Corporate Treasury News

Aktuelle Entwicklungen und Trends im Bereich Treasury kompakt zusammengefasst

Ausgabe 141 | März 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

At-Risk-Risikomaße im Treasury

At-Risk-Maße sind heute noch nicht Standard

Eine der herausfordernden Aspekte des Treasury ist das Management der Risiken, die sich aus seinen originären Aufgaben (Bereitstellung von Liquidität, Finanzierung und Anlage, Management von Fremdwährungen) ergeben. Eine Grundvoraussetzung für das Management dieser Risiken ist die Identifikation der verschiedenen Risikofaktoren und die Quantifizierung der potenziellen Auswirkungen. Bezüglich der Identifikation der relevanten wesentlichen Risikofaktoren haben sich Standards im Treasury etabliert, an denen sich die meisten Unternehmen orientieren.

Weniger einheitlich sieht es bei der Quantifizierung von Risiken aus. Auf der methodischen Seite lässt sich eine kontinuierliche Weiterentwicklung von Kennzahlen, mathematischer Modelle und Berechnungsverfahren beobachten, welche die stetig wachsenden technologischen Möglichkeiten ausnutzen. Bei der praktischen Anwendung findet sich dagegen eher ein Spektrum unterschiedlicher Herangehensweisen.

Im Bereich des Marktrisikos finden nominales Exposure und einfache Sensitivitäten, wie eine fest vorgegebene Wechselkursveränderung oder eine konstante Parallelverschiebung aller Zinskurven, als primäre Kennzahlen immer noch weite Verbreitung. Beim Kreditrisiko gegenüber Banken bilden typischerweise Anlagevolumen und Rating den Kern der Limit-Vergabe und Anlagesteuerung. Die Verwendung von tatsächlichen Risikomaßen wie zum Beispiel Value-at-Risk oder Cashflow-at-Risk sind längst noch nicht Standard im Corporate Treasury. Und auch dort, wo sie als Kennzahlen bereits Teil des Berichtswesens sind, bilden sie häufig nicht das Herz der tatsächlichen Risikosteuerung.

Die Portfolioperspektive als Treiber

Nach der Identifikation der wesentlichen Risikofaktoren bildet die Ermittlung des zugehörigen Exposures den zweiten logischen Schritt in der Risikomessung. Innerhalb der komplexen Zusammenhänge der operativen und finanziellen Prozesse eines Unternehmens ist die Umsetzung nicht einfach. Die Herausforderungen reichen von Detailfragen wie dem im Buchungssystem tatsächlich zur Buchung verwendeten Wechselkurs (tagesaktueller oder doch Vortageskurs?) über organisatorische Fragen (woher können Plandaten zur Wechselkursicherung ohne währungsscharfe Planung kommen?) bis zu grundsätzlichen Fragen wie der Absicherung von Translationsrisiken oder der Zielsetzung des Zinsrisikomanagements. Die Auflösung dieser Fragestellungen und Weiterentwicklung der Prozesse zur Exposure-Ermittlung binden häufig einen guten Teil der verfügbaren Kräfte und bringen eine Fokussierung auf einfache, bestandsorientierte Kennzahlen mit sich.

Doch in diesem Fokus geht der Blick auf die Gesamtposition verloren: Das Zusammenspiel der unterschiedlichen Wechselkurse oder Märkte wird nicht berücksichtigt. Betrachten wir ein typisches Beispiel: Aus einer unterstellten Wechselkursveränderung von 10% lässt sich für jede Währung eine Wertveränderung des zu Grunde liegenden Portfolios bestimmen. Rechnerisch lassen sich dann die Einzelwerte zu einem Gesamteffekt zusammenrechnen, doch unterschiedliche Schwankungsbreiten und Abhängigkeiten zwischen den Währungen bleiben dann unberücksichtigt. Eine solche Kennzahl hat damit geringe Aussagekraft und ist für die Steuerung einer Gesamtposition oder eines Teilportfolios kaum geeignet.

Genau diesen Mangel beheben Kennzahlen wie die At-Risk-Risikomaße. Ausgehend von einer Zielgröße wie Marktwert (Value), Cashflow oder Ertrag (Earnings) lässt sich der Effekt eines „sinnvollen“ Szenarios für alle betrachteten Marktvariablen bestimmen. Die Definition von sinnvoll ergibt sich dabei aus einem vorgegebenen Sicherheitslevel (Konfidenzniveau). Die Möglichkeit den Gesamteffekt den einzelnen Risikofaktoren zuzuordnen bleibt dabei erhalten. Anstelle der separaten Steuerung der Einzelgrößen tritt jedoch das Management des Portfolios als zusammenhängende Größe.

In der praktischen Umsetzung kann dann zunächst das einfache Limit für Nominal oder Sensitivität pro Risikofaktor (als zum Beispiel Währung) durch ein At-Risk-Limit ersetzt werden, womit schon einmal die unterschiedlichen Volatilitäten berücksichtigt werden. Die Berücksichtigung von Diversifikations- und Cluster-Effekten zwischen den Risikofaktoren ergibt sich aber erst über den Wechsel von faktorspezifischen Limiten zu einem Portfoliolimit.

Herausforderungen

Während bei Banken das Management finanzieller Risiken Teil des Grundgeschäftes darstellt, ist das Corporate Treasury als notwendige Funktion neben

dem eigentlichen operativen Geschäft typischerweise schlank aufgestellt, gerade auch in Bezug auf Kapazitäten für quantitative Methodik und Datenanalyse sowie der zugehörigen Software-Tools. Lösungen im Corporate Treasury bedürfen entsprechend eines hohen Grades an Automatisierung und Standardisierung und müssen sich in die bestehende IT-Landschaft gut integrieren.

Auch die Zusammenstellung von geeigneten Marktdaten ist in der Regel mit einigen Schwierigkeiten verbunden. Ereignisse wie Währungen, die entfallen oder neu hinzukommen, Referenzzinsen, die wechseln, oder Veränderungen in Marktkonventionen müssen beim Aufbau und der Pflege von Datenhistorien richtig berücksichtigt werden. Wird bei einer Währungsumstellung beispielsweise keine künstliche Historie für eine neue Währung ergänzt, werden die gängigen Verfahren implizit einen konstanten Preis unterstellen und das tatsächliche Risiko unterschätzen. Zu den Zeitreihen für die eigentlichen Marktdaten können dann auch zusätzliche Daten wie Korrelationen oder Volatilitäten hinzukommen, die sowohl hinsichtlich Verfügbarkeit und Vollständigkeit besonderer Beachtung bedürfen.

Auf der methodischen Seite müssen nicht nur die richtigen Risikomaße festgelegt und zwischen unterschiedlichen Berechnungsverfahren (zum Beispiel modell-basierte Näherungsverfahren oder Simulationsansätze) gewählt werden, sondern auch Möglichkeiten zur Ergebnisverifikation für die betrachteten Zeiträume bedacht werden.

Neben diesen fachlichen Aspekten ist beim Wechsel zu einer Portfoliosicht und neuen Risikomaßen eine sorgfältige Einbindung aller betroffenen Bereiche notwendig.

Ein durchdachtes Vorgehen als roter Faden

Die Einführung von At-Risk-Risikomaßen ist kein Selbstzweck, sondern direkt mit einer Portfoliobetrachtung verbunden. Für eine erfolgreiche Umsetzung ist es notwendig, zunächst die Zielsetzung abzustimmen, da sich ganz unterschiedliche Anforderungen ergeben können. Beispielsweise fällt die Wahl des richtigen Berechnungsverfahren ganz unterschiedlich aus, wenn man eine retroperspektive, periodische Berechnung von At-Risk-Werten für reine Berichtszwecke neben eine Echtzeitberechnung für die aktive Steuerung der Position legt. Genauso ergeben sich aus der Wahl eines täglichen oder wöchentlichen Betrachtungszeitraums ganz andere Möglichkeiten zum Backtesting als bei einem Jahreshorizont und es sind gegebenenfalls auch unterschiedliche Markteffekte zu berücksichtigen.

Aus der Zielsetzung lassen sich also die möglichen Verfahren eingrenzen, die dann unter Berücksichtigung der kundenspezifischen System- und Datenlandschaft in eine geeignete Lösung gebracht werden müssen. An dieser Stelle ist eine sorgfältige Analyse notwendig, wenn am Ende ein hoher Grad an Automatisierung und Integration erreicht werden soll.

Auf diesen Grundlagen kann dann die eigentliche Implementierung erfolgen, die typischerweise die folgenden Blöcke enthält:

- **Marktdaten** — Erhebung und Bereinigung der historischen Marktdaten, Ergänzung gegebenenfalls fehlender Marktvariablen und Sicherstellung eines Prozesses zur laufenden Datenversorgung und deren Qualitätssicherung
- **Systeme** — Konfiguration bzw. Anpassung des Treasury-Management- oder Reporting-Systems, gegebenenfalls Integration eines separaten Tools zur Berechnung der Risikokennzahlen
- **Reporting** — Anpassung und Erstellung der notwendigen Berichte zur Positions-, Daten- und Risikoanalyse
- **Limit-System** — Adaption der Limit-Logik basierend auf den At-Risk-Risikomaßen und Festlegung initialer Limite
- **Validierung** — Überprüfung der implementierten Lösung und Aufbau eines Prozesses zum regelmäßigen Backtesting

Die verschiedenen Arbeitspakete sind dabei nicht vollständig voneinander getrennt, sondern können (und müssen zumindest teilweise) parallel bearbeitet werden.

Der Aufwand lohnt sich

Für das Treasury ergeben sich beim Wechsel auf eine Portfolio-orientierte Betrachtung und den Einsatz passender Risikomaße wie Cashflow-at-Risk oder Value-at-Risk neue Möglichkeiten. Ein unmittelbarer Vorteil ist die (richtige) Berücksichtigung von Diversifikations- und Cluster-Effekten in der Risikomessung.

Es öffnet sich damit auch die Tür für eine genauere Steuerung unter Abwägung von Risiko und erwartetem Ertrag. Prinzipiell kann so der Wertbeitrag des Treasury vergrößert werden, ohne dass dafür zwangsläufig größere Risiken eingegangen werden müssen.

Die Steuerung kann dabei klassisch über exogene Limite erfolgen, es besteht aber die Option – quasi als weitere Ausbaustufe – Ansätze aus der finanzmathematischen Portfoliotheorie anzuwenden, bei denen über geeignete Optimierungsalgorithmen eine bestmögliche Zusammensetzung des Portfolios bestimmt wird.

Die Umsetzung eines Portfolioansatzes kann dabei sowohl in Teilbereichen erfolgen, also beispielsweise speziell im Währungsmanagement, sie kann aber auch in einen ganzheitlichen Ansatz integriert werden, der sich beispielsweise in Form eines Risk Appetite Frameworks formulieren lässt und der über Märkte oder organisatorische Einheiten hinweg eine einheitliche, konsistente Abwägung zwischen Risiko und Ertrag forciert.

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

Wo liegt nochmal? – Knowledge Management im Finance Bereich

Knowledge Management ist ein allgegenwärtiger Begriff in der Arbeitswelt. Die bekannteste Online Wissensdatenbank „Wikipedia“ beschreibt Knowledge Management zum deutschen Wissensmanagement wie folgt: „Wissensmanagement ist die methodische Einflussnahme auf die Wissensbasis eines Unternehmens (organisationales Wissensmanagement) bzw. eines Individuums (persönliches Wissensmanagement). Unter der Wissensbasis werden alle Daten und Informationen, alles Wissen und alle Fähigkeiten verstanden, die diese Organisation bzw. Person zur Lösung ihrer vielfältigen Aufgaben hat oder haben sollte.“[1]

Im privaten Umfeld haben bekannte Plattformen längst die strukturierte Aufbereitung von Wissen übernommen. Zu Fragen aus der Welt des Sports, Produktrezensionen oder Urlaubsschnäppchen konsultieren wir Suchmaschinen, recherchieren auf Verkaufsplattformen oder bewerten Angebote mittels Vergleichsportalen. All dies sind Wissensdatenbanken, durch die unsere Anliegen schnell und zielsicher beantwortet werden. Im beruflichen Kontext gestaltet sich die strukturierte Wissensbeschaffung weitaus schwieriger, die Geschwindigkeit der privaten Sucherfolge ist nur bedingt übertragbar. Zunächst wird dies regelmäßig der Komplexität des individuellen Sachverhalts geschuldet sein. Zusätzlich sind erhoffte Antworten zumeist schlecht aufbereitet sowie kaum im notwendigen, individuellen Detailgrad verfügbar.

In einer solchen Situation kann eine eigens angelegte Wissensdatenbank Abhilfe schaffen. Diese kann durch diverse Quellen wie der Recherche in der eigens angeschafften Literatursammlung, dem Durchsuchen von historischen Daten in einer ausgefeilten Ordnerstruktur, im E-Mail-Postfach abgelegte Ab-

[1] Wissensmanagement – Wikipedia

stimmungen oder Mitschriften aus OneNote o.ä. gespeist werden. Hierbei sind wir auch auf unser eigenes Erinnerungsvermögen angewiesen, um die Informations- und Datenflut zu überblicken. Herauszufinden, ob und in welcher Form ein aktuell zu bewertender Sachverhalt gegebenenfalls in einem vergangenen Projekt gelöst wurde, wird mit zunehmender Datenmenge immer herausfordernder. Manch einer mag sich an das zerrende Gefühl der niemals endenden Suche nach einer speziellen Datei oder dem Versuch das passende Schlagwort für die E-Mail-Ablage einzugeben, erinnern. Es gibt unzählige Beispiele im Arbeitsalltag, in denen wir auf die Verfügbarkeit von individuellem Wissen angewiesen sind. Betrachten wir die oben dargestellte Definition von Wissensmanagement, so wird insbesondere von „methodischer Einflussnahme auf die Wissensbasis eines Unternehmens“ gesprochen. Ob die sehr verbreitete Vorgehensweise, Inhalte in den Untiefen des eigenen E-Mail-Postfaches zu suchen, die oben stehende Definition einer Methodik erfüllt, sei dem Leser selbst überlassen. Doch selbst wenn jeder Einzelne die eigene Datenlage überblickt, ist diese individuelle Wissensbasis nicht allen Mitarbeitern zugänglich und zudem bei Verlassen des Unternehmens zumeist passé. Der Aufbau einer eigenen Datenbank kann darüber hinaus sehr mühsam sein. Es bedarf sehr häufig viel Interaktion mit Kolleginnen und Kollegen, um die gewünschte Information zu erhalten und für einen erneuten Abruf speichern zu können.

Entscheidet man sich im Unternehmen eine Knowledge Datenbank aufzubauen, so ist in einem ersten Schritt eine umfassende Wissensmanagementstrategie zu definieren. Anschließend sollte eine geeignete, technische Lösung auf dem die Strategie dargestellt werden kann ausgewählt sowie Zugriffsrechte festgelegt werden. Es empfiehlt sich in dieser Phase den Fokus auf das Design des Wissenssystems zu legen und für alle verständlich zu gestalten. Dies ist sehr wichtig, damit eine kontinuierliche Aufnahme neuer Inhalte, Ergänzungen und Korrekturen stattfindet. Die Knowledge Datenbank sollte davon leben fortan weiter bespielt zu werden, anstelle im Zeitpunkt des Go-Live ein möglichst umfassendes und vollständiges Wissensmanagement-Systems darzustellen. Durch die konsequente Einbindung in den Arbeitsalltag wird das so entstandene „Wiki“ zu einer systematischen Ablage von Daten wie Vorlagen, Präsentationen und Verweisen auf Literaturquellen. Ergänzend können schriftliche Ausarbeitungen zu Fragestellungen in Form von Artikeln bereitgestellt werden oder beispielsweise auch mit erläuternden Videosequenzen für spezifische Anwendungsfälle eine weitere Form des Wissenstransfers ergänzt werden. Eine Knowledge Datenbank schafft in einem Umfeld von unendlich verfügbaren Informationen und Antworten eine verlässliche Quelle zur Informationsbeschaffung für Ihr Team und erlaubt darüber hinaus Prozesse und Vorgehensweisen zu standardisieren.

„Als ein Ergebnis des heutigen wissens- und innovationsorientierten Kommunikationszeitalters wird das im Unternehmen vorhandene Wissenskapital immer mehr zum entscheidenden Produktionsfaktor. (…) Diese stellt eine Erweiterung der Auffassung dar, Information (zum Beispiel im Rahmen der Marktgestaltung und -beeinflussung) als betriebliche Ressource bzw. als Produktionsfaktor zu sehen.“[2]

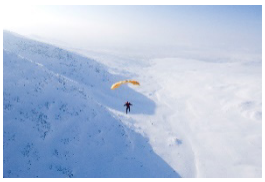
Eine Knowledge Datenbank ermöglicht ein signifikant beschleunigtes Onboarding von neuen Mitarbeitern, ein besseres Enablement sowie Effizienzgewinne bei der Bearbeitung von fachlichen oder administrativen Aufgabenstellungen. Eine solche Plattform kann sich schnell als zentrales Nachschlagewerk etablieren und unterstützt das gesamte Team im daily business. Ein Nebeneffekt kann die reduzierte Ablage von Informationen auf anderen Sharepoints, die über die Jahre in Vergessenheit geraten, sein. Zusätzlich geht relevantes Wissen nicht zwangsweise mit Austritt eines Mitarbeiters verloren und kann stattdessen im Unternehmen gespeichert werden.

Die Nutzung von standardisierten Prozessen, Vorlagen und Wissen spart zeitliche und kognitive Ressourcen, die für die Ausarbeitung von neuen Sachverhalten und Würdigung der Datenqualität benötigt werden. Es entsteht Raum, der für Innovation und Veränderung genutzt werden kann.

Autoren:
Ralph Schilling, CFA, Partner, Head of Finance and Treasury Management, Treasury Accounting & Commodity Trading, KPMG AG
Marie Czentarra, Managerin, Finance and Treasury Management, Treasury Accounting & Commodity Trading, KPMG AG

[2] Wikipedia

Cyber Security im Corporate Treasury: Herausforderungen und Lösungsansätze



Im Zeitalter der Digitalisierung hat die Cyber Security in allen Bereichen der Unternehmensführung, einschließlich des Corporate Treasury, eine zentrale Bedeutung erlangt. Der Treasury-Bereich steht aufgrund seiner zentralen Rolle in der finanziellen Steuerung und der Verarbeitung sensibler Finanztransaktionen besonders im Fokus von Cyberkriminellen. Dieser Artikel beleuchtet die spezifischen Cyber-Gefahrenpotenziale im Corporate Treasury, insbesondere im Zahlungsverkehr und in der Datensicherheit, und erörtert die Anforderungen an Treasury Management Systeme (TMS) zur Erhöhung der Cybersicherheit. Zudem wird untersucht, wie Künstliche Intelligenz (KI) dazu beitragen kann, die Sicherheitsarchitektur im Corporate Treasury zu stärken.

Anlass für diesen Artikel gibt uns, dass in den letzten Jahren die Bedrohung durch Cyberangriffe im Finanzbereich und in anderen Sektoren der Wirtschaft weiterhin erheblich zugenommen hat, sowohl in quantitativer wie auch in qualitativer Hinsicht. Der jährliche Schaden, der der deutschen Wirtschaft durch Cyberkriminalität entsteht, wird auf etwa 206 Milliarden Euro geschätzt. Bemerkenswert ist dabei der steigende Anteil organisierter Kriminalität an diesen Angriffen, wobei 61 % der betroffenen Unternehmen die Attacken auf solche Kriminellen zurückführen.[3] Cyberkriminelle nutzen dabei eine breite Palette von Techniken, einschließlich Phishing, Angriffe auf Passwörter und Ransomware, wobei der Einsatz von künstlicher Intelligenz die Effizienz und Zielgenauigkeit dieser Angriffe weiter erhöht. Die Risikoeinschätzung der Unternehmen hat sich parallel dazu erhöht. Trotz des Bewusstseins für die Gefahren und der zunehmenden Anzahl von Angriffen fühlen sich viele Unternehmen nicht ausreichend vorbereitet. Die Situation gewinnt an Brisanz, wenn man berücksichtigt, dass erhebliche Investitionen in die IT-Sicherheit vorgenommen werden. Beispielsweise wurden gemäß des Bundesamts für Sicherheit in der Informationstechnik in ihrem Lagebericht in 2022 ein Betrag von rund 7,8 Mrd. Euro in Cybersicherheit investiert[4].

Gefahrenpotenziale im Corporate Treasury

Im Folgenden gehen wir auf typische Bereiche im Corporate Treasury ein, die durch Cyber Crime eine Gefahr für das Corporate Treasury darstellen. Diese sind als Beispiele zu verstehen, von denen es noch zahlreiche weitere gibt.

1. **Zahlungsverkehr:**
   Im Zahlungsverkehr stehen Unternehmen vor einer Vielzahl von Gefahren, darunter Phishing-Angriffe, KI-gestützten Identitätsdiebstahl und Malware-Infektionen. Diese Risiken können die Zahlungsverkehrsprozesse direkt bedrohen.
   Ein weiteres, oft unterschätztes Risiko ergibt sich, wenn ein Unternehmen einem Cyberangriff ausgesetzt ist, und dabei muss es nicht einmal die Treasury-Abteilung sein, die direkt angegriffen wird. Die IT-Abteilung könnte in solchen Fällen gezwungen sein, präventiv Systeme und Schnittstellen herunterzufahren, um den Angriff einzudämmen, was unbeabsichtigte Konsequenzen für die Treasury-Abteilung nach sich zieht. Ohne Zugang zu kritischen Systemen wird es schwierig, Zahlungsaufträge an Banken zu übermitteln. Auch die Informationen darüber zu sammeln, welche Zahlungen überhaupt fällig sind, wird ohne IT-Infrastruktur schnell zu einer großen Herausforderung.
   Neben dem Schutz vor unmittelbaren Angriffen durch gängige Sicherheitsmaßnahmen wie Verschlüsselungen und Zwei-Faktor-Authentifizierungen ist es deshalb sinnvoll, Notfallpläne zu haben. Diese Pläne sollten sicherstellen, dass die IT-Abteilung die Zahlungsfähigkeit des Unternehmens auch im Ernstfall unterstützen kann. Auch wenn es logisch ist, wird teilweise einfach übersehen wie groß das Chaos und die Auslastung der IT in einem ernstzunehmenden Angriff ist.

[3] www.forschung-und-wissen.de/nachrichten/oekonomie/gezielte-cyberattacken-auf-deutsche-wirtschaft-13378487

[4] www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8

2. **Datensicherheit:**
   Ein weiteres wichtiges Thema im Bereich der Cyber Security im Corporate Treasury ist die Datensicherheit. Unternehmen im Corporate Treasury verwalten eine Vielzahl von sensiblen Daten, wie zum Beispiel Bank- und Finanzdaten, Kundeninformationen und Geschäftsgeheimnisse. Diese Daten müssen vor unbefugtem Zugriff geschützt werden, um die Integrität und Vertraulichkeit der Daten zu gewährleisten. Eine der größten Bedrohungen für die Datensicherheit sind Hackerangriffe, bei denen Betrüger versuchen, in das Netzwerk des Unternehmens einzudringen und vertrauliche Daten zu stehlen. Die Sicherheit sensibler Finanzdaten ist eine weitere zentrale Herausforderung. Datenlecks können durch externe Angriffe, aber auch durch interne Schwachstellen wie unzureichende Zugriffskontrollen oder menschliche Fehler verursacht werden. Die Folgen sind nicht nur finanzieller Natur, sondern betreffen auch den Verlust von Geschäftsgeheimnissen und Vertrauen in Kunden und Lieferanten. Als Beispiele sind hier Bankdaten, interne Finanzinformationen und Transaktionsinformationen zu nennen.

3. **Fraud Management:**
   Ein weiteres wichtiges Thema im Bereich der Cyber Security im Corporate Treasury ist das Fraud Management. Betrugsversuche haben in den letzten Jahren durch den Einsatz ausgefeilter Techniken zugenommen. Betrüger versuchen oft, Unternehmen im Corporate Treasury zu betrügen, indem sie gefälschte Rechnungen oder Zahlungs-anweisungen einreichen. Auch Fälle von Unterwanderung von Unternehmen durch Kriminelle wurden bekannt. Um sich gegen diese Bedrohungen zu schützen, ist es wichtig, dass Unternehmen im Corporate Treasury ihre Prozesse und Systeme absichern.
   Dazu gehört zum Beispiel die Implementierung von Kontrollmechanismen, um sicherzustellen, dass Zahlungen nur an autorisierte Empfänger geleistet werden. Auch die Überprüfung von Rechnungen und Zahlungsanweisungen auf Unregelmäßigkeiten kann dazu beitragen, Betrug zu verhindern. Oft wird versucht über wiederkehrende Zahlungen in kleinen Beträgen Kontrollen zu umgehen und unter dem Prüfradar zu agieren. Dabei nutzen Betrüger nicht nur technische, sondern auch soziale Schwachstellen aus. Ein Beispiel hierfür ist das CEO-Fraud, bei dem Mitarbeiter durch gefälschte Anweisungen vermeintlich höhergestellter Personen zu Überweisungen verleitet werden.

Welche Maßnahmen können Treasurer ergreifen und welche Anforderungen ergeben sich an Treasury Management Systeme?

Der Treasurer spielt eine Schlüsselrolle bei der Gewährleistung der Cybersicherheit im Unternehmen. Zu den Maßnahmen gehören die Entwicklung und Implementierung von Sicherheitsrichtlinien und -verfahren, die Investition in fortschrittliche Technologien und die Schulung von Mitarbeitern.

Es ist wichtig, dass Unternehmen im Corporate Treasury eine Kultur der Sicherheit fördern. Dazu gehört zum Beispiel die Sensibilisierung der Mitarbeiter für die Bedeutung von Cyber Security und die Einrichtung von Richtlinien und Verfahren zur Sicherung von Daten und Systemen.
Bei der Auswahl von Treasury Management Systemen (TMS) sollten Treasurer darauf achten, dass diese Systeme über fortschrittliche Sicherheitsfunktionen verfügen. Ein modernes TMS sollte auch in der Lage sein, sich nahtlos in andere Sicherheitssysteme zu integrieren, um ein umfassendes Sicherheitsnetz zu schaffen. Folgende Anforderungen sind bei der TMS-Auswahl von besonderer Bedeutung:

1. **Mehrschichtige Sicherheitsarchitekturen:**
   Dazu gehören Firewalls, Verschlüsselungstechniken, Zwei-Faktor-Authentifizierung und regelmäßige Sicherheitsupdates.
2. **Echtzeit-Überwachung und -Analyse:**
   Die Fähigkeit, Transaktionen in Echtzeit zu überwachen und zu analysieren, ist entscheidend, um verdächtige Aktivitäten frühzeitig zu erkennen.
3. **Benutzermanagement und Zugriffskontrolle:**
   Starke Zugriffskontrollen und die Verwaltung von Benutzerberechtigungen helfen, das Risiko interner Bedrohungen zu minimieren.
4. **Compliance und Reporting:**
   Ein TMS muss die Einhaltung relevanter Standards und Vorschriften unterstützen und über effektive Reporting-Funktionen verfügen.

Nutzung von Potenzialen der künstlichen Intelligenz zur Erhöhung der Sicherheit

Neben den oben genannten Funktionen der TMS können KI-Modelle einen wertvollen Beitrag zur Verstärkung der Cybersicherheit im Corporate Treasury leisten.

Die Integration von Künstlicher Intelligenz (KI) in die Cybersicherheitsstrategie des Corporate Treasury bietet innovative Möglichkeiten, um sich gegen eine Vielzahl von Cyberbedrohungen zu wappnen.

Die folgenden Punkte beleuchten detailliert, wie KI zur Stärkung der Cybersicherheit beitragen kann:

1. **Anomalie-Erkennung:**
   KI-Systeme können kontinuierlich große Mengen an Transaktionsdaten analysieren, um Muster zu erkennen und Anomalien zu identifizieren, die auf potenziellen Betrug oder Cyberangriffe hindeuten. Durch das Lernen aus historischen Daten sind KI-Modelle in der Lage, normale von verdächtigen Aktivitäten zu unterscheiden, selbst wenn diese auf den ersten Blick unauffällig erscheinen. Dies ermöglicht eine schnelle Reaktion auf potenzielle Bedrohungen, oft bevor Schaden entstehen kann.
2. **Predictive Analytics:**
   Durch die Nutzung von Predictive Analytics können KI-Systeme zukünftige Risiken vorhersagen, basierend auf Trends und Mustern in den gesammelten Daten. Dies umfasst die Vorhersage von Betrugsversuchen, Cyberangriffen und anderen Sicherheitsverletzungen. Solche Prognosen ermöglichen es Treasury-Teams, präventive Maßnahmen zu ergreifen, um Risiken zu minimieren, bevor sie sich materialisieren.
3. **Automatisierung von Sicherheitsüberprüfungen:**
   KI kann genutzt werden, um Routine-Sicherheitsüberprüfungen zu automatisieren, wodurch die Effizienz erhöht und menschliche Fehler reduziert werden. Dies beinhaltet die automatische Überprüfung von Software-Updates und Sicherheitspatches, die Überwachung von Netzwerkverkehr auf ungewöhnliche Muster und die Durchführung von Schwachstellenanalysen. Die Automatisierung solcher Aufgaben entlastet das IT-Sicherheitsteam, sodass es sich auf komplexere Sicherheitsherausforderungen konzentrieren kann.
4. **Verbesserung der Reaktionszeiten:**
   Im Falle eines erkannten Sicherheitsvorfalls können KI-gestützte Systeme automatisch vordefinierte Abwehrmaßnahmen einleiten, um den Schaden zu begrenzen. Dies beinhaltet das Isolieren betroffener Systeme, das Blockieren verdächtiger IP-Adressen und das Erstellen von Sicherheitskopien wichtiger Daten. Die Fähigkeit zur sofortigen Reaktion verringert die Auswirkungen von Cyberangriffen erheblich und kann in einigen Fällen den Angriff vollständig neutralisieren, bevor er sich ausbreiten kann.
5. **Anpassungsfähigkeit und Lernen:**
   Ein herausragendes Merkmal von KI-Systemen ist ihre Fähigkeit zu lernen und sich anzupassen. Da Cyberbedrohungen sich ständig weiterentwickeln, ist die Fähigkeit eines Sicherheitssystems, aus neuen Angriffsmethoden zu lernen und seine Verteidigungsmechanismen entsprechend anzupassen, entscheidend. KI-Modelle werden kontinuierlich mit neuen Daten trainiert, was ihre Effektivität im Laufe der Zeit verbessert.

Die Integration von KI in die Cybersicherheitsmaßnahmen des Corporate Treasury ermöglicht somit nicht nur die effektive Bekämpfung aktueller Bedrohungen, sondern auch eine proaktive Vorbereitung auf zukünftige Risiken. Durch die Kombination von menschlicher Expertise mit der Leistungsfähigkeit der KI können Unternehmen ein robustes Sicherheitsnetzwerk aufbauen, das der ständig wechselnden Landschaft der Cyberbedrohungen gewachsen ist.

Fazit und Ausblick

Die Bedeutung der Cybersicherheit im Corporate Treasury nimmt stetig zu, angetrieben durch die Digitalisierung und die fortschreitende Professionalisierung von Cyberkriminellen. Diese Entwicklung stellt Treasury-Abteilungen vor große Herausforderungen, die ein umfassendes Risikomanagement, Datensicherheit und effektives Fraud Management erfordern. Der Treasurer spielt dabei eine zentrale Rolle in der Entwicklung und Implementierung von Sicherheitsstrategien, einschließlich der Auswahl von Treasury Management Systemen mit fortschrittlichen Sicherheitsfeatures und der Förderung von Mitarbeiterbildung.

Die Integration von KI-Technologien wie Anomalie-Erkennung, Predictive Analytics und automatisierten Sicherheitsüberprüfungen verspricht eine signifikante Verstärkung der Cybersicherheitsmaßnahmen. Diese Instrumente ermöglichen es, aktuelle und zukünftige Bedrohungen proaktiv zu identifizieren und zu bekämpfen.

Effektiver Schutz vor Cyberbedrohungen erfordert dynamische und anpassungsfähige Abwehrstrategien, kontinuierliche Schulung und Sensibilisierung der Mitarbeiter sowie eine enge Zusammenarbeit zwischen dem Treasury, IT-Sicherheit und externen Partnern.

Die Zukunft der Cybersicherheit im Corporate Treasury hängt maßgeblich von der Fähigkeit ab, sich schnell an neue Bedrohungen anzupassen, innovative Sicherheits-technologien zu implementieren und eine starke Si-cherheitskultur im Unternehmen zu etablieren.

Autoren:
Börries Többens, Partner, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG
Nils Bentzien, Manager, Finance and Treasury Management, Corporate Treasury Advisory, KPMG AG

Impressum

Herausgeber

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt

Redaktion

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

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

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

Newsletter kostenlos abonnieren

www.kpmg.de

www.kpmg.de/socialmedia