orka Newsletter | Commercial

Betrug durch manipulierte Rechnungen – so schützen Sie Ihr Unternehmen

Der Versand von Rechnungen per E-Mail ist für viele Unternehmen ein fester Bestandteil ihres Alltags, genau wie eine rein digitale Absprache von Handlungsabläufen. Dabei sind Unternehmensdaten oft leicht im Internet für die Allgemeinheit zugänglich. Diese Gegebenheiten machen sich Cyberkriminelle zunutze: Fake-Rechnungen von vermeintlichen Lieferanten, CEO-Fraud oder Phishing – die Betrugsmaschen sind vielfältig. Der sogenannte Überweisungsbetrug ist weit verbreitet und zieht für die Betroffenen in der Regel erhebliche finanzielle Schäden nach sich.

Der beste Schutz gegen Betrugsmaschen dieser Art besteht darin, präventive Sicherheitsmaßnahmen zu ergreifen und Mitarbeitende entsprechend zu sensibilisieren.

Was aber ist zu tun, wenn es bereits zu einer Zahlung auf eine manipulierte Rechnung gekommen ist?

In diesem Newsletter erfahren Sie, woran Sie Fake-Rechnungen erkennen, wie Sie sich davor schützen können und welche Schritte erforderlich sind, falls eine Zahlung auf eine solche Rechnung bereits erfolgt ist. Zudem beleuchten wir, welche Ansprüche Ihrem Unternehmen in diesem Fall möglicherweise zustehen.

orka

Die unterschiedlichen Facetten von Überweisungsbetrugsfällen

Betrüger verschaffen sich häufig Zugang zu EDV-Systemen von Unternehmen und suchen gezielt nach eingegangenen Rechnungen im PDF-Format. Diese werden manipuliert, indem die ursprünglich angegebene IBAN des tatsächlichen Rechnungsstellers durch eine Kontoverbindung des Betrügers ersetzt wird. Die gefälschte Rechnung wird anschließend unter einer E-Mail-Adresse versandt, die dem Absender den Anschein eines vertrauten Geschäftspartners verleiht. Mitunter findet zusätzlich eine E-Mail-Korrespondenz zwischen dem Unternehmen und den Betrügern statt, wodurch der Eindruck entsteht, dass es sich um den rechtmäßigen Rechnungssteller handelt. In anderen Fällen teilen als Mitarbeiter von Vertragspartnern getarnte Betrüger eine angeblich „neue“ Bankverbindung mit und leiten so Zahlungen zur Begleichung echter Rechnungen auf ihr eigenes Bankkonto um.

Eine weitere Betrugsmasche ist der sog. „CEO-Fraud“, bei dem sich die Täter als Führungskräfte des Unternehmens selbst ausgeben und Mitarbeitende anweisen, schnell eine Überweisung auszuführen.

Daneben fordern Betrüger mittels Phishing-Mails, -Anrufen oder -SMS dazu auf, Daten zu überprüfen und zu aktualisieren. Als Vorwand wird dabei oft der baldige Ablauf von Abonements oder Verträgen genannt oder auch ein Sicherheitsvorfall suggeriert, auf Grund dessen eine Passwort-Aktualisierung notwendig sein soll.

Zahlungspflicht nach Überweisung auf eine Fake-Rechnung

Im Falle der Zahlung einer manipulierten Rechnung stellt sich in einem ersten Schritt die Frage, ob Ihr Unternehmen die Zahlung erneut an den tatsächlichen Vertragspartner anweisen muss. Eine Zahlungsverpflichtung erlischt grundsätzlich erst dann, wenn der geforderte Betrag an den jeweiligen Gläubiger geleistet wird, oder – bei Zahlung an einen Dritten – wenn dieser im Voraus ausdrücklich vom Vertragspartner zur Entgegennahme der Zahlung ermächtigt wurde oder der Vertragspartner die Zahlung im Nachhinein genehmigt (§§ 362 Abs. 2, 185 BGB). Dies ist bei Betrugsfällen mittels gefälschter Rechnungen nicht der Fall.

Zurechnung der Fake-Rechnung nach den Grundsätzen der Anscheinsvollmacht

Im Einzelfall kann bei der Versendung manipulierter Rechnungen eine Zurechnung nach den Grundsätzen der Anscheinsvollmacht in Betracht kommen, sodass die

Zahlung auf eine gefälschte Rechnung dann ausnahmsweise Erfüllungswirkung hat (in diese Richtung etwa OLG Saarbrücken, Urteil vom 06.06.2019 – 5 U 84/18). Bei der Anscheinsvollmacht handelt es sich um eine Rechtsfigur, bei welcher der angebliche Vertreter (in diesem Fall der Betrüger) für die vertretene Person auftritt, ohne dass die erforderliche Vollmacht tatsächlich vorliegt. Unter bestimmten Voraussetzungen wird das Handeln des Anscheinsvertreters dem vermeintlich Vertretenen auch dann zugerechnet, wenn der Vertretene hiervon keine Kenntnis hatte.

Erforderlich ist der **objektive Rechtsschein einer Eigenerklärung.** Ein solcher Rechtsschein kann beispielsweise dadurch gesetzt werden, dass eine Fake-Rechnung täuschend echt wirkt – etwa durch die Verwendung echter E-Mail-Adressen von Mitarbeitenden oder das Nachahmen offizieller Briefbögen.

Eine Zurechnung nach den Grundsätzen der Anscheinsvollmacht setzt weiter voraus, dass der Vertragspartner **durch mangelnde Sorgfalt diesen Rechtsschein zurechenbar** gesetzt hat. Der Vertretene muss das Handeln des vermeintlichen Vertreters nicht kennen, aber es bei pflichtgemäßer Sorgfalt hätte erkennen und verhindern können. Maßgeblich ist dafür, ob die Sicherheitsmaßnahmen des Unternehmens den branchenüblichen Anforderungen genügten. Die Beweislast liegt grundsätzlich bei dem Unternehmen, dessen IT-Systeme kompromittiert wurden.

Das Auftreten eines Betrügers als Anscheinsvertreter muss grundsätzlich mit einer **gewissen Dauer und Häufigkeit** einhergehen. In den meisten Fällen wird

daran die Zurechnung scheitern. Sollte diese Voraussetzungen in den hier vorliegenden Fällen der Identitätstäuschung ausnahmsweise für nicht erforderlich gehalten werden, sind jedoch höhere Anforderungen an die Zurechenbarkeit zu stellen.

Maßgeblich ist zuletzt, ob der Empfänger der Fake-Rechnung **berechtigterweise darauf vertrauen durfte, dass es sich um eine echte Forderung des Vertragspartners handelt.** Anhaltspunkte hierfür sind:

- Ist die Rechnung einer konkreten Bestellung zuzuordnen?
- Weist die Fake-Rechnung eine professionelle Gestaltung auf?
- Gibt es formale Ungereimtheiten wie Rechtschreibfehler oder falsche Formatierungen?
- Ist die Rechnung digital oder handschriftlich unterzeichnet?
- Erfolgt die Kommunikation über bekannte Ansprechpartner?

Letztlich hängt die rechtliche Bewertung davon ab, ob der Vertragspartner Ihres Unternehmens angemessene

Schutzmaßnahmen ergriffen hat und ob Ihr Unternehmen als Empfänger misstrauisch hätte werden müssen.

Zudem ist die Anwendbarkeit der Grundsätze der Anscheinsvollmacht in Fällen einer Zahlung auf eine manipulierte Rechnung in der Rechtsprechung nicht abschließend geklärt und konturiert (vgl. z.B. OLG Karlsruhe, Urteil vom 27.07.2023 – 19 U 83/22 und OLG Schleswig, Urteil vom 18.12.2024 – 12 U 9/24, die in vergleichbaren Fällen keine Zurechnung nach den Grundsätzen der Anscheinsvollmacht, aber eine Schadensersatzpflicht unter gewissen Voraussetzungen des Vertragspartners erwägen).

In der Praxis bleibt somit das Risiko bestehen, dass Ihr Unternehmen trotz der Zahlung an den Betrüger weiterhin gegenüber dem Vertragspartner leistungspflichtig bleibt.

Bei Verdacht lieber vorher beim Vertragspartner erkundigen:

Die Zahlung auf eine Fake-Rechnung entbindet i.d.R. nicht von der Zahlungspflicht gegenüber dem Vertragspartner!

Mögliche Rückzahlungs- und Schadensersatzansprüche

Es besteht die Möglichkeit, dass Ihrem Unternehmen sowohl gegenüber dem Vertragspartner als auch gegenüber den beteiligten Kreditinstituten – der eigenen Bank und der Empfängerbank – Ansprüche auf Rückzahlung bzw. Schadensersatz zustehen. Dies erfordert jedoch immer eine auf den jeweiligen Fall abgestimmte Prüfung, denn die Art des Betrugs, die ergriffenen Sicherheitsmaßnahmen und auch das Handeln der Beteiligten unterscheiden sich von Fall zu Fall.

Schadensersatzansprüche gegenüber dem Vertragspartner

Ein Schadensersatzanspruch gegen den Vertragspartner in Höhe der auf eine manipulierte Rechnung hin getätigten Zahlung kann sich etwa aus einer schuldhaften Verletzung einer vertraglichen Nebenpflicht oder – soweit der Anwendungsbereich der DSGVO eröffnet ist – aus Art. 82 DSGVO ergeben.

Ob die von dem Vertragspartner implementierten Sicherheitsmaßnahmen dem branchenüblichen Standard entsprechen, spielt auch für die Frage möglicher Schadensersatzansprüche eine entscheidende Rolle.

Denn zu den vertraglichen Rücksichtnahmepflichten (§ 241 Abs. 2 BGB) gehört insbesondere auch die Implementierung angemessener IT-Sicherheitsmaßnahmen, um einen Cyberangriff zu verhindern. Das OLG Karlsruhe stellte dabei in einer Entscheidung aus dem Jahr 2023 an das „übliche Maß“ der Vorkehrungen keine allzu hohen Anforderungen: So hielt es das OLG Karlsruhe bereits für ausreichend, dass das E-Mail-Konto des Vertragspartners mit einem Passwort geschützt war, das nur zwei Personen bekannt war, regelmäßig

geändert wurde und durch eine Windows-Firewall sowie eine weitere Schutzsoftware abgesichert war (Urteil vom 27.07.2023 – 19 U 83/22). Eine Pflicht zur Nutzung einer Ende-zu-Ende-Verschlüsselung oder einer Transportverschlüsselung sah das Gericht nicht.

Demgegenüber bejahte das OLG Schleswig einen Schadensersatzanspruch eines Empfängers einer gefälschten Rechnung gegenüber dessen Vertragspartner gemäß Art. 82 DSGVO und begründete dies u.a. damit, dass der Vertragspartner beim Versand geschäftlicher E-Mails mit personenbezogenen Daten keine Ende-zu-Ende-Verschlüsselung genutzt hatte (OLG Schleswig, Urteil vom 18.12.2024 – 12 U 9/24).

Zukünftig werden die Pflichten von Unternehmen im Bereich der IT-Sicherheit durch die europäische NIS-2-Richtlinie und deren Umsetzung in deutsches Recht näher gesetzlich konturiert (unseren Newsletter zur Umsetzung der NIS-2-Richtlinie finden Sie hier).

Ob ein Schadensersatzanspruch gegen Ihren Vertragspartner besteht, hängt demnach maßgeblich von den konkreten Umständen des Einzelfalls ab – insbesondere von den betroffenen Daten, den tatsächlich ergriffenen Sicherheitsmaßnahmen und deren Angemessenheit im jeweiligen Kontext sowie von der Anwendbarkeit der DSGVO, bestehender gesetzlicher Pflichten zur IT-Sicherheit und zukünftig des Umsetzungsgesetzes zur NIS-2-Richtlinie. Es bedarf also einer sorgfältigen Prüfung. Sollte ein Schadensersatzanspruch im Einzelfall bestehen, könnte er dem Zahlungsanspruch des Vertragspartners entgegengehalten werden.

Haftung der Kreditinstitute

Neben der möglichen Haftung des Vertragspartners stellt sich die Frage, ob Ansprüche gegen die beteiligten Kreditinstitute bestehen.

Rückzahlungsanspruch gegen die eigene Bank

Nach § 675u S. 2 BGB besteht ein Erstattungsanspruch gegen die eigene Bank regelmäßig dann, wenn es sich um einen **nicht autorisierten** Zahlungsvorgang handelt. Eine Autorisierung fehlt, wenn der Bankkunde dem Zahlungsvorgang nicht zugestimmt hat, beispielsweise durch das TAN-Verfahren oder die Eingabe einer PIN, oder wenn er den Vorgang rechtzeitig widerrufen hat. Ein Widerruf ist jedoch nur bis zum Eingang des Zahlungsauftrags bei der Bank möglich (§§ 675j Abs. 2, 675p Abs. 1 BGB) und kommt daher in den meisten Fällen von Fake-Rechnungen nicht mehr in Betracht.

Die Gründe für die Autorisierung spielen dabei keine Rolle. Es ist daher unerheblich, ob Ihr Unternehmen die Überweisung aufgrund der Fake-Rechnung unter einer falschen Annahme getätigt hat. Die

Autorisierung bleibt wirksam, sofern das Authentifizierungsverfahren der Bank ordnungsgemäß durchlaufen wurde – der eigentliche Fehler liegt dann nicht innerhalb dieses Verfahrens, sondern bereits auf der vorgelagerten Ebene der Rechnungsstellung.

Schadensersatzanspruch gegen die Empfängerbank

Auch Ansprüche gegen die Empfängerbank sind in der Praxis nur unter besonderen Voraussetzungen durchsetzbar. Die Geltendmachung von Schadensersatzansprüchen erfordert in der Praxis schwer zu erbringende Nachweise für die Anspruchsvoraussetzungen, z.B. dass ein fehlerhafter Legitimierungsprozess der Empfängerbank gerade ursächlich für den durch die Überweisung auf ein falsches Konto entstandenen Schaden war.

Auch eine Haftung aus dem Verhältnis der Banken untereinander scheidet aus. Nach der Rechtsprechung des BGH (Urteil vom 06.05.2008 – XI ZR 56/07) entstehen durch das Innenverhältnis der Banken keine Schutzpflichten zugunsten der Bankkunden. Das bargeldlose Massenzahlungssystem soll vor allem eine schnelle und reibungslose Abwicklung gewährleisten – individuelle Schutzmechanismen für einzelne Kunden sind hierbei nicht vorgesehen.

Allerdings kommt ein Schadensersatz (aus abgetretenem Recht) immer dann in Betracht, wenn die Empfängerbank aufgrund konkreter Anhaltspunkte hätte erkennen müssen, dass es sich um eine betrügerische Zahlung handelt. In diesem Fall könnte eine Verletzung ihrer Sorgfaltspflichten vorliegen, denn die Kreditinstitute haben sich auch untereinander so zu verhalten, dass die Rechtsgüter der jeweils anderen Bank und die der Kunden nicht verletzt werden (§ 241 Abs. 2 BGB). Eine Verletzung dieser Sorgfaltspflichten wäre dann gegeben, wenn die Empfängerbank bei der Auszahlung an den Täter dessen betrügerische Absichten erkannt hat oder hätte erkennen müssen.

Schadensersatzanspruch gegenüber dem Zahlungsempfänger

Ein Schadensersatz- bzw. Rückzahlungsanspruch gegen den betrügerisch agierenden Zahlungsempfänger ist häufig faktisch schwer durchsetzbar. Zunächst muss dazu die Identität des Betrügers ermittelt werden. Hierzu bietet sich neben einer Anfrage bei der Bank des Zahlungsempfängers ein Antrag auf Einsicht in die bei der Polizei bzw. bei der Staatsanwaltschaft geführte Ermittlungsakte an.

Versicherungsschutz unter einer Vertrauensschaden- oder Cyberversicherung

Im Betrugsfall kann sich auch eine Prüfung lohnen, ob für den durch die Zahlung auf eine Fake-Rechnung entstandenen

Vermögensabfluss oder damit zusammenhängende Kosten Versicherungsschutz besteht, etwa unter einer Vertrauensschaden- oder Cyberversicherung.

Eine **Vertrauensschadenversicherung** bietet mitunter Versicherungsschutz für Schäden, die durch Zahlungen aufgrund einer gefälschten Anweisung, Bestellung oder Rechnung entstehen.

Zwar liegt ein Versicherungsfall i.S.d. **Cyberversicherung** im Falle der Zahlung auf eine Fake-Rechnung häufig nicht vor, wenn nicht das IT-System des versicherten Rechnungsempfängers, sondern lediglich das IT-System des Vertragspartners kompromittiert ist. Dann fehlt es nämlich an einer nach den gängigen Cyberversicherungsbedingungen erforderlichen Informationssicherheitsverletzung bzw. Netzwerksicherheitsverletzung bezogen auf die IT-Systeme des versicherten Unternehmens (s. LG Hagen, Urteil vom 15.10.2024 – 9 O 258/23). Auch besteht für den Abfluss von Vermögenswerten selbst häufig kein Versicherungsschutz in der Cyberversicherung.

Maßgeblich sind aber immer die konkret vereinbarten Versicherungsbedingungen und die jeweiligen Einzelfallumstände. Im Betrugsfall bietet sich deshalb eine genaue Prüfung des Versicherungsschutzes an.

Präventive Maßnahmen und Handlungsempfehlungen im Ernstfall

Der beste Schutz gegen Fake-Rechnungen besteht darin, präventive Sicherheitsmaßnahmen zu ergreifen und Mitarbeitende entsprechend zu sensibilisieren.

Doch auch im Falle einer Zahlung auf eine gefälschte Rechnung ist Ihr Unternehmen nicht schutzlos. Es bestehen diverse Handlungsmöglichkeiten. In jedem Fall ist schnelles und gezieltes Handeln entscheidend.

Erste Maßnahmen im Betrugsfall:

- Stoppen Sie weitere Zahlungen und informieren Sie Ihre Mitarbeitenden.
- Kontaktieren Sie unverzüglich Ihre Bank und bitten Sie um eine Stornierung der Überweisung.
- Erstatten Sie umgehend Strafanzeige.
- Lassen Sie mögliche Rückforderungsansprüche gegen den Vertragspartner, Banken oder andere Beteiligte prüfen.

Ihre Ansprechpartner

Dr. Frank Wältermann
Rechtsanwalt, Partner
Commercial

T +49 211 60035-280
frank.waeltermann@orthkluth.com

Maria Müller, LL.M. (Nottingham)
Commercial
Senior Associate

T +49 211 60035-252
maria.mueller@orka.law

Leonie Kolyvas
Rechtsanwältin, Associate
Commercial

T +49 211 60035-182
leonie.kolyvas@orka.law

Gereon Conrad, LL.M.
Rechtsanwalt, Salary Partner
Criminal Compliance

T +49 211 60035-343
gereon.conrad@orka.law

Felix Meurer
Rechtsanwalt, Salary Partner
Datenschutz, IT & Outsourcing

T +49 30 509320-117
felix.meurer@orka.law


One Team.
One Goal.