www.betriebs-berater.de

Betriebs Berater

BB

22|2025

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

26.5.2025 | 80. Jg.
Seiten 1217–1280

DIE ERSTE SEITE

WIRTSCHAFTSRECHT

STEUERRECHT

BILANZRECHT UND BETRIEBSWIRTSCHAFT

ARBEITSRECHT

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Patrick Bernd Findeis, StB, und Peter Braun, StB

Cyberrisiko E-Rechnung

Mit der Einführung der E-Rechnung vollendet das Umsatzsteuergesetz (UStG) einen Kurswechsel, der vor einigen Jahren noch nicht denkbar war. Einer der Autoren war Mitte bis Ende der 90er Jahre als Betriebsprüfer in Hessen eingesetzt. Zu dieser Zeit wurden Vorsteueransprüche rigoros versagt, wenn keine papierhafte Originalrechnung vorgelegt werden konnte. Akzeptiert wurden später aufwändig elektronisch signierte Dateien und, nach Wohlwollen des Prüfers, ausgedruckte unsignierte (PDF)-Dateien. Mit der Aufgabe des Vorrangs der papierhaften Rechnung zugunsten einer digitalen Rechnung vollzog das UStG zum 1.1.2025 nun eine Kehrtwende (s. BMF-Schreiben vom 15.10.2024) – mit Seiteneffekten. Im Folgenden wird aufgezeigt, welche Cyberrisiken die Einführung der E-Rechnung mit sich bringt und wie denkbare Handlungsoptionen aussehen könnten. Auf die E-Rechnung im engeren Sinne und auf detaillierte technische Beschreibungen wird nicht eingegangen. Der Aufsatz wendet sich an alle Berufskolleginnen und -kollegen, welche die Geschäftsführung bzw. die erste und zweite Führungsebene in Unternehmen beraten oder die selbst die Eingangsrechnung für ihre Mandantschaft verbuchen und ggf. Zahlungsfreigabelisten vorbereiten.

I. 266 Mrd. Euro Schaden durch Cyberangriffe

Kriminelle haben im Jahr 2024 durch Cyberangriffe Schäden in Höhe von rund 266 Mrd. € bei deutschen Unternehmen verursacht.[1] Das beinhaltet Schäden durch betrügerisch herbeigeführten tatsächlichen Geldabfluss, Personalaufwände, Neubeschaffung von Hardware und externe Kosten für IT-Sachverständige und Rechtsberater. Damit werden Schäden in der Größenordnung der kassenmäßigen Einnahmen im Jahr 2023 der Umsatzsteuer (einschließlich Einfuhrumsatzsteuer) mit 291,4 Mrd. Euro bzw. der Lohnsteuer mit 236,2 Mrd. Euro verursacht.[2]

Die Pflicht zur Entgegennahme von E-Rechnungen ab dem 1.1.2025 hebt das Thema Rechnungsbetrug nun auf eine digitale und damit automatisierbare Ebene. Leider gute Voraussetzungen für Kriminelle; es ist daher mit deutlich höheren Schadensummen in der Zukunft zu rechnen. Im Status quo berichten bereits drei von vier Unternehmen mit über zehn Mitarbeitenden über Cyperangriffe.[3] Das bedeutet, dass auch kleine und mittelständische Unternehmen angegriffen werden.

II. Neue und alte Risiken beim Rechnungsempfang

Unternehmen mussten sich in der Vergangenheit schon mit den Themen rund um erfundene oder gefälschte Rechnungen auseinandersetzen. Dubiose Unternehmensverzeichnisse oder Kriminelle haben in der Vergangenheit damit von sich Reden gemacht. Die Pflicht zur Entgegennahme von E-Rechnungen fügt diesem Bestandsrisiko nun

1 Bitkom, Studie „Wirtschaftsschutz 2024", www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz (Abruf: 19.2.2025).
2 Destatis, Steuereinnahmen 2023 summieren sich auf rund 916 Milliarden Euro, 5.6.2024, www.destatis.de/DE/Themen/Staat/Steuern/Steuereinnahmen/steuereinnah men.html (Abruf: 19.2.2025).
3 Bitkom, Organisierte Kriminalität greift verstärkt die deutsche Wirtschaft an, www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an#_ (Abruf: 19.2.2025).

ein neues, ein Cyberrisiko, hinzu. Die neuen Risiken werden durch die Menge an zugelassen Formaten[4] begünstigt. Dazu gehören unter anderem die im Design der E-Rechnung fehlende Signatur und das gesetzlich zugelassene unsichere Transportmedium E-Mail. Auch das massenhafte Fluten des E-Rechnungseingangs kann zu einem Risiko erwachsen. Diese neuen Gefahren werden nachfolgend beleuchtet.

1. Keine Signatur und unsicherer Transportder E-Rechnung

a) XML per E-Mail ist gesetzeskonform

In der einfachsten gesetzeskonformen Form ist eine E-Rechnung eine sogenannte XML-Datei, die per E-Mail an den Rechnungsempfänger, oftmals eingebettet in eine PDF-Datei im ZUGFerd-Format, geschickt wird.[5] Diese einfache und preisgünstige Lösung wird von den meistens Unternehmen in DE bevorzugt.

Eine XML-Datei ist ein allgemeines Datenformat, das dazu geschaffen wurde, dass sich Maschinen untereinander Daten zusenden und im Bedarfsfall, mit etwas Mühe, ein Mensch die Informationen lesen kann. Dazu ist der XML-Standard als Klartextstandard definiert. Dies wurde für die E-Rechnung unverändert übernommen.

Eine E-Rechnung im XML-Format enthält daher neben den Angaben zum leistenden Unternehmer und Leistungsempfänger sowie den Details zum Inhalt der abgerechneten Leistung auch Angaben und Anweisungen zum Zahlungsweg und Zahlungsziel im Klartext (z. B. IBAN, BIC, Zahlungsziele und Skonti). Jedoch fehlen Sicherheitsmechanismen wie digitale Signaturen oder Kontrollsummen (Hashes). Das heißt, dass

- auf Grund der fehlenden Signatur der Rechnungsaussteller/-übersender nicht technisch geprüft werden kann und
- auf Grund der fehlenden Kontrollsummen nicht technisch geprüft werden kann, ob die eingegangene bzw. verarbeitete/gebuchte Rechnung der ursprünglich versendeten Rechnung entspricht.

Der E-Mail-Standard fordert weder Verschlüsselungen noch Signaturen.[6] Dadurch kann eine zwischen Absender und Empfänger abgefangene und veränderte Mail nicht leicht und einfach erkannt werden. Das heißt, dass das offene Transportmedium E-Mail eine Manipulation beim Versand, während der Übermittlung von Sender zum Empfänger und sogar im Postfach des Empfängers leicht und einfach möglich macht.

Mittels unterschiedlicher Zusatzprodukten zu gängigen E-Mail-Programmen kann eine Signatur und/oder Verschlüsselung nachgerüstet werden. Die Herausforderung hierbei ist, dass sich Sender und Empfänger einer Mail auf denselben Standard einigen. Innerhalb von Konzernen mag das noch möglich sein; am freien Markt ist dieses Ansinnen, wie auch die De-Mail[7], gescheitert.[8]

Die Analyse von Webanwendung nach international anerkannten Standards (OWASP) zeigt, dass zu den häufigsten Schwachstellen von IT-Anwendungen mangelnde Verschlüsselung und unsicheres Design gehören. Beide Aspekte rangieren auf der OWASP Top Ten 2025 auf den Plätzen 2 und 4 und stellen für Cyberkriminelle somit einen lukrativen Ansatz für Angriffe dar.[9]

Die Verbindung von diesen beiden unsicheren Elementen führt im Ergebnis dazu, dass eine E-Rechnung als XML-Datei via E-Mail offener ist als jede Postkarte und ohne Spuren zu hinterlassen manipuliert werden kann.

b) Ein Beispiel

Der folgende kurze Ausschnitt aus einer E-Rechnung soll verdeutlichen, wie leicht lesbar, und damit einfach änderbar, eine XML-E-Rechnung ist. In dem Ausschnitt gibt der Rechnungsaussteller an, dass er via Überweisung bezahlt werden möchte und gibt als Zahlungsweg seine IBAN und BIC an:

```
<ram:SpecifiedTradeSettlementPaymentMeans>                => Beginn Zahlungsweg
  <ram:TypeCode>58</ram:TypeCode>                         => Code 58 = Überweisung
  <ram:PayeePartyCreditorFinancialAccount>                => Beginn Zielkontodaten
    <ram:IBANID>DExx 1234 5678 9012 3456 78</ram:IBANID>  => Ziel-IBAN
    <ram:AccountName>Lieferant 001</ram:AccountName>      => Kontoinhaber
  </ram:PayeePartyCreditorFinancialAccount>               => Ende Zahlungsweg
  <ram:PayeeSpecifiedCreditorFinancialInstitution>        => Beginn kontoführende Bank
    <ram:BICID>GENODEFxxxx</ram:BICID>                    => ZielBIC
  </ram:PayeeSpecifiedCreditorFinancialInstitution>       => Ende kontoführende Bank
 </ram:SpecifiedTradeSettlementPaymentMeans>              => Ende Zahlungsweg
```

Wer auch immer im Laufe der Erstellung, Übermittlung oder Verarbeitung der E-Rechnung Zugriff auf diese XML erlangt, kann diese Angaben leicht und einfach ändern. Wegen der fehlenden Kontrollsummen kann dies auch spurlos erfolgen. Wird die IBAN manipuliert, fließt die Zahlung, ohne Schuldbefreiung auszulösen, an einen kriminellen Dritten. Werden Positions- oder Summenbeträge manipuliert, fließt ggf. ein Mehrfaches des Rechnungsbetrags erst einmal ab. Ersteres ist ein definitiver finanzieller Schaden, während letzteres mindestens die Liquiditätssituation negativ beeinflussen kann, wenn nicht gar auch zu einem definitiven finanziellen Schaden führen kann.

c) Glaubhafte Szenarien durch Social Engineering

Selbst wenn bei der Bearbeitung der Eingangsrechnung eine abweichende/neue Kontoverbindung auffällt, kann durch sogenanntes Social Engineering durch den Angreifer ein glaubhafter Kontext aufgebaut werden. Zum Beispiel könnte im Weiteren in der E-Rechnung in einem Hinweistextfeld behauptet werden, dass der Lieferant die Einführung der E-Rechnung zum Anlass nimmt, seine Prozesse stärker zu digitalisieren und deswegen für alle neuen E-Rechnungen eine eigene Bankverbindung eingerichtet hat. Um Mahnungen oder Service- oder Lieferunterbrechungen vorzubeugen, möchte bitte nur noch auf die neue Bankverbindung überwiesen werden. Ein leider sehr glaubhafter Ansatz.

Erleichtert wird das Social Engineering durch die ZUGFerd-Rechnungsformat. Die XML-Datei mit dem maschinenlesbaren Anteil ist dabei in eine menschenlesbare PDF eingebunden. Wird nun der Rechnungsinhalt anhand der PDF geprüft, aber die Zahlung anhand der XML ausgelöst, dann kommt es bei einer entsprechend manipulierten XML-Datei zum Schadenfall. Mit solchen Manipula-

4 BMF, 15.10.2024 – III C 2 – S 7287-a/23/10001 :007 („E-Rechnungs-Erlass"), BStBl. I 2024,1320, Rn. 4 ff.
5 E-Rechnungs-Erlass, Rn. 28 ff.
6 Internet Engineering Task Force (IETF), RFC 5322 – Internet Message Format, Okt. 2008, www.rfc-editor.org/info/rfc5322 (Abruf: 19.2.2025).
7 *Wölbert*, Bundesregierung kündigt Ende von De-Mail in der Verwaltung an, www.heise.de/news/Bundesregierung-kuendigt-Ende-von-De-Mail-in-der-Verwaltung-an-9180138.html (Abruf: 19.2.205).
8 Bundesamt für Sicherheit in der Informationstechnik (BSI), E-Mail-Verschlüsselung, www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung.html (Abruf: 19.2.205).
9 Open Worldwide Application Security Project (OWASP), OWASP Top Ten 2025, owasp.org/www-project-top-ten/ (Abruf: 19.2.205).

tionen steht dem Betrug durch Social Engineering Tür und Tor offen.

Übrigens: Jede Eurobanknote hat fünf bis sieben Sicherheitsmerkmale.[10] Eine gefälschte E-Rechnung ist, aus Vorsteuersicht, bares Geld. Ohne ein einziges Sicherheitsmerkmal.

d) Denkbare Gegenmaßnahmen

Wachsame Mitarbeitende: Der beste Social-Engineering Angriff geht ins Leere, wenn Mitarbeitende wachsam und mit einem gesunden Maß an Misstrauen gegenüber plötzlichen Abweichungen vom bisherigen Ablauf ausgestattet sind. Denkbar sind interne Anweisungen, nach denen z. B. die in einer E-Mail behaupteten Gründe für Änderungen von Zahlungswegen immer mit dem Lieferanten zu verproben sind.

Gestufte Änderungsrechte: Je nach Kritikalität von Stammdaten sind gestufte Änderungsrechte bzw. Freigabemechanismen als Gegenmaßnahme denkbar. Das heißt, Änderungen an Daten wie beispielsweise eine USt-ID, eine IBAN, Zahlungsziele etc. dürfen nur von ausgewählten Personen/Abteilungen vorgenommen und freigegeben werden. Änderungen müssen protokolliert werden. Mehrfache Änderungen innerhalb weniger Stunden müssen einen Security Incident auf höherer Ebene auslösen.

Ergänzend soll erwähnt werden, dass im Bereich der sog. Kleinen und Mittleren Unternehmen teilweise noch Zahlungen über externe Software ohne Stammdatenmanagement anzutreffen ist. Gerade hier ist erhöhte Aufmerksamkeit der Mitarbeitenden essentiell, da aufgrund des manuellen Vorgehens automatisierte Kontrollen herausfordernd sind. Eine prozessuale Anpassung ist dringend geboten zur Minimierung des Risikos.

Gelebtes und forciertes Mehr-Augen-Prinzip: Bei der Freigabe von Rechnungen, Waren-/Serviceeingängen, Zahlungen und Datenänderungen ist ein systemseitig forciertes Mehr-Augen-Prinzip als Gegenmaßnahme denkbar. Je nach Art/Höhe/Auslöser der Änderung ist ggf. ein Sechs-Augen-Prinzip bzw. Freigabe durch bestimmte Leistungsebenen (Teamleitung, Abteilungsleitung, Bereichsleitung, …) notwendig.

Technische Ebene: Hier würden nur Lösungen in Gestalt von Signatur und Prüfsummen Abhilfe schaffen. Diese sind im E-Rechnungsstandard nicht vorgesehen; damit hat der Empfänger wohl gegenüber dem Lieferanten keinen Rechtsanspruch darauf. Allerdings ist fast jeder Lieferant wieder Empfänger von anderen Leistungen – vielleicht regelt das ja der Markt.

2. Fluten des ERP-Systems mit E-Rechnungen

a) Motivation der Täter/Schadensbild

Mit dem Fluten eines Systems sind Angriffe gemeint, die durch Überlastung eine Serviceunterbrechung herbeiführen sollen. Diese Angriffe werden auch denial-of-service (DOS) Angriffe genannt.[11] Ziel einer DOS ist, das angegriffene System lahmzulegen und das angegriffene Unternehmen damit zu schädigen. Die Angriffe werden erst eingestellt, wenn der Kriminelle eine erpresserische Geldzahlung erhalten hat.

Das Schadensbild kann je nach Integrationstiefe des ERP in die täglichen Abläufe zwischen dem Stillstand der kaufmännischen Abteilung über nicht funktionierende Zutritts-/Zugrisskontrollen bis hin zum Stillstand der Produktion wegen fehlender Ressourcen/Rohstoffe variieren.

b) E-Rechnung – der direkte Zugang zum ERP-System über das Internet

Durch die Pflicht zur Annahme von E-Rechnungen per E-Mail wird eine direkte Anbindung an das ERP-System über einen frei über das Internet erreichbaren Zugang geschaffen. Das heißt, der Zugang ist leicht und einfach erreichbar und kann mit unsinnigen Mails bzw. Mails mit betrügerischen E-Rechnungen geflutet werden. Während üblicher Spam durch etablierte Filtermaßnahmen hinreichend zuverlässig abgewehrt werden kann, sind kleine, kurze Mails mit einem XML-Anhang unverdächtig bzw. der Regelfall. Denn im Idealfall einer E-Rechnung reden Maschinen mit Maschinen; da sind weder Anreden noch Grußformeln üblich oder notwendig.

Geht ein Cyberkrimineller her und erzeugt für eine Stunde 1000 Mails pro Minute mit Absenderadressen wie „invoicing@dax-40-unternehmen.de“ oder mit erfundenen Absendernamen und flutet den E-Rechnungseingang sind verschiedene negative Szenarien denkbar.

- Szenario 1 – der E-Rechnungseingang ist nicht mehr möglich
- Szenario 2 – das ERP-System beschäftigt sich (fast) nur noch mit der E-Rechnung
- Szenario 3 – das ERP-System bricht zusammen

c) Auswirkungen eines nicht (vollumfänglich) einsatzbereiten ERP-Systems

Je nachdem, wie hoch der Integrationsgrad des ERP-Systems in das jeweilige Unternehmen ist, sind die Auswirkungen auf ein lahmgelegtes ERP-System unterschiedlich. Die Bandbreite der negativen Auswirkungen reichen von einer nicht handlungsfähigen kaufmännischen Abteilung über Störungen in der Zeiterfassung und/oder Zutrittskontrolle bis hin zu Auswirkungen in produktive Abteilungen.

Die finanziellen Schäden und Ausfallzeiten im Einzelfall sind folglich ebenfalls einer Bandbreite unterworfen. Ein laufendes ERP-System zu betreuen und warten ist an sich komplex; ein hochgradiges integriertes ERP-System im Fehlerfall ohne Datenverluste wieder lauffähig zu bekommen, ein zeitaufwändiges und kostenträchtiges Unterfangen.

Im Zusammenhang mit angegriffenen IT-Systemen beliefen sich die Gesamtkosten der deutschen Wirtschaft für das wieder Ingangsetzen von IT-Systemen und ausgefallener Erträge im Jahr 2024 auf rund 93,7 Mrd. Euro.[12]

d) Angriffe zu ungünstigen Zeiten und Erpressung

In einer perfiden Abwandlung findet das Fluten ggf. außerhalb der üblichen Bürozeiten oder am Wochenende statt. Sofern der E-Rechnungseingang nicht unter einer umfänglichen 24/7-Beobachtung steht, kann es am Montagmorgen zu einer bösen Überraschung in Gestalt eines nicht (vollumfänglich) einsatzbereiten ERP-Systems kommen.

Auch dieser Teilaspekt darf nicht außer Acht gelassen werden. Denn nach der Top 10 der häufigsten Fehler nach international anerkannten Standards (OWASP) in IT-Anwendungen stehen mangelnde Protokollierung und Überwachung auf den Plätzen 5 und 9.[13]

10 EZB, DIE Sicherheitsmerkmale der Euro-Banknoten, www.ecb.europa.eu/euro/pdf/material/A1_poster_secfeatures_de.pdf (Abruf: 19.2.2025).
11 BSI, DoS- und DDoS-Attacken, www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html (Abruf: 19.2.2025).
12 Bitkom, Studie „Wirtschaftsschutz 2024“, www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz (Abruf: 19.2.2025).
13 OWASP, OWASP Top Ten 2025, owasp.org/www-project-top-ten/ (Abruf: 19.2.2025).

e) Spamfilter und Säumnis

Ob klassische Methoden der Spam-Bekämpfung zielführend sind, muss sich zeigen. Zumal wegen der Pflicht zur Annahme von E-Rechnungen dann die Frage im Raum steht, ob eine verworfene E-Mail eine Meldepflicht an den Sender auslöst. Denn der Rechnungsabsender darf auf den Empfang und die Verarbeitung und Begleichung vertrauen. Ggf. tritt Säumnis und Mahnung ein.

Im Falle einer fehlerhaft verworfenen E-Rechnung (sog. false positive) stellt sich die Herausforderung, dass der Absender der Rechnung in der Lage sein muss, die Rechnung erneut senden zu können. Sonst fehlt die Rechnung im System des Empfängers oder die Rechnung muss als „andere Rechnung" manuell erfasst werden.

Für das eigene ERP-System heißt das auch, dass es in der Lage sein muss, E-Rechnungen ggf. erneut zu versenden, auch an andere Mailadressen, ohne dass die Rechnung an sich storniert und neu verarbeitet werden muss. Das Pendant in der analogen Welt ist der erneute postalische Versand einer Rechnung.

f) Denkbare Gegenmaßnahmen

Denkbar ist, dass der E-Rechnungseingang gegenüber dem ERP-System durch eine Zwischenkomponente verbunden ist (sog. Konnektor). Der Konnektor bietet die Möglichkeit, den E-Rechnungseingang bei Bedarf vom ERP-System zu trennen (Isolierung). Z. B. außerhalb der Bürozeiten, am Wochenende oder während eines Angriffs zum Fluten des Systems. Das heißt, eingehende E-Rechnungen werden nicht mehr automatisch weitergeleitet, sondern verbleiben in der Warteschlange im E-Rechnungseingang. Die Warteschlange kann bei Angriffen ggf. gesäubert werden, um einem Fluten entgegenzuwirken, oder mit einer gedrosselten Geschwindigkeit abgearbeitet werden.

Alle Aktionen müssen hinreichend protokolliert werden, um im Recherchefall den Aktionsablauf belastbar und lückenlos nachvollziehen zu können.

3. Manipulation ERP-Systems mittels E-Rechnungen

a) Wenn eine E-Rechnung mehr beinhaltet, als sie sollte

Die schädlichsten Angriffe auf IT-Systeme haben zum Ziel, das System dazu zu bewegen, von Außen eingeschleuste Anweisungen auszuführen. Im Ergebnis übernimmt der Angreifer damit (Teil-)Kontrolle über das System bzw. dessen Funktionen. Angriffe dieser Art heißen „Injection" (Einschleusungen) und sind auf Platz 3 der OWASP Top Ten 2025 zu finden.[14]

Ausgangspunkt dafür sind in der Regel freizugängliche Zugangspunkte, im vorliegenden Fall der E-Rechnungseingang. Hier können XML-Dateien eingeliefert werden, die definitiv vom System geöffnet, gelesen und verarbeitet werden. Komponenten, die Daten aus externen Quellen, hier über den E-Rechnungseingang, verarbeiteten, müssen gehärtet sein. Gehärtet bedeutet, dass auch fehlerhafte Daten nicht dazu führen, dass die Komponente „abstürzt" oder sich zu unerwünschtem Handeln verleiten lässt. Ungehärtete Komponenten tragen das Risiko, dass durch manipulierte XML-Dateien das ERP-System leicht und einfach von Außen angegriffen und, im schlimmsten Fall, lahmgelegt wird.

b) Denkbare Auswirkungen

Je nach Tiefenkenntnis des Angreifers über die Art des eingesetzten ERP-Systems und anderer IT-Komponenten können die Auswirkungen ein lahmgelegtes ERP-System, eine manipulierte Zahlungsanweisung oder sogar Zugriff auf das komplette System bedeuten.

Sofern die Komponente, die die eingehende XML-Datei liest und verarbeitet, für z. B. mehr als eine Funktion im IT-System genutzt wird, kann durch entsprechende Leitangaben die Komponente dazu gebracht werden, die XML-Datei nicht an die FiBu-Komponente, sondern an die Zugriffskontrollkomponente weiterzuleiten. In diesem Szenario könnte sich ein Angreifer durch eine manipulierte E-Rechnung Zugangskonten einrichten oder bestehenden Zugangskonten mit höheren Rechten ausstatten. Die daraus resultierenden Risiken und Schäden sind annähernd grenzenlos.

c) Denkbare Gegenmaßnahmen

Alle IT-Komponenten, die Daten von Außen erhalten, sind gehärtet. Inhaltlich fehlerhafte Daten oder fehlerhaft aufgebaute Daten müssen sicher verworfen werden.

Zentrale IT-Komponenten leiten Daten nicht quer zwischen einzelnen Teilbereichen. Eine über den E-Rechnungseingang eingelieferte XML-Datei darf z. B. nicht an das Berechtigungssystem weitergegeben werden. Ein- und Ausgabewege müssen definiert und gegeneinander isoliert sein.

Der zwischen E-Rechnungseingang und ERP-System geschaltete Koppler (siehe oben) kann denkbarerweise um eine Funktion erweitert werden, die die XML-Dateien auf fehlerhafte und/oder unplausible Daten hin überprüft.

Alle Aktionen müssen hinreichend protokolliert werden, um im Recherchefall den Aktionsablauf belastbar und lückenlos nachvollziehen zu können.

III. Fazit und Ausblick

Die E-Rechnung birgt große Möglichkeiten, den Digitalisierungsgrad in der Rechnungsabwicklung zu erhöhen. Mit der Digitalisierung ist es geboten, den neuen Risiken und den alten Risiken in neuen Gewändern durch Schulungen, Anleitungen und gehärteten IT-Systemen zu begegnen. Gerade unzureichende Dokumentationen erhöhen die Eintrittswahrscheinlichkeiten von Schäden, da ggf. nicht klar war oder ist, wer hätte wann was tun müssen.

Idealerweise werden mit Lieferanten Prozeduren abgesprochen, dass Änderungen von Zahlungswegen und -bedingungen stets außerhalb von Rechnungen erfolgen und nur im Rahmen von direkter Kontaktaufnahme erfolgen. Dies konterkariert auf den ersten Blick das Erhöhen des Digitalisierungsgrads. Tatsächlich trennt es die beiden unterschiedlichen Aufgaben „Abrechnen über eine Leistung" und „Änderung von Zahlungsdaten" sauber voneinander und unterwirft beide Aufgaben ihren eigenen Regeln.

Je nach dem, wie „mission critical" ein ERP-System ist, bieten sich technische Monitoring- und Isolierungseinrichtungen an, um Angriffe frühzeitig zu erkennen und ggf. verhindern oder abmildern zu können.

Die Autoren selbst präferieren ein zentrales Austauschsystem für Rechnungen, wie z. B. in Italien. Ohne auf die Einzelheiten des italienischen Systems einzugehen, verspricht ein zentrales Austauschsystem für Rechnungen einen authentifizierten und autorisierten Austausch

14 OWASP, OWASP Top Ten 2025, owasp.org/www-project-top-ten/ (Abruf: 19.2.2025).

von Rechnungen. Absender und Empfänger sind gleichermaßen authentifiziert und zum Stellen von Rechnungen autorisiert. Dadurch reduziert sich auch die Komplexität von Prüfsystemen, da der Austausch von Rechnungen auf ein einheitliches Format in einem einheitlichen Verfahren reduziert wird. Die notwendigen Investitionen der Wirtschaft stehen einem Gesamtschaden von 266 Mrd. Euro gegenüber und können als durchaus angemessen angesehen werden. Der Rückgang von Steuerschäden, 2,2 Mrd. Euro in Italien beim grenzüberschreitenden Handel im Jahr 2019[15], tritt dabei fast in den Hintergrund.

15 *Heinemann/Stiller*, Digitalization and cross-border tax fraud: evidence from e-invoicing in Italy, refubium.fu-berlin.de/handle/fub188/43130 (Abruf: 3.2.2025).

Patrick Bernd Findeis, StB, seit 1994 im deutschen Steuerrecht, begann Patrick Findeis bei der Finanzverwaltung und kam über die HeLaBa, PwC und KPMG Dubai zur BDO AG als Leiter Tax Technology; er vereint Steuerberater und Programmierer in seiner Person. Er beherrscht die Fachsprache der Steuer und die der IT. Verfahrensrecht, Grundsteuer, Datenverarbeitung und Datenvisualisierungen bilden seine Schwerpunkte.

Peter Braun, StB, seit 1996 im deutschen Steuerrecht, begann Peter Braun bei einer mittelständischen Kanzlei und ist aktuell bei der BDO AG tätig als Manager und Steuerberater im Bereich Tax Technology; seine Schwerpunkte sind die E-Rechnung, E-Commerce, Prozessberatung, Digitalisierung und Einsatz von künstlicher Intelligenz.