Cyberbetrug im Geschäftsverkehr: Zahlungspflicht bleibt bestehen

Business-E-Mail-Compromise: OLG Linz verpflichtet Unternehmen zur erneuten Zahlung

Die Klägerin, eine ungarische Lebensmittelproduzentin, erhält rund 95.000 Euro zugesprochen, nachdem die beklagte, oberösterreichische Handelsgesellschaft den Rechnungsbetrag infolge eines Cyberangriffs auf ein falsches Konto überwiesen hatte. Hacker hatten den laufenden E-Mail-Verkehr manipuliert und gefälschte Kontodaten eingeschleust. Das Oberlandesgericht Linz entschied, dass die Zahlungspflicht trotz Fehlüberweisung bestehen bleibt und verpflichtete die Beklagte zur vollständigen Zahlung. Das Urteil ist rechtskräftig.

Die Klägerin belieferte die Beklagte regelmäßig mit Mohnprodukten. Bestellungen, Rechnungen und organisatorische Abstimmungen wurden routinemäßig per E-Mail abgewickelt. Im Herbst 2021 schalteten sich unbekannte Täter in diesen E-Mail-Verkehr ein und sendeten eine manipulierte Nachricht, die eine angebliche neue Bankverbindung der Klägerin enthielt. Die Mitarbeiterin der Beklagten hatte zwar kurz Zweifel, veranlasste dennoch anschließend zwei Überweisungen von insgesamt 95.348,- Euro auf das betrügerische Konto. Als der Betrag bei der Klägerin nicht einlangte, forderte diese die offene Zahlung erneut ein.

Die Positionen der Parteien

Die Klägerin machte geltend, die Zahlungspflicht sei durch die Überweisung auf das falsche Konto nicht erfüllt worden. Der Hackerangriff sei der Sphäre der Beklagten zuzurechnen, da deren E-Mail-Konto manipuliert worden sei und die fremde polnische Kontoverbindung erkennbar gewesen wäre. Da die Beklagte für den korrekten Zahlungseingang hafte, schulde sie weiterhin den offenen Betrag.

Die Beklagte wandte im Kern ein, der Angriff sei ausschließlich auf die IT-Struktur der Klägerin zurückzuführen. Die Klägerin hätte ihre Systeme besser schützen müssen.

Erstgericht: Verschulden auf beiden Seiten

Das Landesgericht Linz sprach nur die Hälfte des eingeklagten Betrags zu und nahm ein gleichteiliges Verschulden beider Parteien an. Nach zusammengefasster Ansicht des Gerichts hätten Mitarbeiter:innen auf beiden Seiten den Cyberangriff erkennen können, da die Absenderadresse im Schriftverkehr deutlich verändert war.

Da beide Parteien somit die Möglichkeit gehabt hätten, die Manipulation rechtzeitig zu bemerken und zu verhindern, erschien dem Erstgericht lediglich ein Zuspruch von 50 Prozent des Forderungsbetrags gerechtfertigt.

Berufungsgericht: Verschulden liegt allein bei der Beklagten

Das Oberlandesgericht Linz beurteilte den Fall anders und gab der Klägerin zur Gänze Recht. Grundsätzlich: Die Überweisung auf das falsche Konto erfüllt die Schuld nicht, und das Risiko einer Fehlüberweisung liegt prinzipiell beim zahlenden Unternehmen.

Ein Mitverschulden der Klägerin verneinte das Gericht ausdrücklich. Zwar erfolgte der Hackerangriff über die technische Infrastruktur der Klägerin, doch gab es keinerlei Feststellungen, dass eine technische Nachlässigkeit auf ihrer Seite ursächlich gewesen war. Ebenso wenig steht fest, dass die Klägerin Hinweise auf den Betrug erhalten hat oder Verdacht schöpfen hätte müssen. Diesbezüglich liegt die Behauptungs- und Beweislast bei der Beklagten.

Im Gegensatz dazu kam es bei der Beklagten zu konkreten Zweifeln an der plötzlichen Änderung der Kontodaten. Die Beklagte hätte nach Ansicht des Oberlandesgerichts einfache und zumutbare Schritte zur Überprüfung der Bankdaten setzen können – etwa durch telefonische Nachfrage. Da somit weder ein technischer Fehler noch ein vorwerfbares Verhalten auf Seiten der Klägerin festgestellt wurde, verpflichtete das Oberlandesgericht die Beklagte zur vollen Zahlung.

Das Urteil ist rechtskräftig. Die Entscheidung ist im RIS abrufbar: Weblink

Rückfragehinweis

Dr. Wolfgang SEYER
Telefon: +43 57 60121 11627
Mobil: +43 676 8989 41627
E-Mail: medienstelle.olglinz@justiz.gv.at

Mag. Wolf-Dieter GRAF
Telefon: +43 57 60121 11640
Mobil: +43 676 8989 41640
E-Mail: medienstelle.olglinz@justiz.gv.at