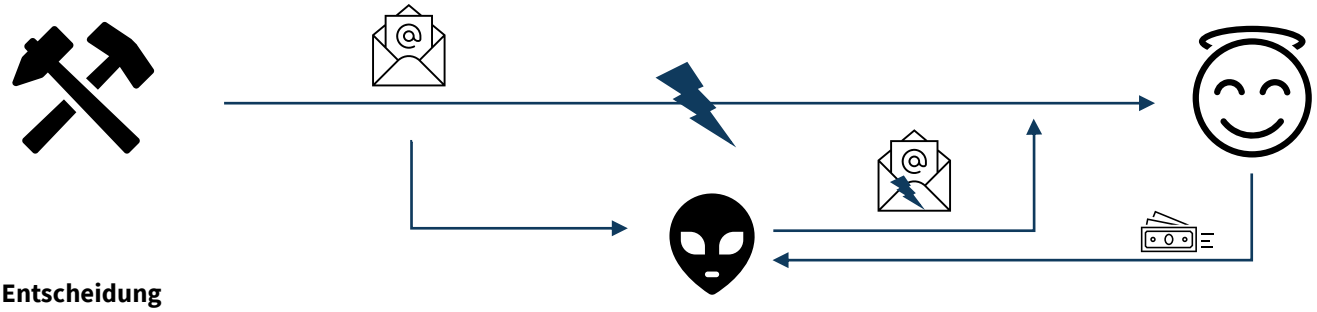
Rechnungen per E-Mail nur mit Verschlüsselung

Eine aktuelle Entscheidung des Schleswig-Holsteinischen OLG (18.12.2024 - 12 U 9/24) beschäftigt sich mit dem derzeit häufig anzutreffenden Hacker-Angriff **Man-in-the-Middle**.

Sachverhalt

Ein Unternehmen hatte eine Rechnung per E-Mail an einen Verbraucher (= **B2C-Geschäft**) versendet. Die E-Mail wurde durch einen Hacker abgefangen. Auf der Rechnung wurde die Bankverbindung manipuliert. Sodann wurde diese an den Kunden weitergeschickt. Dieser zahlte daraufhin den Rechnungsbetrag nicht an das Unternehmen sondern auf das Konto der Betrüger.



Entscheidung

Die Zahlungsklage des Unternehmens gegen den Kunden wurde abgewiesen. Die Zahlung hat nach Auffassung des OLG zwar keine Tilgungswirkung. Aufgrund eines Verstoßes gegen die Datenschutzgrundverordnung steht dem Kunden jedoch ein Schadensersatzanspruch in Höhe des Rechnungsbetrages zu, den er der Forderung entgegenhalten kann.

Das OLG bezog sich auf die Regelung des Art. 32 DSGVO. Hiernach müssen Unternehmen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Eine (in den meisten E-Mails verbreitete) reine Transportverschlüsselung (TLS) reiche nicht aus. Das finanzielle Risiko durch Verfälschung der angehängten Rechnung sei zu groß. Es biete dem Kunden keinen ausreichenden Schutz. Vielmehr sei eine **Ende-zu-Ende Verschlüsselung** zu wählen.

Für den unternehmerischen Geschäftsverkehr hatte das OLG Karlsruhe (27.07.2023 – 19 U 83/22) in einem vergleichbaren Fall festgestellt, dass im **B2B-Bereich** keine gesetzliche Regelung existiere. Entscheidend seien die berechtigten Sicherheitserwartungen des jeweiligen Geschäftsverkehrs und die Zumutbarkeit entsprechender Maßnahmen. Unternehmen seien jedoch in der Pflicht, nachzuweisen, dass ihre Sicherheitsmaßnahmen den Anforderungen der DSGVO entsprechen.

Handlungsempfehlungen

- Eine Ende-zu-Ende Verschlüsselung sollte im B2C-Bereich zwingend-, im B2B-Bereich dringend eingesetzt werden. Prüfen Sie die Möglichkeit ggf. mit Hilfe Ihres IT-Supports.
- Noch sicherer ist die Verwendung eines Passwortschutzes.
- Die Verschlüsselungspflicht betrifft auch E-Rechnungen, die seit dem 01.01.2025 schrittweise eingeführt werden. Hierbei handelt es sich um einen maschinenlesbaren XML-Datensatz (≠ pdf-Dokument). Eine postalische Versendung ist aus diesem Grund allenfalls während des Übergangszeitraums sinnvoll.
- Eine vertragliche Vereinbarung bzw. eine Einwilligung in ein niedrigeres Schutzniveau ist hoch umstritten:
  - Im B2C-Bereich ist das Risiko der Unwirksamkeit groß.
  - Zwischen Unternehmen dürfte dagegen eine individualvertragliche Vereinbarung zulässig sein; eine einseitige Mittelung des Schutzniveaus in AGB reicht dagegen – nicht zuletzt aufgrund der gängigen Abwehrklauseln – aus unserer Sicht nicht aus.

Wir unterstützten Sie gerne bei der rechtlichen Umsetzung.

Dr. Christopher Weidt, LL.M. (Leeds)
Rechtsanwalt