkehr gebe es nicht. Insbesondere sei auch der sachliche Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) im Streitfall nicht eröffnet, da diese nur für die Verarbeitung von Informationen gelte, die sich auf eine natürliche Person beziehen (Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO).

Ferner sei auch eine ausdrückliche Vereinbarung über notwendige Verschlüsselungsmaßnahmen des Mailverkehrs zwischen den Parteien unterblieben, wobei insbesondere der beklagte Käufer, von dem die Initiative der Mail-Abwicklung ausgegangen sei, Datensicherheitsanforderungen unerwähnt gelassen habe.

Das Maß an notwendigen Sicherheitsvorkehrungen im geschäftlichen Mailverkehr bestimme sich daher vorliegend nach den berechtigten Sicherheitserwartungen des maßgeblichen Verkehrs unter Berücksichtigung der Zumutbarkeit.

1.) Sender Policy Framework (SPF)

Diese Auslegung zugrunde gelegt, komme die Anwendung eines „Sender Policy Framework“-Verfahrens schon aus tatsächlichen Gründen nicht in Betracht.

Dabei handle es sich nämlich um ein Protokoll, mit dem geprüft werden könne, ob der sendende E-Mail-Server berechtigt ist, für die Domäne E-Mails zu verschicken.

Beeinflussbar sei die Anwendung des Verfahrens aber nur bei Betreiben eines eigenen Mail-Servers und nicht – wie beim Verkäufer der Fall – bei Rückgriff auf Serverleistungen eines Dritten.

2.) Verschlüsselung des PDF-Anhangs

Die Verschlüsselung von PDF-Dateien sei im geschäftlichen Verkehr unüblich, es sei denn, es gehe um den Austausch empfindlicher Betriebs- oder Geschäftsgeheimnisse.

Bereits insofern könne diese Verschlüsselungsart nicht als zu beachtender Sicherheitsstandard angesehen werden.

Unabhängig davon sei dem Käufer bei Öffnen des PDF aber zwangsweise bekannt gewesen, dass dieses nicht verschlüsselt gewesen sei, weil anderenfalls ein Passwort abgefragt worden wäre. Durch das Öffnen des PDF und die Zugrundelegung des Inhalts für nachfolgende Handlungsentscheidungen habe der Käufer daher selbst einen Verschlüsselungsschutz abbedungen.

3.) End-zu-End-Verschlüsselung

Wenn auch von offiziellen Stellen zur Einrichtung einer End-zu-End-Verschlüsselung im geschäftlichen Mailverkehr zur Vermeidung von Vertraulichkeitsrisiken geraten werde, werde dieses Verfahren bisher nur stark vereinzelt angewendet und diene daher nicht als Orientierungshilfe für einen allgemein verbindlichen Sicherheitsstandard.

Hinzu komme, dass für eine End-zu-End-Verschlüsselung sowohl der Versender als auch der Empfänger über die notwendigen Zertifikate verfügen müssten, deren Anwendung also nicht nur vom Versender abhänge.

4.) Transportverschlüsselung

Die Transportverschlüsselung von Mails sei ein Prozess, bei dem der Inhalt der Übermittlung zwischen Absender und E-Mail-Anbieter, zwischen zwei E-Mail-Anbietern und zwischen E-Mail-Anbieter und Empfänger verschlüsselt werde, wobei dieser automatisiert abläuft und in der Regel keine Aktion des Absenders oder Empfängers erfordere. Als Verschlüsselungsmechanismus diene ein SSL/TLS-Protokoll.

Maßgeblich für die Anwendung des Protokolls sei aber, dass sich die Serveranbieter der kommunizierenden Mailadressen einem Verbund angeschlossen hätten, in welchem das Protokoll durch gegenseitige technische Abstimmung überhaupt zum Einsatz kommen könne.

Dessen Implementierung hänge also maßgeblich von den Serverspezifikationen ab und sei vom Sender oder Empfänger nicht individuell beeinflussbar.

Auch insoweit scheide mithin die Zugrundelegung als allgemeinverbindlicher Sicherheitsstandard aus.

III. Fazit

Nach Ansicht des OLG Karlsruhe existierten im geschäftlichen E-Mail-Verkehr zwischen Unternehmen jedenfalls dann, wenn es nicht um die Übermittlung besonders schützenswerter Informationen oder von Betriebsgeheimnissen gehe, keine allgemeinverbindlichen Sicherheitsvorkehrungen zur Verhinderung von Datenmissbrauch.

Insbesondere ist die DSGVO, die durchaus die Einrichtung technischer und organisatorischer Sicherheitsmaßnahmen vorschreibt, nicht anwendbar, wenn ausschließlich Informationen zwischen juristischen Personen per Mail ausgetauscht würden.

Komme es im Zuge einer geschäftlichen Mailkommunikation zwischen zwei juristischen Personen zu einer Datenmanipulation mit anschließendem Scamming, könne sich ein Schuldner die Zahlung auf ein Betrugskonto nicht schuldbefreiend anrechnen lassen.

Zu beachten ist, dass die Entscheidung ausdrücklich nur für eine Mailkommunikation zwischen zwei juristischen Personen erging. Anders dürfte der Fall insofern zu bewerten sein, wenn die geschäftliche Kommunikation zwischen natürlichen Einzelunternehmen oder die Kommunikation mit Verbrauchern betroffen ist. In diesem Fall findet die DSGVO nämlich uneingeschränkt Anwendung und kann dazu

verpflichten, geeignete Sicherheitsvorkehrungen zur Vertraulichkeitswahrung von E-Mail-Inhalten zu treffen.

Autor:
RA Phil Salewski
Rechtsanwalt