IT-Sicherheit und IT-Compliance - was müssen Unternehmen tun?

IT Security Update - Special Edition „IT-Sicherheitsrecht kompakt“

Do, 16.05.2024, 09:00 - 11:30

IT-Kanzlei dr-lapp.de

Aktueller Fall – Zahlung an Hacker

Kaufvertrag über einen gebrauchten Pkw Daimler Typ E200T zum Preis von 13.500 €

Auf Wunsch der Käuferin wird die Rechnung vom Geschäftsführer der Verkäuferin per E-Mail gesendet

Rechnung nennt in Briefkopf und Fußzeile ein Konto der Verkäuferin bei der Sparkasse T

OLG Karlsruhe, Urteil vom 27. Juli 2023 – 19 U 83/22 –, juris

Hacking

Zwei Minuten nach der Mail erhält die Käuferin eine erneute Mail

Abgesendet von der E-Mail-Adresse der Verkäuferin

neue Rechnung mit gleichem Briefkopf (Bankverbindung)

Hacking

Fußzeile der Rechnung jedoch mit Bankverbindung eines P.D. (Kontoinhaber) bei der S-Bank

Anrede in der Mail per „Sie“, statt sonst per „Du“

„Bitte senden Sie uns nach der Herstellung der Decke eine Kopie nach der Banküberweisung“

Schaden

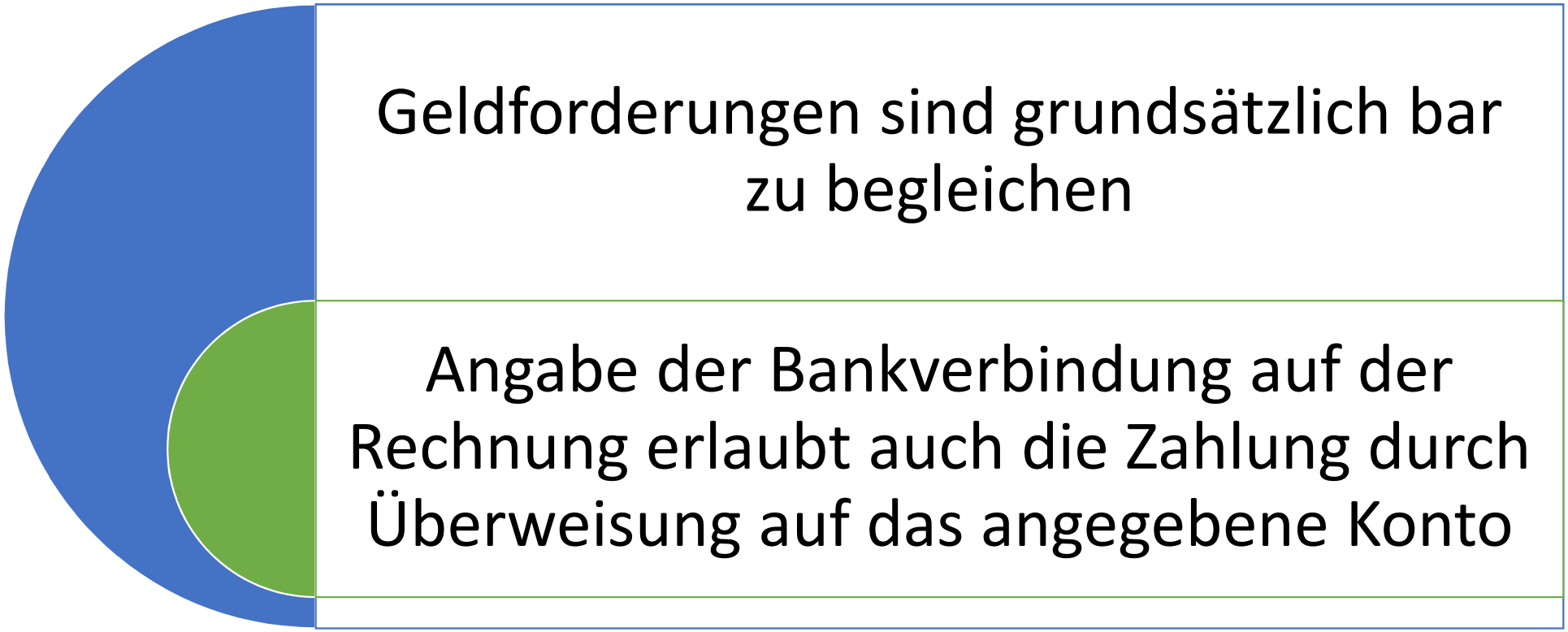
Käuferin zahlt auf das Konto des P.D. bei der S-Bank, das in der Fußzeile der zweiten Rechnung angegeben war

Geld ist weg

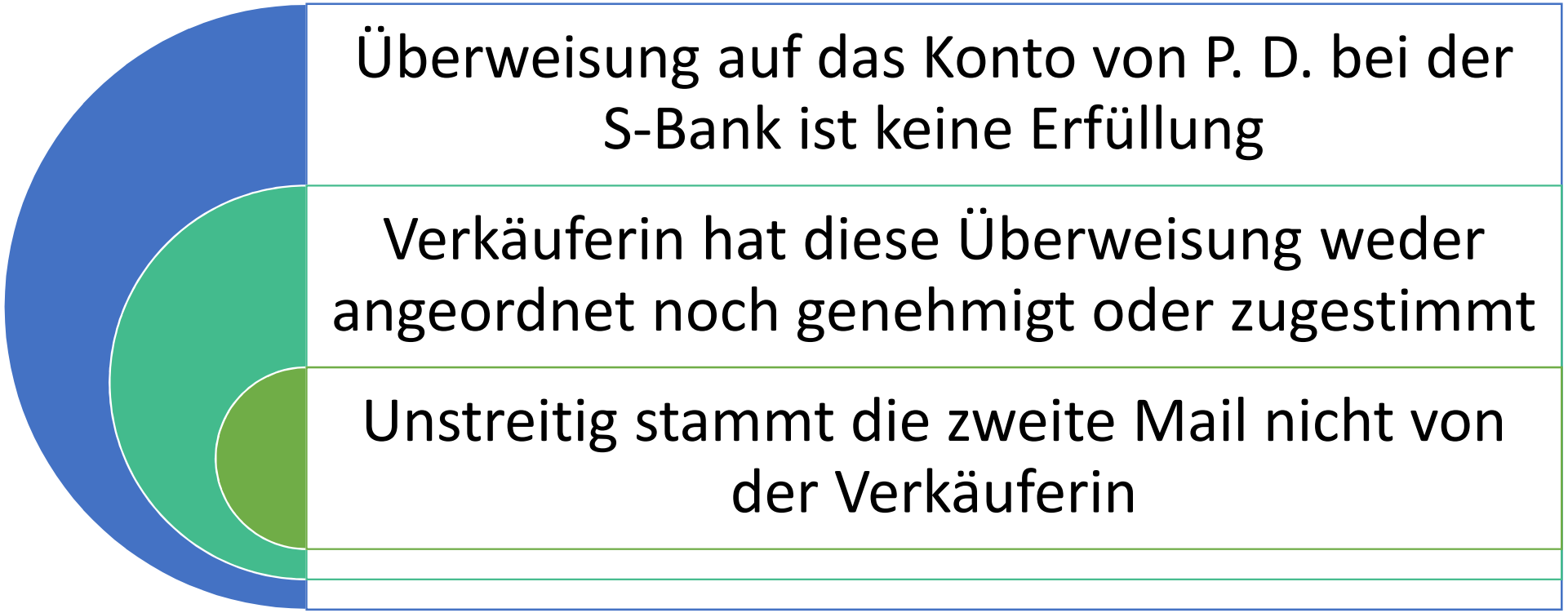
Verkäuferin will weiter Zahlung des Kaufpreises

Käuferin will nicht doppelt zahlen

Rechnung ist nicht bezahlt



Überweisung reicht nicht



Halzband

BGH hatte in der Entscheidung ***Halzband*** den Inhaber eines eBay Kontos für Schutzrechtsverletzungen und Wettbewerbsverstöße eines Dritten haften lassen, wenn er die Zugangsdaten nicht ausreichend gesichert hatte.

OLG Frankfurt hält das für die Frage der Erfüllung einer Geldschuld nicht für vergleichbar

Zwischenergebnis

- Kaufpreis ist nicht bezahlt
- Käuferin hat Anspruch auf Rückzahlung
- Eventuell Schadensersatzanspruch

Schadensersatzanspruch

Sicherheit bei der Verkäuferin

- Passwort zum E-Mail-Konto neun Stellen aus Buchstaben und Zahlen
- Firewall von Microsoft
- Vollversion des Antiviren-Programms von X-Security mit eingestellter automatischer Updatefunktion
- „Zwei-Faktor-Authentifizierung“ für den Zugang zum E-Mail-Postfach sei wohl möglich, aber nicht eingerichtet

Sicherheit bei der Verkäuferin

Passwörter waren ausschließlich auf den PCs des Geschäftsführers und eines Mitarbeiters S. hinterlegt, zu denen nur diese beiden Personen Zugang hatten

Start des PC nur mit Passwort

Sicherheit bei der Käuferin

Kennwort zum E-Mail-Konto aus Zahlen und Sonderzeichen und 20 Stellen

Zugriff haben der Geschäftsführer, beide IT-Administratoren sowie Mitarbeiter des genutzten Diensteanbieters N.

Zweifaktorauthentifizierung war nicht möglich und wurde auch nicht für erforderlich gehalten

Sicherheit bei der Käuferin

Laptops mit Bitlocker verschlüsselt

Windows Passwort: mind. acht Zeichen mit Klein- und Großbuchstaben, Sonderzeichen und Zahlen

Mail-Konto auch auf einem iPhone

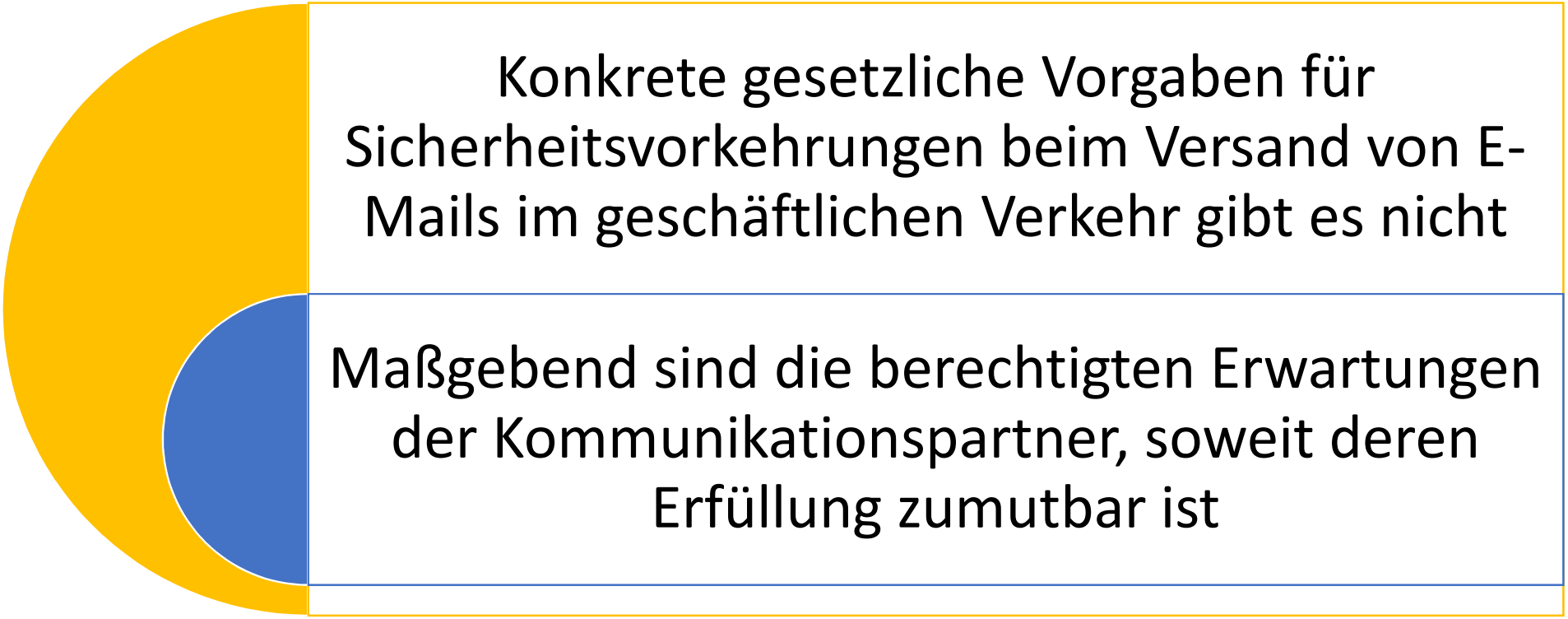
Vertragliche Verpflichtung

Vertrag wurde telefonisch geschlossen

Käuferin hat per E-Mail die Überweisung vorgeschlagen und Bankkonto erfragt

Konkrete Vereinbarungen zur IT-Sicherheit bei E-Mail etc. wurden nicht getroffen

Gesetzliche Verpflichtung



Orientierungshilfe DSK

Konferenz der unabhängigen Daten-schutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021

- Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Orientierungshilfe DSK - Maßnahmen

Pflichten beim Versand von E-Mail bei normalem Risiko

- insbesondere Transportverschlüsselung TLS

Pflichten beim Versand von E-Mail bei hohem Risiko

- Ende-zu-Ende-Verschlüsselung
- qualifizierte Transportverschlüsselung

Berufsgeheimnisträger

- Abwägung nach Risiko

Datenschutzrecht und IT-Compliance

Datenschutzrecht schützt personenbezogene Daten und regelt hierfür Anforderungen an die Sicherheit

IT-Sicherheitsrecht schützt die im Unternehmen vorhandenen Informationen insbesondere vor fremden Zugriff und Verlust

Ziel des Datenschutzrechts ist auch die Richtigkeit und Unversehrtheit der personenbezogenen Daten

Auch in E-Mails zwischen Unternehmen sind oft personenbezogene Daten, beispielsweise die Namen der handelnden Geschäftsführer

Verschlüsselung

Transportverschlüsselung ist Standard und verpflichtend

Verschlüsselung der Dateianhänge und Ende-zu-Ende-Verschlüsselung der gesamten Kommunikation erfordert Mitwirkung der Gegenseite und komplexere Vorgehensweise

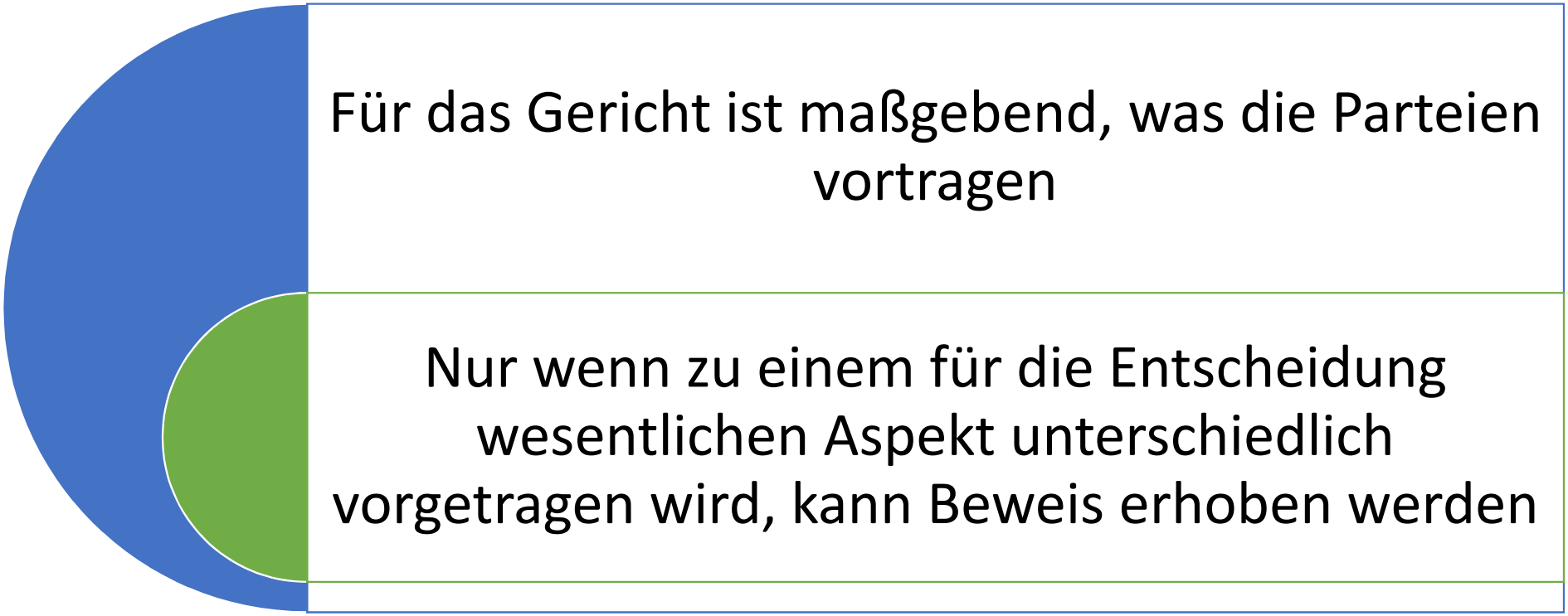
Kausalität

Nach dem übereinstimmenden Vortrag der Parteien ist der Hergang nicht geklärt,

Andere Kunden der Verkäuferin haben ähnlich veränderte Rechnungen erhalten

Trotzdem sah das OLG Karlsruhe keinen Beweis ersten Anscheins, damit keine Kausalität

Prozessuale Wahrheit



Mitverschulden der Käuferin

Unstimmigkeiten in der zweiten E-Mail

- Anrede „Sie“ statt wie sonst „Du“
- sprachliche Fehler („ausgestelltes“ Bankkonto)
- vollkommen unverständlicher Satz („Bitte senden Sie uns nach der Herstellung der Decke eine Kopie nach der Banküberweisung“)

Mitverschulden der Käuferin

Unstimmigkeiten in der Rechnung

- Zwei Bankverbindungen
- Natürliche Person ohne erkennbaren Bezug zum Verkauf als Kontoinhaber genannt

Keine Ausreden

„ich habe die Mail nicht vollständig gelesen“

- unvollständiges Lesen einer Nachricht, in der es immerhin um die Änderung der Kontoverbindung geht, auf die ein fünfstelliger Kaufpreis gezahlt werden soll, ist nach Ansicht des OLG Karlsruhe auch für sich betrachtet unsorgfältiges Handeln

Ergebnis

Kaufpreis muss von der Käuferin bezahlt werden

Gegebenenfalls muss die Überweisung zurückgefordert werden

Mitverschulden gleicht mögliches Verschulden in diesem Fall vollständig aus

IT-Kanzlei dr-lapp.de GbR

- **Dr. Thomas Lapp**
  Rechtsanwalt und zertifizierter QVM-Mediator
  Fachanwalt für IT-Recht

- **Corinna Lapp**
  Rechtsanwältin und Mediatorin
  Fachanwältin für IT-Recht

Berkersheimer Bahnstraße 5, 60435 Frankfurt

Tel.: 069/9540 8865 - anwalt@dr-lapp.de

IT-Kanzlei dr-lapp.de