Corporate Treasury News

Aktuelle Entwicklungen und Trends im Bereich Treasury kompakt zusammengefasst

Ausgabe 149 | November 2024

Liebe Leserinnen und Leser,

wir freuen uns, Ihnen die neueste Ausgabe unserer Corporate Treasury News präsentieren zu können.

Wenn Sie Fragen oder Anregungen zu Themen haben, die hier kurz behandelt werden sollen, dann schreiben Sie uns: de-corporate-treasury@kpmg.com

Aktuelle Meldungen rund um das Finanz- & Treasury-Management finden Sie bei uns im Internet oder über Twitter.

Mit besten Grüßen

Ralph Schilling, Nils Bothe, Börries Többens

Unsere Leistungen für Sie! Schauen Sie rein:
FTM Image-Video

Inhalt

Veranstaltungen & Termine

Webinar zu Cashflow-at-Risk und Value-at-Risk im Treasury

Unter dem Titel *Navigating Financial Risk with CFaR and VaR* veranstalten KPMG und ION Treasury ein Webinar, in dem die Einsatzmöglichkeiten und Herausforderungen moderner Risikomaße im Corporate Treasury diskutiert werden.

Experten von KPMG und ION Treasury führen dabei unter anderem durch folgende Punkte:

- Grundlagen zu CFaR und VaR: Einblick in die Methodik und Herangehensweise
- Praktische Anwendung von at-Risk-Risikomaßen: Wie können Corporate Treasuries Risikomaße als gewinnbringende Werkzeuge im Risikomanagement, Hedging oder zur Investitionsentscheidung anwenden?
- Erfahrungen mit der Umsetzung: Welche Herausforderungen und aktuellen Trends gibt es bei der Einführung und Umsetzung entsprechender Konzepte – und auf welche Erfolgsgeschichten können wir zurückblicken?

Das Webinar richtet sich sowohl an Teilnehmer, die VaR und CFaR bisher nicht einsetzen und an grundlegenden Anwendungen interessiert sind, als auch an Zuhörer, die bereits Erfahrung mit den Konzepten haben und fortgeschrittene Einsatzmöglichkeiten betrachten möchten.

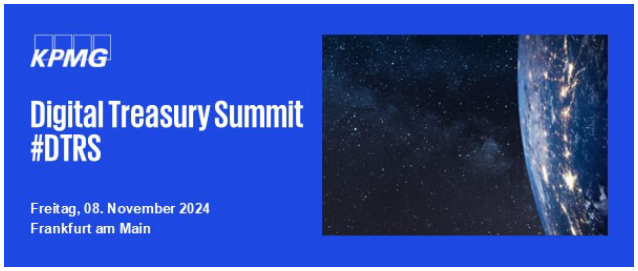
Datum: 26. November 2024
Uhrzeit: 16:00 CET
Registrierung: Link

Global Treasury Survey

Wir laden Sie herzlich dazu ein, an unserer Umfrage „Global Treasury Survey“ teilzunehmen.

Wie sind Corporate Treasury-Abteilungen in Unternehmen weltweit derzeit aufgestellt? Welche technischen Mittel werden bei der Arbeit eingesetzt und wie wird die Performance des Treasury gemessen? Ihr Input hilft uns, wertvolle Einblicke zu gewinnen und daraus Handlungsempfehlungen für Sie zu entwickeln, die wir in einem kostenfreien Whitepaper mit Ihnen teilen werden. Werden Sie Teil einer Analyse und Einwertung im globalen Kontext!

Digitale Entwicklungen eröffnen der Treasury-Funktion im Unternehmen neue Möglichkeiten



KPMG lud zum 9. Digital Treasury Summit nach Frankfurt ein.

Wenn sich die Corporate Treasury Community in den Frankfurter Geschäftsräumen der KPMG trifft, dann kann das nur eins bedeuten: Der nächste Digital Treasury Summit findet statt!

Über 100 Teilnehmer füllten am 08. November den großen Konferenzbereich am Frankfurter Flughafen. „Zusammenkommen, um mit Peers zu netzwerken, über den eigenen Tellerrand hinauszuschauen und mit neuen Ideen und vielfältigen Eindrücken wieder nach Hause zu fahren, das ermöglichen wir unseren Gästen mit diesem Event, das mittlerweile einen festen Platz im Kalender vieler Treasurer hat“, erklärt Nils Bothe, Partner im Bereich Finance & Treasury Management und Leiter der Abteilung Corporate Treasury Advisory.

Zusätzlich hatten wieder 10 Aussteller ihre Stände aufgebaut und informierten Interessierte über die neuesten Software-Entwicklungen für das Treasury.

Bild 1: Digital Treasury Summit 2024 /#DTRS2024
Quelle: KPMG AG

Wie jedes Jahr griffen die Vorträge an diesem kurzweiligen Tag neue Entwicklungen im Treasury Management auf. Die Möglichkeiten der Digitalisierung schreiten immer weiter voran und der Einsatz von Künstlicher Intelligenz eröffnet neue Perspektiven, die es zu erforschen und bewerten gilt.

Gherri D’Innocenzo, Head of Cash Management Payments, Standards & Projects bei Siemens gab einen spannenden Einblick, wie der Weg zum Real Time Treasury mittels Banking APIs aussehen kann und mit welchen Herausforderungen dabei zu rechnen ist. Gleich im Anschluss hielt Dr. Gerd Berghold, Head of Treasury Operations and Digital Treasury bei der Deutschen Bahn einen abwechslungsreichen Vortrag zu aktuellen Möglichkeiten der Digitalisierung, indem er verschiedene Anwendungsfälle lebendig beschrieb. Nach der Kaffeepause skizzierte Dr. David Saive, Special Advisor International Trade, Finance & Digitalization des Deutschen Nationalkomitees der Internationalen Handelskammer (ICC Germany e.V.) den Stand der Digitalisierung des internationalen Handels und der Handelsfinanzierung.

Im Anschluss starteten 3 Breakout Sessions mit jeweils 2 parallelen Vorträgen. In der ersten Session legten Julia Schlosser und Lasse Becker von SAP die Funktionsweise sowie die Vorteile einer Inhouse Bank und Payment Factory dar. Zeitgleich gaben Dr. Stefan Gröger und Julius Pfahl von der Prof. Schumann GmbH Einblicke in die Nutzung von KI zur Vorhersage des Geschäftsverhaltens im Zahlungsverkehr.

Bild 2: Interessierte Zuhörer
Quelle: KPMG AG

Nach der Mittagspause präsentierte Karel Cup von ION typische Herausforderungen von Treasury Analytics-Lösungen im Umfeld von Treasury-Management-Systemen. Anhand von konkreten Beispielen wie einem zentralen Zahlungsprozess oder der automatisierten FX-Sicherung illustrierte er die unterschiedlichen Anforderungen im operativen und Management-Berichtswesen und die Besonderheiten, die sich aus einer Umsetzung direkt im TMS oder alternativ in einem Data Lake/Enterprise Datawarehouse-Ansatz ergeben. Parallel dazu startete ein neues Format: Der Roundtable „Digitaler Euro“ bot den interessierten Teilnehmern nach einem kurzen Impulsvortrag die Möglichkeit mit KPMG-Expertin Anne-Sophie Gógl zu diskutieren. Dies führte zu einem intensiven Austausch, der sich bis in die anschließende Kaffeepause zog.

Den Vortrag in der letzten Breakout Session übernahm nach dem krankheitsbedingten Ausfall des ursprünglichen Referenten kurzfristig Dr. Dirk Bondzio, Risk Management-Experte und Teil des Finance & Treasury Management Teams der KPMG. Er stellte die Ergebnisse der von KPMG durchgeführten Umfrage „Resilient Treasury“ vor und erläuterte anschließend die wichtigsten Voraussetzungen, die ein krisensicheres und widerstandsfähig aufgestelltes Treasury, insbesondere in den Bereichen Risikomanagement und Liquiditätsplanung ermöglichen. Parallel gab es im Roundtable „KI im Finanzbereich und im Treasury“ mit KPMG-Partner und KI-Experte Andreas Fachinger erneut die Möglichkeit zum intensiven Austausch, die wieder rege genutzt wurde.

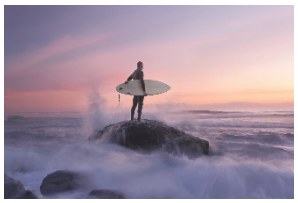
Den krönenden Abschluss bildete die Keynote von Prof. Dr. Christian Debus, der einen kurzweiligen Rückblick auf 30 Jahre Treasury warf, nicht ohne daraus Lehren für die Zukunft zu ziehen.

Genug Gesprächsstoff also, um anschließend noch einmal bei Kaffee & Kuchen beisammenzustehen. „Das viele positive Feedback zu der Veranstaltung und zu der angenehmen, familiären Atmosphäre bei uns freut uns sehr,“ berichtet Börries Többens, Partner, Finance & Treasury Management. „Dafür bedanken wir uns und laden alle Interessierten herzlich zum 10. Digital Treasury Summit im Herbst 2025 ein!“

Bild 3: Die Referenten, v.l.: Lasse Becker, SAP, Andreas Fachinger, KPMG, Dirk Bondzio, KPMG, Julius Pfahl, Prof. Schumann GmbH, Prof. Dr. Christian Debus, VDT, Gherri D’Innocenzo, Siemens, Dr. Gerd Berghold, Deutsche Bahn, Karel Cup, ION, Nils Bothe, KPMG, nicht im Bild: Julia Schlosser, SAP, Dr. Stefan Gröger, Prof. Schumann GmbH, Dr. David Saive, ICC Germany, Anne-Sopie Gógl, KPMG und Börries Többens, KPMG
Quelle: KPMG AG

Autoren:
Ralph Schilling, CFA, Partner, Head of Finance and Treasury Management, Treasury Accounting & Commodity Trading, KPMG AG
Nils Bothe, Partner, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG
Börries Többens, Partner, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG

Was Payment Gateways wirklich bringen



Mehrwert, Nutzen, Sicherheit

"Payment Gateways" (oder "Payment Hubs") werden immer wieder als Bestandteil einer modernen Zahlungsabwicklung beworben. Doch was genau verbirgt sich hinter dem Begriff? Für welche Unternehmen und Anwendungsfälle lohnt sich der Einsatz eines Payment Gateways wirklich? Welche Vorteile können erzielt werden? Was sollte beim Einsatz in Bezug auf bereits vorhandene Systeme und den Aspekt der Sicherheit beachtet werden?

Auf den Punkt gebracht

Ein Gateway bezeichnet in der IT eine Verbindung zwischen zwei oder mehreren Systemen in der Rolle des Vermittlers und meint

a) … **im Kontext des digitalen Zahlungsverkehrs im Handel:** die Abwicklung von elektronischen Zahlungen (meist Kreditkarten und Debitkarten) zwischen Käufern (Kunden) und Verkäufern (Händler), wobei das Gateway als Vermittler Zahlungstransaktionen an angebundene PSPs[1] und Acquirer[2] weiterleitet. (z.B. ACI, SPREEDLY, NUVEI, aber auch andere)[3]

b) … **im Kontext des klassischen Zahlungsverkehrs bei Corporates:** die Abwicklung von Finanztransaktionen auf Bankkonten bei Hausbanken vor allem für ausgehende Zahlungen (Lieferanten, Mitarbeiter, Ämter) aber auch eingehende Lastschriften (Kunden). Dabei stellt das Payment Gateway die Verbindung vom Unternehmen zur Bank her – ähnlich zu einem Electronic-Banking System. Dabei sind die Grenzen zum Treasury Management System (TMS) häufig fließend (z.B. SERRALA, TIS, OMIKRON, aber auch andere)[4]

Der folgende Artikel konzentriert sich dabei auf die Aspekte eines Payment Gateway im klassischen Zahlungsverkehr (b).

Die wichtigsten Features einfach erklärt

Ein Payment Gateway bindet auf der externen Seite die Hausbanken eines Unternehmens über die verfügbaren Kanäle EBICS, H2H, SWIFT (und mittlerweile API) an. Auf der internen Seite stellt er die Verbindung zu den ERP- und Accounting-Systemen her. Er sorgt damit für einen ersten wesentlichen Vorteil im Vergleich zum Einsatz von E-Banking-Systemen: den automatischen Upload von Zahldateien ohne manuelle Intervention (= Straight Through Processing). Weiterhin bietet ein Payment Gateway meist eine Formatbibliothek an, mit der Zahlungsinformationen von intern genutzten Schnittstellen-Formaten in landesspezifische und von den jeweiligen Banken anerkannte XML-Formate konvertiert werden.

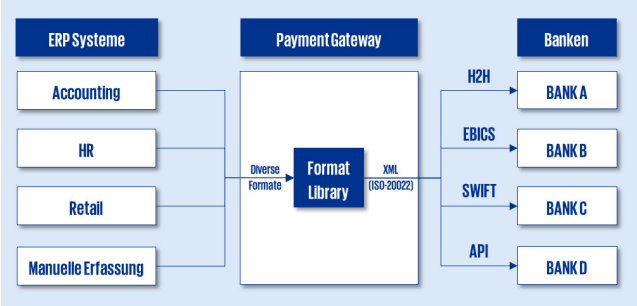


Abbildung 1: Systemlandschaft mit Payment-Gateway zum Versand von Zahldateien
Quelle: KPMG AG

[1] Ein *Payment Service Provider (PSP)* stellt die technische Infrastruktur für die Abwicklung bargeldloser Zahlungsmethoden an der Schnittstelle zum Endkunden bereit – sowohl online im E-Commerce (über den Checkout-Prozess) als auch im stationären Handel (über Zahlungsterminals).

[2] Ein *Acquirer* ist eine Bank oder ein Finanzdienstleister, der die Autorisierung und Abwicklung von Kartenzahlungen übernimmt und die Beträge auf die Bankkonten der Händler auszahlt.

[3] Die Auswahl der Anbieter wurde zufällig getroffen. Es handelt sich hierbei um illustrative Beispiele ohne Wertung hinsichtlich der Relevanz oder Kompetenz der jeweiligen Anbieter.

[4] Gleiche Anmerkung wie unter Fußnote 3.

Darüber hinaus bietet ein Payment Gateway typischerweise einen Umfang zusätzlicher Funktionalitäten, wie zum Beispiel (Liste nicht erschöpfend):

- die Verwaltung von Bank-Stammdaten
- die Verwaltung von Nutzern und Freigaberechten
- die Freigabe von Zahlungen
- die Nachverfolgung und Fehleranalyse von Zahlungen
- den Empfang von Kontoauszügen
- ein Reporting für Konten, Salden und Transaktionen
- gegebenenfalls eine Liquiditätsvorschau oder sogar Liquiditätsplanung

Das Gateway steht damit in direkter Konkurrenz zu den E-Banking-Systemen der Banken, die bei seiner Nutzung nur noch als Fallback oder für Spezialzahlungen benötigt werden. Ein Einsatz wirkt sich daher auch auf die Zusammenarbeit mit den Banken aus.

Zusammenarbeit mit Banken verändert sich

Im Payment Gateway werden zunächst Kontostammdaten bankübergreifend verwaltet. Das kann erstmals Transparenz über alle Bankkonten weltweit herstellen (sofern noch nicht vorhanden) oder zu einer Redundanz im Stammdaten-Management führen (wenn die Stammdaten bereits in ERP-Systemen erfasst sind). Bei der Nutzung von Corporate Seal können sogar Freigaberechte ohne Zutun der Bank administriert werden – oft ein großer Geschwindigkeitsvorteil bei der Anpassung von Limiten zum Beispiel für neue Mitarbeiter. Bei der Analyse von Fehlern in Zahldateien ist die Bank weiterhin gefragt aber das Gateway bringt auch hier Möglichkeiten zur Validierung von und Fehlersuche in Zahldateien mit.

Die zusätzlichen administrativen Aufgaben im Payment Gateway bringen zunächst mehr Aufwand und Verantwortung für die Treasury-Abteilung mit sich. Allerdings stärken die neuen Aufgaben auch die Wahrnehmung des Treasury als kompetenten Ansprechpartner der Tochtergesellschaften und Service-Funktion im Konzern.

Offensichtlich verändert ein Payment Gateway auch die Zusammenarbeit mit den Hausbanken. Manche Banken sehen sich durch den Einsatz in die Rolle eines reinen “Backends“ und Zahlungsabwicklers gedrängt oder ihre Relevanz bei Implementierungsprojekten schwindet, was mit einzelnen Häusern zu Verstimmungen führen kann. Andere Banken sorgen sich um Themen wie Haftung und Betrugsprävention oder lassen sich vertraglich weitergehende Rechte in Bezug auf die anlassbezogene Herausgabe von Daten (z.B. Log-Files zur Freigabe-Historie) zusichern. Die meisten Banken gehen jedoch proaktiv mit dem Trend um, unterstützen Kunden bei ihren Implementierungsprojekten oder schließen sogar Kooperationen mit Payment Gateways.

Auslagerung der Formatpflege spart Geld und beschleunigt IT-Projekte

Einige Payment-Gateways stellen bankenspezifische, länderspezifische und vorgetestete Zahlformate in Form einer Bibliothek (Payment Library) bereit. Somit ist das Gateway in der Lage, aus Zahlungsinformationen in unterschiedlichen internen Formaten (z.B. CSV, TXT oder IDOC aus einem ERP) ein valides XML-Zahlformat nach ISO-20022-Standard zu generieren. Dies bietet zahlreiche Vorteile:

- Wenn Zentralbanken neue Zahlarten einführen (z.B. Instant Payments, Realtime Payments oder Split Payments) können Zahlformate pro Bank schnell produktiv genommen werden.
- Bei der Ablösung von Altformaten (z.B. DTAZV) und der Einführung des ISO-Standard sind Formatbibliotheken hilfreich, da sie die technische Migration beschleunigen und vereinfachen.
- Zudem können neue Zahlläufe schneller umgesetzt und damit zusätzliche Zahlvorgänge in der Buchhaltung automatisiert werden.

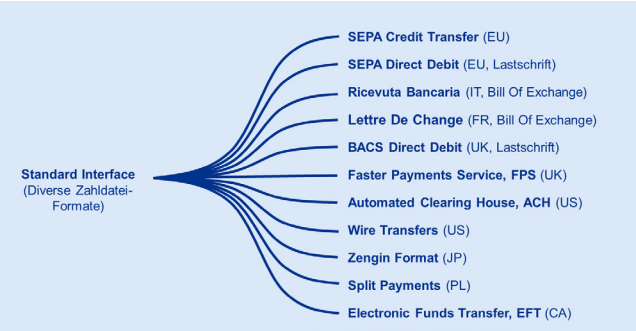


Abbildung 2: Formatbibliothek eines Payment-Gateway
Quelle: KPMG AG

Zwar bieten auch ERP-Systeme in gewissem Maß Vorlagen für landesspezifische Zahldatei-Formate – diese sind aber mit einem Customizing-Aufwand an die Formatspezifikationen der jeweiligen lokalen Banken anzupassen. Vor allem fällt der initiale Format-Test gemeinsam mit der Bank umfangreicher aus und hängt von der Verfügbarkeit der bankseitigen Implementation-Managern ab. Auch die Verantwortung und der Aufwand für die Pflege und Wartung der Formate liegt in der IT-Abteilung des Unternehmens. Mit den vorvalidierten und automatisch gewarteten Formaten einer Payment Library hingegen kann interner IT-Aufwand eingespart und effizient zum Dienstleister ausgelagert werden.

Abzugrenzen sind Auslagerungen, die über die Formatpflege und das E-Banking und damit das Funktionsspektrum eines Payment Gateway hinausgehen. Für eine Auslagerung des kompletten Zahlungsverkehrs inklusive der Befüllung und Vorbereitung von Zahldateien für Vendor-Payments oder komplexe HR-Zahlungen sowie deren Verbuchung und die Überwachung des Settlement sind wiederum andere Anbieter erforderlich (z.B. ADP, Bottomline Technologies, PAYONEER, DATEV, aber auch andere)[5].

Verbesserung der Governance und Gebühreneinsparungen

Mit der Zentralisierung der Bankstammdatenverwaltung. Bankanbindung, Kontenadministration und Zahlungsabwicklung schafft das Payment Gateway automatisch eine stärkere Abhängigkeit der Tochtergesellschaften von der Zentrale. Dies verbessert die Übersicht über lokale Bankkonten und Freigaberechte, erleichtert die Durchsetzung einheitlicher Limite und zwingt die Töchter zur stärkeren Abstimmung mit der zentralen Treasury-Abteilung bei der Eröffnung und Schließung von Bankkonten. An einer derartigen Verbesserung der Governance dürfte nicht zuletzt der CFO stark interessiert sein. Zudem kann mit der Zentralisierung die Grundlage für ein späteres Shared-Service-Center (Payment Factory) gelegt werden.

Auf der Kostenseite stehen den Einsparungen bei der Formatpflege und dem Effizienzgewinn durch einen vereinheitlichten Admin-Prozess zunächst die Kosten für die Software-Subscription einer weiteren Cloud-Plattform entgegen. Zusätzlich stärkt ein Payment Gateway jedoch den Wettbewerb zwischen den Banken in Bezug auf:

- die Zuverlässigkeit und Dauer der Zahlungsausführung
- die Einführung neuer Zahlarten
- und nicht zuletzt das Pricing.

Der Wechsel eines Bankkontos hin zu einer besseren oder günstigeren Bank ist nach wie vor mit Aufwand verbunden aber in Bezug auf das technische Setup in einem Payment Gateway deutlich schneller und einfacher. Bei hohen Transaktionsvolumen sollten sich die Fixkosten für die Softwaremiete daher mittelfristig amortisieren.

Welche Risiken gibt es – und wie kann man ihnen begegnen?

Die technische Zahlungsfähigkeit eines Unternehmens in die Hände eines Cloud-Anbieters zu legen, könnte zunächst nachvollziehbare Bedenken bei einem verantwortungsvollen Treasurer hervorrufen – zum Beispiel in Bezug auf die Datensicherheit, das Provider-Risiko und die Kontrolle über den Zahlungsverkehr.

Um trotzdem in den Genuss der Vorteile zu kommen, können **operative Risiken** zunächst durch die Auswahl eines passenden Anbieters begrenzt werden, der die erforderliche Verfügbarkeit und Zuverlässigkeit garantiert (Failover, Backup, Limitierung der Downtimes) – am besten nachweislich mit einem passenden SLA (Service Level Agreement) und einer ISO-Zertifizierung. Bei genauerer Betrachtung wird man dabei erkennen, dass sich das Ausfallrisiko und die Verfügbarkeit des Supports bei den meisten Anbietern heute auf einem Niveau ähnlich dem von Banken bewegt.

Die Einhaltung des Datenschutzrechts (GDPR, DSGVO) und die **Datensicherheit** wird von Behörden in Unternehmen bekanntlich mittels hoher Strafen vehement durchgesetzt und ist heute breit im öffentlichen Bewusstsein angekommen. Dies lässt dem Schutz personenbezogener Informationen im Zahlungsverkehr (z.B. Bankverbindungen) oder gar sensibler Daten (z.B. Gehaltszahlungen) eine besondere Rolle zukommen. Auslagerungsunternehmen wie Payment Gateways treffen dafür in der Regel Vorkehrungen im Vertragswerk und den Prozessen. Aber auch das Treasury sollte hierzu Maßnahmen ergreifen – z.B. in Form von:

- eines Berechtigungskonzepts
- klaren Vorgaben und Schulungen für Admins
- Freigabeprozessen
- und einer Dokumentation

Zudem sollte eine Tochtergesellschaft, welche die Zentrale mit der Abwicklung des Zahlungsverkehrs beauftragt, diese Aufgabe initial mit geeigneten Verträgen delegieren, um eine rechtliche Basis für die Zentralisierung zu schaffen. Eine Auslagerung ist weiterhin ein guter Anlass, sich einmal grundlegend mit Datenschutz und Datensicherheit zu befassen, um den Missbrauch sensibler Nutzerdaten zu verhindern.

[5] Die genannte Auswahl von Anbietern, die als Auslagerungspartner für weiterer Teile des Zahlungsverkehrs fungieren können, wurde zufällig getroffen. Es handelt sich hierbei um illustrative Beispiele ohne Wertung hinsichtlich der Relevanz oder Kompetenz der jeweiligen Anbieter.

Cybersicherheit im Zahlungsverkehr

Neben den bereits genannten Risiken dürfte auch das Thema **Cybersicherheit** in Zusammenhang mit Payment Gateways einige Bedenken aufwerfen. Cyberangriffen sind zunächst alle am Prozess des Zahlungsverkehrs beteiligten Parteien in ähnlichem Maß ausgesetzt:

- **Banken (und auch Zentralbanken):**
  Banken stehen besonders im Fokus von Cyber-Attacken aber unterliegen auf der anderen Seite einem hohen regulatorischen Druck. Neue Gesetze wie die Verordnung DORA (Digital Operational Resilience Act) machen strenge Vorgaben zur Cybersicherheit und zwingen die Banken zu hohen Investitionen in Sicherheit und Betrugserkennung. Diese sind auf der anderen Seite auch erforderlich, um eine komplexe und umfangreiche Infrastruktur und Organisation zu schützen.
- **Cloud-Anbieter (Payment Gateways oder Treasury-Management-Systeme):**
  Cloud-Anbieter haben bei geringerer Größe auch geringere Budgets zur Verfügung. Andererseits sind sie als Technologieführer am besten in der Lage, sich mit technischen Maßnahmen gegen Bedrohungen zu schützen (Authentisierung, Verschlüsselung, Dynamische IP-Adressen, usw.). Sie unterliegen zwar nicht den strengen Gesetzen der Aufsichtsbehörden aber durchlaufen meist Zertifizierungen zur Informationssicherheit (wie zum Beispiel ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 oder SOC 2, um nur einige zu nennen). Cloud-Anbieter schaffen es daher immer wieder, Cyberangriffe erfolgreich abzuwehren[6].
- **Corporates (mit einer On-Premise-Installation des ERP oder TMS):**
  Das schwächste Glied in der Kette dürften leider noch oft die Unternehmen selbst sein, wenn sie nicht ausreichend in Cybersicherheit investieren, Notfallpläne vorhalten oder IT-Security-Zertifizierungen durchführen. Durch die Speicherung sensibler Daten zum Zahlungsverkehr in ERP-Systemen, E-Mail-Programmen oder Folder-Strukturen sind die Unternehmen einem hohen Risiko ausgesetzt.

Wenn ein Unternehmen über die Erhöhung der IT-Sicherheit im Zahlungsverkehr nachdenkt, dürfte somit eine Auslagerung von weiteren Prozessen zu Cloud-Anbietern oft sogar eine Verbesserung im Vergleich zum Status Quo darstellen.

Schlüsselentscheidungen für eine zukunftsfähige Payment-Strategie

Zusammenfassend erschließt ein kluges IT-Setup des Zahlungsverkehrs finanzielles Potenzial und ist ein wichtiger Stellhebel für Verbesserungen. Vor dem Start größerer Zahlungsverkehrs-Projekte kann es deshalb sinnvoll sein, sich (neben der Bankenstrategie) über die konkrete Payment-Strategie Gedanken zu machen und zum Beispiel folgende Fragen zu klären:

- **Formatentwicklung:**
  Make or Buy?
- **Administration von Limiten:**
  Inhouse oder bei Banken?
- **Governance:**
  Zentralisierung oder Dezentralisierung des Zahlungsverkehrs?
- **Stellenwert von Sicherheit:**
  Manuelle Schnittstellen oder Automatisierung?

Die nächste ERP-Migration oder ein Projekt zur Ablösung von Altformaten könnten zum Beispiel ein guter Anlass sein, sich einmal grundlegend mit der Payment-Strategie zu beschäftigen und die IT-Landschaft einem Review zu unterziehen – vor allem hinsichtlich des Einsatzes eines Payment Gateways.

Autoren:
Nils Bothe, Partner, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG
Sascha Uhlmann, Senior Manager, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG

---

[6] Amazon Web Services (AWS) ist ein exemplarischer Vertreter der Branche und setzt zahlreiche innovative Tools im Bereich Früherkennung, Abwehr und Schutz vor Cyberattacken ein. AWS zufolge konnten mithilfe dieser Tools bereits zahlreiche Angriffe abgewehrt werden. („In the first quarter of 2023 […] we stopped over 1.3M outbound botnet-driven DDoS attacks")

Quelle: Ryland, M. (2023, September 28). How AWS threat intelligence deters threat actors. AWS Security Blog. Verfügbar unter: https://aws.amazon.com/de/blogs/security/how-aws-threat-intelligence-deters-threat-actors

Ransomware-Erpressungszahlungen erreichen neue Rekordwerte: Wie sich Treasuryabteilungen auf das Worst-Case-Szenario vorbereiten können

Parallel zu einer immer stärker vernetzten Welt nehmen auch die Versuche von Ransomware-Angriffen auf Unternehmen immer weiter zu und die Summe an Erpressungszahlungen erreichte im letzten Jahr neue Rekordwerte.[7]

Unter einem Ransomware-Angriff versteht man dabei die Verschlüsselung von Daten eines Unternehmens und die Erpressung von Lösegeldzahlungen zur Entschlüsselung.

Finanzabteilungen sind dabei ein attraktives Ziel für Cyberkriminelle, da es hier sensible Finanzdaten zu erbeuten gibt und geschäftskritische Prozesse wie der Zahlungsverkehr behindert oder unterbunden werden können. Bei einem Ransomware-Angriff sind eben diese Datenmengen im ersten Schritt das Ziel von Angriffen und es kommt üblicherweise zu einer Verschlüsselung von einzelnen Dateien, ganzer Laufwerke oder zur Blockierung des Zugangs zu Applikationen. Ein erfolgreicher Ransomware-Angriff kann dementsprechend nicht nur zu erheblichen finanziellen Verlusten führen, sondern auch das Vertrauen der Kunden, Lieferanten und Investoren in das Unternehmen beeinträchtigen. Das führt zu einem sehr hohen Schadenpotenzial.

Zusätzlich zu präventiven Maßnahmen, um sich vor Ransomware-Angriffen zu schützen, sollten Unternehmen daher eine Business-Continuity-Strategie ausarbeiten, um selbst für den Schadensfall vorbereitet zu sein. Strukturen zu schaffen, welche auch unter schwierigen Bedingungen die betriebliche Kontinuität sicherstellen oder wiederherstellen, kann das Ausmaß des Schadens erheblich verringern.

Methoden und Arten der Angriffe

Bei einem Ransomware-Angriff wird der Zugriff auf die internen Daten eines Unternehmens durch eine Verschlüsselung blockiert. Dabei kommen sowohl ein öffentlicher als auch ein privater Key zum Einsatz, die zum Verschlüsseln bzw. Entschlüsseln der betreffenden Daten verwendet werden. Der öffentliche Key wird an die Opfer des Angriffs gesendet, während der private Key nur den Angreifern bekannt ist. Auf diese Weise können die Angreifer die Daten verschlüsseln, ohne dass die Opfer in der Lage sind, sie zu entschlüsseln, es sei denn, sie zahlen eine geforderte Lösegeldsumme. Wenn das Lösegeld nicht innerhalb der Frist gezahlt wird, besteht die Bedrohung und die resultierende Gefahr, dass die Angreifer den privaten Schlüssel löschen, wodurch eine Entschlüsselung der Daten in der Regel unmöglich gemacht wird.

Die Angriffe können sowohl von gut organisierten Hackergruppen als auch von Einzelpersonen ausgehen. Eine Studie, welche die auf europäische Unternehmen erfolgten Ransomware-Angriffe ausgewertet hat, sieht folgende typische Vorgehensweise:[8]

Zuerst kommt der „Reconnaissance“-Schritt, wobei die Angreifer die Schwachstellen im Informationssystem und den Schnittstellen vom Unternehmen sammeln. Sobald diese Punkte erkannt und die geeignete Angriffsmethode ausgewählt wurden, wird ein entsprechendes Skript über verschiedene Kanäle an das Unternehmen weitergeleitet und versucht, es zum Herunterladen in interne Systeme zu verleiten. Das heruntergeladene Skript sorgt dafür, dass die Angreifer eine Fernkontrolle auf das interne System erhalten und danach die beabsichtigte Verschlüsselung der nicht öffentlichen Daten durchführen.

Alternativ zu dem gezielten Angriff auf Einzelunternehmen bestreiten Hackergruppen regelmäßig den gegenteiligen Weg und attackieren eine Vielzahl von Unternehmen durch die Weiterleitung von entsprechenden Skripten, beispielsweise via E-Mail, um im Nachgang zu prüfen, ob ein Download ins Informationssystem erfolgt ist.

Häufigkeit in Deutschland und Europa

Allein in Deutschland wurden gemäß einer Veröffentlichung vom Bundeskriminalamt im Jahr 2023 von

[7] Vgl. Ransomware-Zahlungen erreichen Rekordhoch – DerTreasurer.

[8] Vgl. The Ransomware Landscape in Europe, European DIGITAL SME Alliance.

mehr als 800 Unternehmen bzw. Institutionen Anzeigen hinsichtlich Ransomware-Angriffen bei der Polizei gemeldet[9], und laut einer EU-Studie[10] ist Deutschland nach den Vereinigten Staaten das weltweit am häufigsten betroffene Land für Ransomware-Angriffe. Die jährliche bundesweite Studie des Bundesamts für Sicherheit in der Informationstechnik aus dem Jahr 2023 zeigt ebenfalls , dass bei den sogenannten Angriffen mit „doppelter Erpressung“ (wobei die Daten nicht nur verschlüsselt werden, sondern auch gedroht wird, dass es zur Datenveröffentlichung kommt) die größte Anzahl an mutmaßlichen Opfern aus Deutschland in einem einzigen Jahr identifiziert wurde und sich die Summe im Vergleich zum Jahr 2022 verdoppelt hat. Die Angriffe beschränkten sich dabei nicht auf einen bestimmten Wirtschaftssektor, sondern stellten eine Bedrohung für Unternehmen verschiedenster Branchen und Größen dar (siehe dazu Abbildung 1), wobei mittelständische Unternehmen statistisch betrachtet, am stärksten betroffen waren.

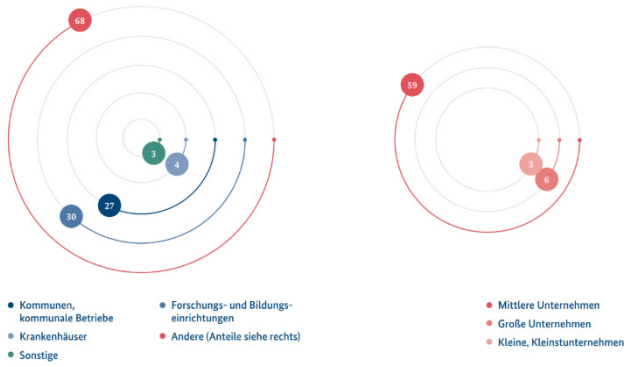


Abb. 1: „Bekannt gewordene Ransomware-Opfer in Deutschland im Berichtszeitszeitraum [2023] nach Art des Opfers“[11] Quelle: Bundesamt für Sicherheit in der Informationstechnik

Mögliche Maßnahmen für Finanzabteilungen

Die steigende technische Komplexität der Treasury-Abteilungen bedeutet, dass die möglichen Quellen solcher Angriffe schwer vollständig aufzulisten sind. Insbesondere können nicht optimal gesicherte APIs, also Programmierschnittstellen, ein Einfallstor für Schadsoftware darstellen[12]. Darüber hinaus werden täglich im Durchschnitt eine Viertelmillion neue Varianten von Schadprogrammen identifiziert, die bei solchen Angriffen in Verwendung kommen und über verschiedene Wege in das technische System der Unternehmen gelangen können.[13] Die Firewall eines Unternehmens, also eine Software, welche den Datenfluss zwischen internen und externen Netzwerken kontrolliert, unterliegt somit einer ständig veränderten Prüfung. Auch menschliche Fehler, wie beispielsweise das Öffnen von Phishing-E-Mails oder das Herunterladen von infizierten Dateien, können zu einem erfolgreichen Angriff führen.

Es ist daher von entscheidender Bedeutung, dass Treasury-Abteilungen angemessene Sicherheitsmaßnahmen ergreifen, um sich vor Ransomware-Angriffen zu schützen. Eine Hauptkomponente der IT-Systemlandschaft einer Treasury-Abteilung besteht dabei in der Implementierung des Treasury-Management-Systems, welches ebenso wie die dazugehörigen Schnittstellen regelmäßig aktualisiert und hinsichtlich ihrer Sicherheit geprüft werden sollte.

Zum Schutz sollten Unternehmen auch andere Maßnahmen ergreifen: Eine Möglichkeit ist, regelmäßige Backups ihrer Daten zu erstellen und diese an einem sicheren Ort aufzubewahren. Insbesondere im Bereich Zahlungsverkehr ist es nicht unüblich, regelmäßig Spiegelungen vom produktiven System zu machen und diese auf einen Disaster-Recovery-Server zu überführen.

Dadurch können sie im Falle eines Angriffs ihre Daten ganz oder zumindest teilweise wiederherstellen, ohne auf die Zahlung von Lösegeld angewiesen zu sein. Trotzdem sollte die Sicherheit solcher Backups immer wieder überprüft und aktualisiert werden, da die Ransomware-Angriffe ebenfalls versuchen, die Wiederherstellung der Daten durch Backups zu gefährden: Laut dem diesjährigen Ransomware-Report von Sophos, einem Entwickler für Sicherheitssoftware, haben 94% der durch Ransomware angegriffenen Unternehmen gemeldet, dass die Angreifer ebenfalls ihre Backups verschlüsseln wollten[14]. Eine Möglichkeit ist hier ein Offline-Backup vorzuhalten[15], damit das Unternehmen selbst für nicht funktionierende Cloud-Backups gerüstet ist.

---

[9] Vgl. EU-Agentur für Cybersicherheit (Daten von Juli 2021 bis Juli 2022), Europäische Union, 2022.

[10] Vgl. Die Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik.

[11] ebd.

[12] Vgl. Unsichere APIs sorgen für Milliardenschäden, der Treasurer, 29. Juni 2022.

[13] Vgl. Die Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik.

[14] Vgl. The State of Ransomware 2024, Sophos, April 2024.

[15] Vgl. Maßnahmenkatalog Ransomware, BSI, 2022.

Eine weitere Schutzmaßnahme ist es, die IT-Systeme des Unternehmens regelmäßig zu aktualisieren und zu patchen, um Schwachstellen zu schließen und Angriffe zu verhindern. Unternehmen sollten auch Schulungen für ihre Mitarbeiter durchführen, um sie über die Risiken von Ransomware-Angriffen zu informieren und sie zu sensibilisieren. Durch eine Kombination dieser Maßnahmen können Unternehmen ihre Chance erhöhen, Ransomware-Angriffe abzuwehren und ihre Daten zu schützen. Nach BSI-Statistiken von August 2022 repräsentierten Spam-Nachrichten etwa 34% aller E-Mails in der Wirtschaft in Deutschland, was besonders hervorhebt, wie essenziell der Schutz gegen diese Angriffe ist[16].

Angegriffen – was nun?

Wenn aber alle diese Maßnahmen nicht ausreichend waren und ein Angriff auf das Unternehmen erfolgreich durchgeführt wurde, bleibt die Frage, ob das gewünschte Lösegeld bezahlt werden sollte. Laut einer europaweiten Studie haben ungefähr 60% der angegriffenen Unternehmen sich entschieden, das Lösegeld zu bezahlen, um wieder auf ihre Daten bzw. ihre IT-Infrastruktur zugreifen zu können[17]. Dasselbe ist insbesondere vor dem Hintergrund erstaunlich, dass selbst eine Lösegeldzahlung die Entschlüsselung der Dateien nicht garantiert, und weiter das Risiko eines Verlustes bzw. einer Veröffentlichung von betriebsinternen Daten besteht.

Bei der Entscheidung bezüglich der auf den Angriff folgenden Reaktion spielt auch die geografische Lage der betroffenen Organisation eine entscheidende Rolle, da je nach Land unterschiedliche regulatorische Vorschriften zu berücksichtigen sind. In den Vereinigten Staaten könnte eine solche Zahlung beispielsweise als Terrorismusfinanzierung eingestuft werden, weshalb hier der rechtliche Rahmen vorab geprüft werden sollte. Striktere Regelungen oder Einschränkungen von Ransomware-Zahlungen könnten außerdem in der Zukunft in vielen Ländern eingeführt werden. Die Organisation „International Counter Ransomware Initiative“, die zurzeit mehr als 40 Länder beinhaltet, setzt sich für härtere Gesetze gegen solche Zahlungen ein, da dadurch Anreize für solche Angriffe geschaffen werden. Bis dahin bleibt es aber die individuelle Entscheidung der betreffenden Unternehmen, einzuschätzen, ob eine Lösegeld-Zahlung oder der Schaden ohne Zahlung für das Unternehmen das kleinere Übel darstellt.

Sollte ein Unternehmen dabei eine Lösegeldzahlung nicht kategorisch ausschließen, sollte es sich im Rahmen der Business-Continuity-Strategie auch mit Kryptowährungen beziehungsweise mit den Verwahrstellen von Kryptowährungen, sogenannten Wallets, befassen. Kryptowährungen werden oft als Zahlungsmittel für Lösegeldforderungen verwendet. Cyberkriminelle nutzen Kryptowährungen aufgrund ihrer dezentralen Natur und Anonymität, um Zahlungen zu erhalten, ohne sofort identifiziert zu werden. Hier sollte geprüft werden, ob bereits vorab Strukturen geschaffen werden, um Zahlungen in Kryptowährungen für das Unternehmen durchführen zu können. Einige Unternehmen gehen hier sogar so weit, bereits bestimmte Kryptowährungen vorzuhalten, um im Schadenfall diese nicht kurzfristig beschaffen zu müssen und sicherzustellen, dass diese Möglichkeit als eine Stand-Alone-Lösung auch ohne klassischen Zahlungsverkehr existiert.

Autoren:
Börries Többens, Partner, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG
Marvin Berning, Manager, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG

[16] Vgl. Ausgabe 08/2022: E-Mails und Spam-E-Mails in der Wirtschaft in Deutschland, BSI.

[17] Vgl. EU-Agentur für Cybersicherheit (Daten von Juli 2021 bis Juli 2022), Europäische Union, 2022.

Änderungen am IFRS 9 und IFRS 7: Neue Leitlinien zur Klassifizierung, Bewertung und Offenlegung von Finanzinstrumenten

Die jüngsten Anpassungen am IFRS 9 und IFRS 7, die das International Accounting Standards Board (IASB) veröffentlicht hat, sollen dazu beitragen, die Klassifizierung, Bewertung und Offenlegung von finanziellen Vermögenswerten und Verbindlichkeiten zu präzisieren. Diese Änderungen basieren auf einem *Post-implementation Review* des IFRS 9, der 2022 abgeschlossen wurde. Obwohl das IASB feststellte, dass der Standard im Wesentlichen wie vorgesehen funktioniert, wurden dennoch Vorschriften identifiziert, die aufgrund von neuen Entwicklungen seit Inkrafttreten des Standards sowie der Rückmeldung von Stakeholdern eine Überarbeitung erforderten.

Ein zentraler Aspekt der Änderungen betrifft die Klassifizierung finanzieller Vermögenswerte durch das sogenannte SPPI-Kriterium (*Solely Payments of Principal and Interest*), welches festlegt, unter welchen Bedingungen finanzielle Vermögenswerte zu fortgeführten Anschaffungskosten und nicht zum beizulegenden Zeitwert zu bewerten sind. Laut SPPI-Kriterium müssen die vertraglichen Zahlungen eines Vermögenswerts ausschließlich aus Tilgungs- und Zinszahlungen bestehen, die auf den ursprünglichen Kapitalbetrag entfallen. Dabei steht die Beurteilung von Zinsbestandteilen in grundlegenden Kreditverträgen im Fokus der Veränderungen, wonach die aktualisierten Leitlinien des IASB zum IFRS 9 nun präzisere Hinweise darauf enthalten, wie Zahlungsströme zu betrachten sind, die sich ausschließlich aus Tilgungs- und Zinszahlungen zusammensetzen und auf den verbleibenden Kreditbetrag entfallen. Zu den typischen Zinskomponenten zählen dabei etwa der Zeitwert des Geldes, potenzielle Ausfallrisiken sowie grundlegende Risiken bei Kreditkontrakten, wie das Liquiditätsrisiko. Auch eine mögliche Gewinnmarge des Kreditgebers kann hier berücksichtigt werden. Wichtig ist hierbei vor allem, dass nicht die Höhe des Entgelts im Vordergrund steht, sondern dass die Zahlungen mit den grundlegenden Risiken und Kosten des Kreditgeschäfts im Einklang stehen. Das bedeutet, dass Zinsen nur dann als Teil einer klassischen Kreditbeziehung gelten, wenn sie hauptsächlich als Entschädigung für die Kreditrisiken und -kosten des Unternehmens angesehen werden. Zahlungen, die diese Anforderung nicht erfüllen oder die grundsätzlich an Variablen gekoppelt sind, die nicht mit den grundlegenden Kreditrisiken oder -kosten einhergehen – etwa Marktbedingungen oder externe Indizes – erfüllen nicht die Kriterien für eine solche Kreditvereinbarung.

Zudem wurden im Zuge des Zahlungsstromkriteriums die Regelungen für Vertragsbedingungen, die den Zeitpunkt oder die Höhe der Zahlungen ändern können überarbeitet. Besonders relevant sind dabei Darlehen, die ESG-bezogene Klauseln enthalten, welche nicht direkt mit Veränderungen der zugrunde liegenden Kreditrisiken zusammenhängen. In Zukunft sind Unternehmen verpflichtet, unter Umständen sowohl qualitative als auch quantitative Analysen durchzuführen, die auf die Signifikanz solcher Klauseln einzahlen, und zwar unabhängig davon, wie wahrscheinlich diese Änderungen eintreten. Konkret bedeutet das, dass finanzielle Vermögenswerte, bei denen zum Beispiel ESG-bezogene Klauseln in den Vertragsbedingungen enthalten sind, zu fortgeführten Anschaffungskosten bewertet werden können, sofern diese keine wesentlichen Auswirkungen auf die vertraglichen Zahlungsströme vorweisen. Informationen über die Auswirkungen solcher Vertragsklauseln sind zudem wie folgt offenzulegen:

- Eine Beschreibung des Ereignisses, das eine Änderung in der Höhe der vertraglichen Zahlungen bedingt.
- Bruttobuchwerte der finanziellen Vermögenswerte und Verbindlichkeiten.
- Quantitative Angaben zu den potenziellen Veränderungen der Zahlungsströme.

Das Ziel des Standardsetters besteht darin, Transparenz zu schaffen und den Adressaten der Finanzberichterstattung die Möglichkeit zu bieten, die Auswirkungen dieser bedingten Ereignisse hinreichend genau nachzuvollziehen.

Ein weiterer Punkt, der durch die Änderungen des IFRS 9 genauer definiert wurde, betrifft die sogenannten nicht rückgriffsberechtigten finanziellen Vermögenswerte (*non-recourse*). Der Begriff "nicht rückgriffsberechtigt" bezieht sich auf Finanzierun-

gen, bei denen der Gläubiger nur auf die Zahlungsströme aus bestimmten, im Vertrag festgelegten Vermögenswerten zugreifen kann. Ein Zugriff auf andere Ressourcen des Schuldners ist dabei ausgeschlossen. Die neuen Regelungen stellen nun klar, dass eine Finanzierung nur dann als "nicht-rückgriffsberechtigt" eingestuft werden darf, wenn die Vertragsbedingungen das Recht des Gläubigers auf die Zahlungsströme dieser speziellen Vermögenswerte beschränken. In der Vergangenheit gab es bei vertraglich verknüpften Instrumenten oft Unklarheiten hinsichtlich der Abgrenzung von Non-Recourse-Finanzierungen. Diese Unsicherheiten führten in einigen Fällen zu unterschiedlichen Ergebnissen bei der Anwendung der entsprechenden Vorschriften. Um diesem Problem entgegenzuwirken, hat das IASB die Anwendungsrichtlinien jetzt präzisiert. Ziel dieser Klarstellungen ist es, eine eindeutige Unterscheidung zu ermöglichen und eine konsistente Anwendung des Standards zu gewährleisten.

Grundsätzlich ist ein finanzieller Vermögenswert auszubuchen, sobald das vertragliche Recht auf den Einbezug von Zahlungsströmen erlischt oder der Vermögensgegenstand übertragen worden ist. Eine Verbindlichkeit wird zum Zeitpunkt ihrer Erfüllung ausgebucht. Neue Vorschriften zur Ausbuchung finanzieller Verbindlichkeiten, die durch elektronische Zahlungssysteme beglichen werden, stellen außerdem klar, dass in bestimmten Fällen Unternehmen die Möglichkeit haben, eine Verbindlichkeit – oder einen Teil davon – bereits auszubuchen, auch wenn das Geld „noch unterwegs“ ist und die Verbindlichkeit somit noch nicht erfüllt wurde.

Eine weitere Änderung betrifft zudem die Offenlegungspflichten für Eigenkapitalinstrumente, die zum beizulegenden Zeitwert bewertet und als erfolgsneutral klassifiziert werden. Unternehmen sind verpflichtet, den Gewinn oder Verlust aus der Bewertung dieser Instrumente detaillierter darzustellen. Dies umfasst unter anderem eine Differenzierung von Beträgen, die einerseits auf ausgebuchte und anderseits auf noch gehaltene Anteile entfallen. Diese Anpassungen sollen die Transparenz erhöhen und eine Nachvollziehbarkeit der Auswirkungen auf die Bilanz sowie die Gewinn- und Verlustrechnung gewährleisten.

Die neuen Regelungen gelten ab dem 1. Januar 2026. Es ist vorgesehen, dass die Anwendung der neuen Vorschriften retrospektiv erfolgt, allerdings ohne verpflichtende Anpassung früherer Perioden.

Fazit

Die Anpassungen am IFRS 9 und IFRS 7 sollen eine einheitliche Anwendung der Vorschriften bei der Klassifizierung und Bewertung von finanziellen Vermögenswerten und finanziellen Verbindlichkeiten gewährleisten und bestehende Unsicherheiten in der praktischen Umsetzung und Offenlegung beseitigen. Ein besonderer Fokus liegt auf der genaueren Handhabung von Zinskomponenten beim SPPI-Test sowie ESG-bezogenen Klauseln in Kreditvereinbarungen.

Sollten Sie Fragen haben oder Unterstützung bei der Umsetzung der Änderungen des IFRS 9 und IFRS 7 benötigen, steht Ihnen das Finanz- und Treasury Management Team jederzeit zur Verfügung.

Autoren:
Ralph Schilling, CFA, Partner, Head of Finance and Treasury Management, Treasury Accounting & Commodity Trading, KPMG AG
Dr. Christoph Lippert, Senior Manager, Finance and Treasury Management, Treasury Accounting & Commodity Trading, KPMG AG

Impressum

Herausgeber

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt

Redaktion

Ralph Schilling
(V.i.S.d.P.)
Partner,
Finance & Treasury
Management
T + 49 69 9587-3552
rschilling@kpmg.com

Nils Bothe
Partner,
Finance & Treasury
Management
T +49 711 9060-41238
nbothe@kpmg.com

Börries Többens
Partner,
Finance & Treasury
Management
T +49 221 2073-1206
btoebbens@kpmg.com

Newsletter kostenlos abonnieren

www.kpmg.de

www.kpmg.de/socialmedia