Corporate Treasury News

KPMG IN DEUTSCHLAND

Ausgabe 45 – Juli 2015

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: www.twitter.com/KPMG_DE_FTM

Mit besten Grüßen,

Prof. Dr. Christian Debus Carsten Jäkel

In dieser Ausgabe

Aktuelle Stellenausschreibungen

- Hochschulabsolvent (m/w) Consulting – Financial Instruments Accounting
- Berater (m/w) Consulting – Financial Instruments Accounting/Valuation
- Hochschulabsolvent (m/w) Consulting – Corporate Regulatory Services (Standorte München und Frankfurt)

Veranstaltungen und Termine

In unseren kostenfreien *Webinaren* nehmen wir zu aktuellen Themen aus dem Bereich Finanz- & Treasury-Management Stellung und informieren Sie über Strategien und die konkrete Implementierung.

Wählen Sie sich online ein und nehmen Sie an unseren thematischen Expertenrunden teil:

27. August 2015, 16:00 Uhr
Finanzinstrumente bei Unternehmenszusammenschlüssen

September 2015, 16:00 Uhr
Maßgeschneiderte Benchmarking-Methodik zur Optimierung der Treasury-Performance

Von jedem Webinar fertigen wir einen Mitschnitt des Vortrags an. Sie finden ihn in unserem Webinar-Archiv.

Lesen Sie unseren aktuellen Blog-Beitrag zum Thema: Treasury steigert Umsatzrendite

Hedge Accounting bei konzerninternen Leistungsfakturen des Kerngeschäfts

Unterschiedliche Konzerne begreifen ihre Währungs(/FX)-Risiken auf verschiedene Art, beispielsweise werden manchmal neben Transaktionsrisiken auch Translationsrisiken gesichert. Auch die Messung und Steuerung des FX-Risikos folgt unterschiedlichen Philosophien. Während beispielsweise in vielen Fällen bereits geplante Zahlungsströme gesichert werden, erfolgt die Sicherung teilweise ausschließlich auf Basis fest kontrahierter Verträge in vorgegebenen Budgetzeiträumen.

Neben diesen zu Recht im Fokus stehenden ökonomischen Überlegungen, sind auch in der Bilanzierung einige Aspekte zu beachten. Während die Hedge-Philosophie und deren Umsetzung meist im Vorfeld abgestimmt werden, um eine bestimmte ökonomische Sicherungswirkung zu erreichen, stellen sich im Rechnungswesen daraus abgeleitete Fragestellungen häufig erst, wenn die Sicherung bereits umgesetzt ist und eine Buchung zwingend erfolgen muss.

Problematisch werden Sicherungsstrategien in der Praxis dann, wenn die Sicherungsderivate eine negative Wertentwicklung aufweisen und ein entsprechender Effekt auch in der Ergebnisrechnung auftaucht. In der Regel soll im Rechnungswesen ein ökonomisch als sinnvoll erachtetes Sicherungskonzept dementsprechend auch bilanziell als Sicherung abgebildet werden (Hedge Accounting). Auch unter Anwendung von Hedge Accounting ist der Aufwand grundsätzlich zu erfassen. Der Ansatz erfolgt allerdings erst in der Periode, in der das Grundgeschäft ergebniswirksam wird. Aus diesem Grund lässt sich der Erfolg der Sicherungsstrategie im FX Hedge Accounting in der Regel gut bilanziell zeigen. Diese Abbildung ist durch die Literatur zu dem Thema für eine Vielzahl von Standardfällen bereits gut beschrieben worden (z.B. KPMG Insights into IFRS 11th, Kapitel 7.7).

Ein in der Praxis häufig vorkommendes Themenfeld wird allerdings nur an wenigen Stellen gewürdigt und sorgt in verschiedenen Konzernen für Zündstoff. Dieses ergibt sich immer dann, wenn in einem Konzern verschiedene Unternehmen mit voneinander abweichenden funktionalen Währungen vorhanden sind und die Produkte erst zwischen diesen Unternehmen fakturiert und nachfolgend an externe Dritte verkauft werden. Die Komplexität bei der Bilanzierung tritt dann auf, wenn die externen Derivate nicht nur auf Ebene des Konzerns, sondern auch auf der Ebene der Einzelgesellschaften in ein Hedge Accounting eingebunden werden sollen.

In der Regel werden bereits sowohl die Sicherungsstrategie als auch die Abrechnungswährung der internen Faktura feststehen. Eine durch das Rechnungswesen angestoßene Änderung der Sicherungsstrategie oder der Abrechnungswährung kommt dementgegen selten in Betracht.

Auf Ebene der Einzelabschlüsse (HGB, IFRS) lassen sich die Sicherungsbeziehungen in der Regel relativ einfach dokumentieren und bilanzieren. Das Thema bekommt allerdings durch die Zwischengewinneliminierung und die Definition des abgesicherten Risikos in der Hedge-Dokumentation eine für den Konzern erweiterte Dimension. So muss beispielsweise die Frage beantwortet werden, wann die Reklassifizierung des other comprehensive income (OCI) erfolgt und in welche P&L-Position das OCI zu reklassifizieren ist. In den nächsten Abschnitten wird dargestellt, dass der Sicherungserfolg für den Einzelabschluss zu einem anderen Zeitpunkte erfolgt als für den Konzernabschluss. Die Definition des abgesicherten Risikos führt darüber hinaus entweder zur Reklassifizierung in den Umsatzerlös oder in die Umsatzkosten.

Beispielfall: Im Zuge der Konzernsteuerung werden in deutschen Gesellschaften (funktionale Währung: Euro) Konsumgüter (Vorratsvermögen) produziert und in Euro an ausländische Vertriebsgesellschaften verkauft. Die ausländischen Vertriebsgesellschaften haben eine, vom Euro abweichende, funktionale Währung (beispielsweise US-Dollar) und verkaufen ihrerseits diese Produkte in der jeweiligen Landeswährung (US-Dollar) an konzernexterne Abnehmer. Da der Konzern durch die Produktion und den zukünftig geplanten Vertrieb einem Euro-/FX+ (im Beispiel: Euro-/US-Dollar+) Risiko ausgesetzt ist, wird dieses Risiko durch das Konzerntreasury mittels Devisentermingeschäfte (Euro+/US-Dollar-) gesichert. Der gesicherte Anteil am geplanten Risiko wird so gewählt, dass der Zahlungsmittelfluss hoch wahrscheinlich ist. Das Grundgeschäft ist nach IAS 39.80 iVm. AG99A zulässig, da ein Weiterverkauf an einen externen Dritten stattfindet.

Durch die Anwendung des Hedge Accounting kommt es im Geschäftsablauf für den effektiven Teil zur Bildung von OCI, das zu dem Zeitpunkt zu reklassifizieren ist, zu dem das gesicherte Risiko ergebniswirksam wird (IAS 39.97/98). Im IFRS- oder HGB-Einzelabschluss ist dies der Zeitpunkt der konzerninternen Faktura. Im Konzern erfasster Gewinn oder Verlust muss allerdings im Zuge der Konsolidierung eliminiert werden und kann daher nicht der Auslöser für die Reklassifizierung werden. Die Umrechnung der Vorräte der ausländischen Tochter in den Vorratsbestand des Konzerns erfolgt zwar zum Stichtagskurs (IAS 21.39(a)) ist allerdings selbst im OCI zu erfassen (IAS 21.39 (c) i.V.m. IAS 21.41) und löst daher ebenfalls keine Reklassifizierung aus. Der Zeitpunkt der Reklassifizierung entspricht daher dem Zeitpunkt des externen Verkaufs, da im Zuge der bilanziellen Erfassung die Umsatzerlöse realisiert und die Umsatzkosten erfasst werden.

Während eine Reklassifizierung in den Konzernumsatz ein häufiges Beispiel in der Literatur zu dem Thema darstellt, führt eine solche Vorgehensweise wie im oben dargestellten Beispiel zu einer Diskrepanz. Der Sicherungserfolg (das OCI) wird auf Ebene des Einzelabschlusses in die Umsatzkosten reklassifiziert, während der Sicherungserfolg (das OCI) im Konzern, unter Anwendung des Standardfalls, im Umsatzerlös reklassifiziert wird. Der Vorteil einer Reklassifizierung in die Umsatzkosten liegt darin, dass auf Ebene der Einzelabschlüsse das konzernexterne Derivat unter Verwendung von internen Derivaten in ein gleichartiges Hedge Accounting des Tochterunternehmens mit einbezogen werden kann. Die US-Dollar-Tochter verfügt dann über ein (konzerninternes) Derivat mit der Treasury-Mutter (Euro+/US-Dollar-) und ein (konzerninternes) Risiko aus dem Europreis fixierten Bezug von Waren. Die zum Zeitpunkt des externen Weiterverkaufs erfolgende Reklassifizierung von OCI in die Umsatzkosten aus dem IFRS- Einzelabschluss kann direkt in den Konzern übernommen werden. Lediglich das OCI für konzerninterne Fakturen, denen kein externer Umsatz gegenübersteht, muss auf Konzernebene erneut abgegrenzt werden.

Entscheidend für den Ausweis der Reklassifizierung ist die Analyse, ob bei dem Hedge der konzerninterne Warenbezug (Euro-/US-Dollar+) oder der konzernexterne Warenverkauf (Euro-/US-Dollar+) gesichert wird. Im Fall von Warenbezug stellen die Umsatzkosten (IAS 39.98) das gesicherte Risiko dar. Die geplante Transaktion muss zu diesem Zweck auf den Zwischenerwerb von Eurovorratsvermögen in einer FX(US-Dollar)-Tochter abstellen. Im Fall des Warenverkaufs (IAS 39.97) stellen die konzernexternen Umsatzerlöse das gesicherte Risiko dar. Die Reklassifizierung kann daher sowohl im konzernexternen Umsatz als auch in den Umsatzkosten des Konzerns gezeigt werden.

Das voranstehende Beispiel hat gezeigt, dass auch in der bilanziellen Abbildung von fest vorgegebenen Geschäftsvorfällen verschiedene Aspekte zu beachten sind und zumindest implizit auch Wahlrechte bestehen. Die Erträge und Aufwendungen der Sicherungsinstrumente können auf diese Weise auch in der Konzern-P&L und der Segmentberichterstattung verursachungsgerecht zugeordnet werden.

Autor: Felix Wacker-Kijewski, Manager, fwackerkijewski@kpmg.com

Wake Up Call: REMIT-Reporting

„Regulierung“ ist ein Begriff, der aus Sicht der Finanzabteilung lange Zeit fast nur im Sprachgebrauch von Banken existiert hat. Noch unter den Eindrücken von EMIR und mit den Herausforderungen von REMIT und MiFID II in Sichtweite sollte mittlerweile jedem klar sein, dass Regulierung nun auch die

Industrie erfasst hat – und zukünftig nicht mehr wegzudenken sein wird. Es wird Zeit, sich den Herausforderungen zu stellen.

Zum Zeitpunkt des Erscheinens dieses Artikels verbleiben keine drei Monate bis zum 07. Oktober, jenem Stichtag, an dem das Reporting von börsengehandelten Energie- und Gaskontrakten an ACER verpflichtend wird. Von emsiger Betriebsamkeit ist jedoch noch nicht viel zu spüren. Viele Unternehmen scheinen diesem Datum überraschend gelassen entgegen zu sehen. Ein Grund dafür kann sein, dass REMIT den betroffenen Unternehmen die Möglichkeit bietet, das Reporting an den entsprechenden Marktplatz oder den Broker (die sogenannten OMPs) auszugliedern. Das Unternehmen selbst muss sich keine Gedanken um die technische Umsetzung machen und wäre damit erstmal fein raus.

Wobei, ganz so einfach ist es nicht. Denn die Verantwortung über die gesamtheitliche Meldung aller relevanten Datenfelder und damit die Einhaltung der gesetzlichen Vorgaben bleibt dem Unternehmen trotz Delegation des Reporting erhalten. Eine Vielzahl von zur Delegation abgestellten OMPs führt dabei zu einer heterogenen Meldelandschaft, über welche es schwierig sein wird, einen Überblick zu behalten. Weil keine universellen Standards zur Datenaufbereitung und dem Reporting bestehen, werden die Meldedaten untereinander nicht so einfach zu aggregieren und abzugleichen sein. Unternehmen, welche einen Überblick über die an ACER gemeldeten Daten behalten wollen, werden einiges an laufenden Aufwand investieren müssen, um am Ball zu bleiben. Dieses Vorgehen erscheint zwar mühsam, ist aber zumindest im Rahmen des Möglichen.

Richtet man den Blick weitere sechs Monate in die Zukunft, so wird klar, dass die eben beschriebene Strategie kurzsichtig und nicht zu Ende gedacht ist. Denn ab dem 7. April 2016 müssen auch die übrigen Transaktionen an ACER gemeldet werden – dies umschließt OTC-Kontrakte und komplexe Energieversorgungsverträge. Gerade OTC-Kontrakte innerhalb einer Unternehmensgruppe oder zwischen Energieversorgungsunternehmen sind davon betroffen. Nicht nur, dass wie im Falle dieser Kontrakte kein OMP bereit steht, um die Meldung zu übernehmen, sondern die Kontrakte sind in ihrer Ausgestaltung auch deutlich heterogener, was das Reporting wesentlich erschwert.

Vor diesem Hintergrund eine abwartende Haltung einzunehmen, führt fast zwangsläufig zum Versäumnis, die gesetzlichen Anforderungen vollumfänglich und korrekt zu erfüllen. Anbieter von Reporting-Lösungen wittern ihre Chance, und tatsächlich können sie einen erheblichen Mehrwert in der Umsetzung bieten. Von der grundsätzlichen Bürde können aber auch sie die betroffenen Unternehmen nicht befreien: eine strukturierte Basis für jegliche Form von Regulierungsanforderungen zu schaffen. Es entspricht nicht den Ansprüchen moderner Finanzabteilungen, sich von einer Regulierung zur nächsten zu hangeln. Es muss eine Grundlage geschaffen werden, welche den Schrecken auch aus noch kommenden Regulierungsanforderungen nimmt. Der Schlüssel dazu liegt in einer zentralen, strukturierten Datenhaltung, welche den gemeinsamen Nenner dieser Anforderungen darstellt.

Kürzlich noch war EMIR der regulatorische Unruhestifter in Industrie und Energiewirtschaft, heute ist es REMIT und morgen MiFID II oder was auch immer danach kommen wird. Je früher sich die Unternehmen der Herausforderung einer zentralen Datenhaltung stellen, desto eher kann auf aufwendige Insellösungen verzichtet werden und eine zentrale Basis für regulatorische Anforderungen geschaffen werden. Warum also warten?

Autor: Paul Ratzenböck, Manager, pratzenboeck@kpmg.com

Roll-Out von Treasury-Systemen – Eine häufig unterschätzte Herausforderung

Fast jedes global agierende Unternehmen setzt heutzutage ein Treasury-Management-System (TMS) eines Standard-Systemanbieters ein oder befindet sich in der Überlegung, ein solches System einzuführen. Eine optimale Nutzung des TMS ist in der Folge aber nicht nur abhängig von den fachlichen Anforderungen des Treasury an das TMS, sondern auch von den

Zielen des Unternehmens in Bezug auf seine internationale Aufstellung, Breite und Anzahl der unterschiedlichen abzubildenden fachlichen Prozesse sowie den lokalen Anforderungen im Rahmen des System-Rollouts. Dabei ergeben sich Herausforderungen, die bei Planung und Durchführung nicht zu unterschätzen sind.

Steigenden Anforderungen an Effizienz, Transparenz und Methodenkompetenz im Treasury begegnen TMS entsprechende Funktionalitäten, operative Verfügbarkeit und Performance. Durch stetig wachsende Organisationen und Operationen in unterschiedlichen Ländern, Regionen und Zeitzonen ist gerade in den vergangenen Jahren die Zunahme von Treasury-Zentren von europäischen Unternehmen in der nordamerikanischen Freihandelszone oder dem nordöstlichen Asien zu verzeichnen. Immer mehr Aufgaben werden daher auch durch lokale Treasury-Mitarbeiter innerhalb dieser Regionen wahrgenommen, wodurch zumeist eine Integration bzw. Kopplung an die bestehende Treasury-Systemlandschaft erforderlich wird.

Insbesondere beim Aufbau einer globalen Plattform für das Treasury-Management gilt es, nicht nur eine Vielzahl verschiedener Systeme und Tools, Schnittstellen und Informationen zu integrieren. Hierbei werden die vor einem Rollout existierenden lokalen Prozesse und IT-Lösungen durch standardisierte Prozesse und Systemfunktionalitäten abgelöst. Die sich hieraus ergebenden Herausforderungen entsprechen nicht selten einer Neueinführung eines TMS. Die Unterschiede von Land zu Land und die damit verbundene häufig geringe Übertragbarkeit eines Rollouts stellen die Beteiligten vor zusätzliche Herausforderungen: Standard-Prozesse sind oft nicht oder nicht in der benötigten Granularität vorhanden, lokale Gegebenheiten sind zu prüfen und Unterschiede zum bisherigen Standard zu analysieren und zu bewerten. Hinzu kommt, dass durch die stetige Dynamik die Ressourcen zumeist knapp und Spezialisten für diese Themen im eigenen Unternehmen rar sind.

Welche Aspekte sind für eine erfolgreiche Umsetzung von internationalen Rollouts zu berücksichtigen?

1. **Planung:** Die Notwendigkeit einer validen und sorgfältigen Planung kann nicht genug betont werden. Vor Beginn der eigentlichen Arbeit müssen die rein fachlichen Anforderungen in ausreichend detaillierten Konzepten dargestellt werden. Daraufhin gilt es zu eruieren, ob die Anforderungen im bestehenden Setup umgesetzt werden können. Ebenso gilt es Interdependenzen zwischen mehreren, sich möglicherweise überschneidenden Rollouts zu identifizieren und in der Rollout-Planung zu berücksichtigen. Hinzu kommt ferner, dass ein Rollout in der Regel. nicht die gesamte Funktionalität eines TMS umfasst, sondern Rollout von Front-Office- und Reportingfunktionalitäten, Back-Office und Settlement, Treasury Accounting, Cash Management, In-house-Bank und Payment Factory-Aspekten möglicherweise in mehreren Schritten umgesetzt werden sollen und die Planung daher längere Zeit in die Zukunft reicht. Hierbei sind dann nicht nur Abhängigkeiten innerhalb der Rollout-Kette zu beachten (beispielsweise sollten für eine Gesellschaft bereits bei einem Rollout der Funktionalität zur Dealerfassung auch diejenigen Anforderungen an das Instrumenten-Setup antizipiert und umgesetzt werden, die erst bei einem späteren Rollout des Treasury-Nebenbuchs relevant werden), sondern ist auch eine Mittelfristplanung über die benötigten Kapazitäten aufzubauen, damit mögliche weitere Projekte nicht gefährdet werden.
2. **Evaluierung fachlicher Anforderungen und Berücksichtigung lokaler Gegebenheiten:** Wie bei jedem TMS-Projekt bilden eindeutige Fachkonzepte die wesentliche Grundlage einer Umsetzung. Diese sind aber vor dem Hintergrund von möglicherweise nicht leicht zu antizipierenden lokalen Spezifika nicht einfach zu eruieren. Dadurch sind der Abdeckungsgrad bzw. mögliche Gaps in der aktuell verfügbaren Systemfunktionalität (und damit gegebenenfalls nötiger umfangreicher Erweiterungen) manchmal schwierig zu bestimmen. Beispielsweise stellen bei einem Back-Office-Rollout für eine indische Gesellschaft lokale Kapitalverkehrsbeschränkungen besondere Anforderungen an die umzusetzenden Settlement-Prozesse und die dafür genutzten Schnittstellen und Dateiformate. Oder aber es bestehen Besonderheiten wie bei durch südamerikanische oder asiatische Gesellschaften genutzten Finanzinstrumenten und gültigen Day Count Conventions. Hinzu kommen häufig steuerliche Besonderheiten.
3. **Treasury IT-Know-How und Übersicht:** Eine der wichtigsten Ressourcen bleibt der Mensch hinter der Maschine. Für Planung und Evaluierung gilt große Sorgfalt, bei der Abstimmung der Interdependenzen und Reihenfolge verschiedener Rollouts ist Übersicht besonders wichtig. Und sehr häufig sind es gerade auch die technischen Unterschiede zwischen Zielländern verschiedener Rollouts und die Möglichkeiten des Unternehmens, auf diese angemessen reagieren zu können, welche ausschlaggebend dafür sind, wie reibungslos

ein Rollout umgesetzt werden kann. Dazu gehören unter anderem Schnittstellen zu lokalen ERP-Systemen oder Zahlungsdateiformate.

Durch neue Technologien wie SaaS oder ASP, die seit einiger Zeit auch im TMS-Markt Einzug halten, können die hier beschriebenen Herausforderungen erheblich reduziert bzw. gegebenenfalls an den Vendor übertragen werden. Bei inhouse betriebenen Lösungen zeigt sich, dass eine professionelle Vorbereitung und Planung sowie ein erfahrenes Projektteam die wesentlichen Schlüsselelemente bei internationalen Rollouts sind.

Autor: Nils Bothe, Senior Manager, nbothe@kpmg.com

Währungsbasis-Spreads und Bewertung von FX-Derivaten

Ähnlich wie Tenorbasis-Spreads in Zinsmärkten einer einzelnen Währung, wuchsen nach der Finanzkrise auch Basis-Spreads zwischen Zahlungsströmen in unterschiedlichen Währungen. Dies hat zur Folge, dass die klassische Zinsparität nicht mehr gilt. Damit ergeben sich nicht mehr die gleichen Eurobeträge, je nachdem ob man heute ein US-Dollar in Euro umtauscht und in den Drei Monate Euribor investiert oder im Vergleich dazu heute ein US-Dollar in den Drei Monate Libor investiert und den resultierenden US-Dollarbetrag mit Hilfe eines heute fair abgeschlossenen Forwards in Euro umtauscht. Die Eurobeträge, die aus diesen beiden Anlagenstrategien resultieren, sind nicht mehr identisch!

Die Differenz ist auf die Währungsbasis zurückzuführen, die seit der Finanzkrise in fairen Forwards eingepreist, jedoch nicht in Euribor- und Libor-Raten enthalten ist. Sie würde eine klare Arbitragemöglichkeit darstellen, die von Marktteilnehmern ausgenutzt werden würde und somit schnell wieder verschwinden sollte. Dies ist auf geänderte Liquiditätspräferenzen der Marktteilnehmer in Bezug auf Währungen und das unterschiedliche Liquiditätsangebot in den verschiedenen Währungsräumen zurückzuführen. Letzteres wird maßgeblich von der unterschiedlichen Geldpolitik der verschiedenen Notenbanken beeinflusst.

Folglich muss die Modellwelt so angepasst werden, dass die oben genannten Effekte berücksichtigt werden und verhindert wird, dass Arbitragemöglichkeiten impliziert werden, die in Realität nicht existieren. Dies bedeutet, dass letztendlich der aus den beiden Anlagestrategien resultierende Eurobetrag wieder identisch sein muss. Um dies zu erreichen und folglich theoretische Arbitragemöglichkeiten zu verhindern, muss entweder auf der Libor- oder Euribor-Seite ein entsprechender positiver oder negativer Zinsaufschlag (Spread) berücksichtigt werden. Dies ist der sogenannte Währungsbasis-Spread. Er kann aus am Markt gehandelten Instrumenten wie zum Beispiel FX-Forwards oder Cross-Currency-Basisswaps berechnet werden.

Daher ist es wichtig, die in solch einem Währungsbasis-Spread enthaltene Information bei jeder Bewertung von Fremdwährungsderivaten (FX-Forwards, Cross-Currency-Swaps, etc.) zu berücksichtigen. Andernfalls würde die Bewertung die aktuelle Marktsituation und die übliche Praxis bei Bewertung und Preisstellung solcher Derivate nicht widerspiegeln. Als Konsequenz entsprechen Bewertungen, die diese Effekte nicht berücksichtigen nicht den Anforderungen des IFRS 13 hinsichtlich der Bestimmung des Zeitwertes. Zur Veranschaulichung: Jemand der Währungsbasis-Spreads nicht in seiner Bewertung berücksichtigt, sollte im Abschlusszeitpunkt signifikant von Null abweichende Markwerte für eigentlich faire abgeschlossene FX-Forwards erhalten, wenn er sie innerhalb seiner eigenen Bewertungsinfrastruktur (z.B. einem Treasury-Management-System) berechnet.

Unglücklicherweise haben dadurch Cross-Currency-Derivate unterschiedliche Werte, je nachdem ob sie beispielsweise aus der Sicht eines US-Investors (der auf Libor-Basis diskontiert), oder eines Eurozonen-Investors (der auf Euribor-Basis diskontiert) gepreist werden. Der Unterschied in der Bewertung spiegelt die Änderung der Währungsbasis zwischen Abschluss- und Bewertungszeitpunkt wider.
Unsere Experten des Finanz- und Treasury-Management-Teams stehen jederzeit gerne für die Beantwortung von Fragen bezüglich der Bewertung von Finanzinstrumenten zur Verfügung. Zusätzlich bieten wir eine Vielzahl von Leistungen im Zusammenhang mit der Implementierung und Optimierung von Treasury-Systemen an.

Autor: Ralph Schilling, Manager, rschilling@kpmg.com

Gastbeitrag

Sechs Wege, um finanziellen Fraud im Treasury zu vermeiden

Fraud ist eine der Hauptsorgen, die CFOs und Treasurer nachts nicht schlafen lässt. Es handelt sich um eine ständig steigende Bedrohung durch die Zunahme von Spear-Phishing sowie von Datenpannen und den auf erfolgreiche Betrugsversuche zurückzuführenden Vertrauensverlust in den Unternehmenswert.

- 53 Prozent aller Unternehmen sind bereits Ziel von finanziellem Fraud gewesen.
- Als Ergebnis daraus haben 50 Prozent aller attackierten Unternehmen einen finanziellen Schaden erlitten.
- Interner Betrug tritt mit 36 Prozent häufiger auf als externer Missbrauch mit einem durchschnittlichen Verlust von US-Dollar 1.971.000 und einem Zentralwert der bei US-Dollar 451.000 liegt.
- Durchschnittlich dauert es 18 Monate von dem Beginn bis zur Entdeckung des Betrugs.

Zu den direkten finanziellen Verlusten kommen die indirekten Verluste dazu, welche verheerend sein können. Möglich sind: fallende Aktienkurse, Verlust von Vertrauen bei Investoren, Kunden und Partnern, Gerichtsverfahren und Strafen. Hieraus ergibt sich die Frage, wovor man sich am meisten hüten soll.

Es existiert eine breite Palette sowohl von internen als auch externen Gefahren, die der Integrität der Unternehmensfinanzen einer Organisation gegenüberstehen. Um die eigene Organisation sicherer zu machen, ist es notwendig zu verstehen, wo die Schwachstellen liegen. Beispiele solcher Schwachstellen beinhalten externes Hacking des Treasury-Systems und der Daten Dritter, hervorgerufen durch Datensicherheitsmängel; zweckwidriger Zugang von Mitarbeitern zu Server-Räumen und internen Netzwerken durch unzureichende physische und datenbezogene Sicherheitsprozesse; betrügerische Bankzahlungen durch Mitarbeiter, absichtlicher oder unabsichtlicher Natur (oft als Folge von Social Engineering oder Phishing-Angriffen); falsche Bestellungen und Rechnungen, die von internen Mitarbeitern an verbundene dritte Parteien in Auftrag gegeben werden; Abwicklungsanweisungen, die Kapital an unbefugte Konten weiterleiten; nachteilige Finanztransaktionen durch Mitarbeiter zu deren persönlicher Bereicherung; ehemalige Mitarbeiter, die nach ihrem Ausscheiden weiterhin als Zeichnungsberechtigte der laufenden Bankkonten bestehen bleiben und unregelmäßiger oder ineffizienter Abgleich von Konten, wodurch betrügerische Transaktionen unbemerkt bleiben.

Sicherheit von Anwendungen: Am häufigsten nutzen die Betrüger unsichere Passwörter und unzureichende Verfahren zur Benutzerauthentifizierung aus. Angreifer suchen gezielt nach unsicheren Passwörtern. Jedes Unternehmen sollte daher sicherstellen, dass keine Einzelpasswort-Verifizierungsverfahren im Einsatz sind, die zum Beispiel den Zugang zum Treasury oder anderen Finanzsystemen durch ein einmaliges Anmelden mit einem Passwort ermöglichen.

Daher nutzen Bankenportale oft eine doppelte Authentifizierung. Hierbei generiert ein kleines Gerät ein zufälliges Passwort, das eingegeben werden muss, wenn die erste User-ID und das User-Passwort korrekt eingetragen wurden. Die meisten Softwareplattformen unterstützen das sogenannte „Bring Your Own Device“ (BYOD), sodass das eigene Smartphone genutzt werden kann, um das einmalig gültige zweite Passwort zu erhalten. Andere Optionen beinhalten Yubikey, was oft in der Region EMEA (Europe, Middle East, Africa) genutzt wird. Doppelte

Authentifizierung alleine wird allerdings nicht als Best-Practice angesehen.
Multi-Faktor-Authentifizierungstechniken kombinieren verschiedene Login- und Authentifizierungsstrategien, um den bestmöglichen Schutz für Unternehmenssysteme zu gewährleisten.

Datensicherheit: Das Speichern von Daten innerhalb eigener Systeme bietet ein weiteres Sicherheitsrisiko, da über 25 Prozent aller Betrugsfälle interner Herkunft sind. Es gestaltet sich zunehmend schwieriger für IT-Abteilungen mit dem zur Verfügung stehenden Budget in führende Lösungen zu investieren, deren Leistungsfähigkeit, Servicegrad und Datensicherheit den Anforderungen eines globalen Treasury entsprechen. Die Mehrheit der CIOs und CFOs sieht in Cloud-basierten Lösungen eine gute Möglichkeit, die Datensicherheit zu verbessern.

Einblick und Überwachung der Bankkonten: Unzureichender Einblick in die Bankkonten und Zeichnungsberechtigten können für das Treasury-Management verhängnisvoll sein. Oftmals sind Informationen über berechtigte und unterzeichnende Personen der Zentrale nicht bekannt. Manchmal sind sie noch eingetragen, obwohl sie das Unternehmen bereits verlassen haben. Die Überwachung der Bankkonten wird für die Unternehmen zunehmend schwieriger, wenn diese organisch oder durch Zukäufe anderer Firmen wachsen. Die Implementierung technischer Lösungen zum Management der Bankkonten kann helfen, die Prozesse zu vereinheitlichen sowie die Transparenz und Überwachung der Bankkonten deutlich zu verbessern.

Digitale Signaturen: Digitale Signaturen sind ein hilfreiches Mittel, um Zahlungsanweisungen aus Systemen von Dritten, zum Beispiel TMS oder ERP, zu authentifizieren. Digitale Signaturen sind persönliche, digitale Identifizierungslösungen auf Basis einer „Public Key Infrastructure“ (PKI). SWIFT's 3SKey – das als industrieführende digitale Signatur-Lösung gilt – kann intern als Teil eines Prozesses zur Zahlungsgenehmigung und extern zur Authentifizierung eines Zahlungspostens angewandt werden, in dem es der Bank bestätigt, dass alle Zahlungen korrekt und gültig sind. Dies hilft nicht nur zur Validierung der Zahlungen, sondern reduziert auch die Tendenz zur Zahlungsablehnung durch die Bank. Der Einsatz digitaler Signaturen, kombiniert mit strengen Passwortregelungen und einem zentralisierten Zahlungsablauf, reduzieren wesentlich die Möglichkeiten eines Zahlungsbetrugs.

Abwicklung von Zahlungen: Spear-Phishing ist der gefährlichste Betrugsversuch im Treasury, weil man persönlich von Cyberkriminellen attackiert wird. Der Fokus liegt auf Zahlungsabwicklungen, da der Erfolg eine direkte Zahlung verspricht – Transfer von Geldern auf falsche Bankkonten. Strenge Passwortregelungen erhöhen zwar das Sicherheitsniveau, aber eine Standardisierung der Zahlungsabwicklung, um die Einhaltung der Prozesse zu gewährleisten, ist auch wiederum gefährlich. Zielgerichtete Angriffe warten nur auf eine Abweichung vom Normalfall; nur ein Fehler ist also nötig, um eine Betrugsmöglichkeit zu eröffnen. Das Standardverfahren sollte sein, mehrfache und elektronische Freigabelevels einzuführen, idealerweise gebunden an das 4-Augen-Prinzip im Treasury-Management-System und der festgelegten Richtlinien oder Limite. Viele Treasury-Teams benutzen digitale Signaturen nicht nur für die externe Verifizierung von Zahlungen, sondern auch für interne Freigaben. Organisationen, die die Abwicklung von Zahlungen trennen und zum Beispiel interne Systeme und externe Bankportale getrennt zur Abwicklung und Genehmigung von Zahlungen nutzen, riskieren betrügerische Vorgänge.

Als Best Practice wird die Steuerung der kompletten Abwicklung von Zahlungen in einem einzigen System angesehen, die den gesamten Weg der Zahlung von der ursprünglichen Anfrage bis zur Durchführung dokumentiert. Dies ermöglicht auch die Integration der Zahlungsgenehmigung (bis zu vier Level) in den Arbeitsablauf. Viele Organisationen zentralisieren weiterhin Treasury und Lieferantenzahlungen an einer zentralen Stelle, um sicherzustellen, dass das Treasury eine globale Transparenz über alle ausgehenden Zahlungen hat. Dies spart nicht nur Kosten, sondern erlaubt auch eine komplette Übersicht über alle ausgehenden Cashflows des Unternehmens.

Standard-Abwicklungsanweisungen: die Abwicklung des Finanzhandels bietet zunehmend Raum für internen Betrug. Der Finanzhandel (Investments, Devisen, Derivate) gehört zur alltäglichen Aktivität des Treasury. Für die gängigen Banktransaktionen kommen in den meisten Fällen Standard-Abwicklungsanweisungen (Standard Settlements Instructions, SSI) zum Einsatz. Für die nicht alltäglichen Geschäfte mit der Bank oder für solche mit anderen Gegenparteien sind SSIs nicht immer vorhanden. Dies schafft eine weitere Grundlage für Fraud, indem Banküberweisungen komplett oder teilweise auf unautorisierte Bankkonten umgeleitet werden. Das Benutzen von Standard-Abwicklungsanweisungen (SSI) im eigenen Finanzsystem verhindert solche betrügerischen Akte und erhöht gleichzeitig die Effizienz. Wichtige Schritte zur Implementierung sind die elektronische Dokumentation der Finanztransaktionen im Treasury-System, inklusive der erteilten Genehmigungen und Limits, um jederzeit eine volle Buchungskontrolle zu ermöglichen; Zahlungsvorlagen sollten jedem Vorgang automatisch zugeordnet werden; zusätzliche Genehmigungen sollten erforderlich sein, um Vorlagen zu bearbeiten oder zu entfernen und jegliche Aktivität elektronisch festgehalten werden; der Abgleich von Trade Tickets zwischen den Gegenparteien und dem Treasury-System sollte in regelmäßigen Abständen durchgeführt werden, um sicherzustellen, dass Ausnahmen keine Chance gegeben wird.

Ein robustes technisches System ist ein kritisches Element in der Sicherheitsgleichung. Auch wenn ein anspruchsvolles Treasury-Management-System (TMS) vorhanden ist, müssen Treasury-Teams sicherstellen, dass sie nicht die Schwachstelle sind, die das Unternehmen potenziellem Betrug aussetzt. Dafür ist es notwendig, dass Unternehmen ihre Mitarbeiter über die Methoden unterrichten, mit denen Betrüger versuchen, Mitarbeiter durch „Social Engineering" dazu zu bringen, entweder sensible Bankdaten preiszugeben oder ihnen Geld zu überweisen. Mitarbeiter müssen gut über die internen Prozesse zum Anstoß und zur Durchführung von Zahlungen Bescheid wissen, um verdächtige Anfragen aufdecken zu können.

Gastautor: Bob Stark, Vice President, Strategy, Kyriba

Übersetzung aus dem Englischen. Den Originaltext finden Sie hier.

*Quelle: "The Association of Corporate Treasurers / Kyriba Treasury Study, 2015"

Impressum

Herausgeber

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt am Main

www.kpmg.de

Redaktion

Prof. Dr. Christian Debus (V.i.S.d.P.)
Partner, Finance Advisory
T +49 69 9587-4264
cdebus@kpmg.com

Carsten Jäkel
Partner, Finance Advisory
T +49 221 2073-1522
cjaekel@kpmg.com

Newsletter kostenlos abonnieren

www.kpmg.de/newsletter