



Marcus Chromik

Welche Anforderungen stellt der technologische Wandel an die Regulierung von morgen?

Das Risikomanagement von Banken hat sich in den vergangenen zehn Jahren grundlegend geändert. Treibende Kraft war die gemeinsame Anstrengung von Politik, Regulierung, Aufsicht und Banken selbst, Fehler, die zur Finanzmarktkrise führten, künftig zu vermeiden. Risikomodelle wurden überarbeitet, Kapitalanforderungen verschärft und der Umgang mit Bestandsrisiken konsequenter geregelt. Zudem wurden Feuerschneisen zwischen den Banken durch die Stärkung der Rolle von Clearinghäusern und – für den Fall der Fälle – auch durch Abwicklungsszenarien und -prozeduren gezogen.

Weites Aufgabenspektrum für CROs

Das Tempo des Wandels wird sich in den kommenden Jahren noch weiter verstärken. Treibende Kraft werden moderne Technologien sein, die völlig neue Optionen zur Risikoerkennung und -steuerung eröffnen. Die Chancen, die sich hinter den Schlagwörtern Big Data, Advanced Analytics, Artificial Intelligence und Internet of Things verbergen, machen das Risikomanagement in diesen Zeiten so spannend.

Mit den neuen technologischen Möglichkeiten ändern sich aber auch die Erwartungen der Kunden. Sie fordern zunehmend ein intuitives Kundenerlebnis. Sie wollen Leistungen jederzeit und auf jedem Endgerät in Anspruch nehmen. Vor allem aber erwarten sie individualisierte Angebote und schnelle Entscheidungen. Das setzt eine starke Automatisierung von Prozessen – auch des Risikomanagements – voraus. Gleichzeitig wandelt sich

auch die Art der Risiken. Heute steht auf der Prioritätenliste von Risikovorständen viel mehr als klassische Risiken wie Kreditrisiken: Banken müssen sowohl für das eigene Haus als auch für ihre Kunden Cyberrisiken abwehren, Geldwäsche und Terrorismusfinanzierung aufdecken sowie die Folgen des technologischen Wandels bewerten. Ein zukunftsweisendes Risikomanagement muss daher alle verfügbaren Daten auswerten, vernetzt denken und handeln.

Voraussetzung für diese Innovation ist aber auch eine zeitgemäße Regulierung. Dazu zählt zum Beispiel eine deutlich schnellere und flexiblere Genehmigung von Risikomodelle. Vor allem das exponentielle Wachstum verfügbarer Daten wird extrem schnelle Modellanpassungen erfordern. Der Umgang mit und die Akzeptanz von Wahrscheinlichkeiten muss von den klassischen Risikoarten auch auf die sogenannten Non-Financial Risks ausgedehnt werden. Denn: Auch die Regulierung muss den technologischen Wandel positiv begleiten und darf nicht in der analogen Welt stehenbleiben.

Es sind spannende Zeiten für das Risikomanagement – Zeiten des Umbruchs, aber auch des Aufbruchs mit zahlreichen neuen technologischen Möglichkeiten und nahezu unerschöpflichen Datenquellen. Risikomanager in Banken können qualitativ hochwertige, komplexe Analysen durchführen und idealerweise in Echtzeit zu Entscheidungen gelangen.

Es ist kein Geheimnis, dass andere Branchen bei Big Data und Advanced Analytics schon viel größere Fortschritte gemacht haben. Google, Amazon und Co.

sind allen anderen Industrien Meilen voraus. Banken sind durch die Bewältigung der Finanzkrise sicherlich in den Rückstand geraten – doch das ändert sich jetzt. Denn nun holt die Branche auf. Auch die Commerzbank richtet sich strategisch neu aus und investiert konsequent in Digitalisierung, Big Data und durch Advanced Analytics gesteuerte Geschäftsprozesse.

Bessere Entscheidungen durch neue Technologien

So sind das Datenmanagement, die Datenanalyse und das Ableiten von Handlungsentscheidungen etwa ein wesentlicher Bestandteil der Strategie und der operativen Effizienz. Wenn Kunden erwarten, dass sie in Sekundenschnelle Bankgeschäfte abwickeln können, muss die Bank in noch kürzerer Zeit Risikobewertungen treffen. Und das ist nur unter Einsatz neuester Technologien möglich.

Das heißt: Risikomanagement, Compliance oder der Finanzbereich sind nicht länger nur für die finanzielle Stabilität und die Einhaltung von Regeln einer Bank von grundlegender Bedeutung. Sie sind zunehmend ein wesentlicher Bestandteil des operativen Geschäftserfolgs. Neue Technologien wie Big Data, Advanced Analytics und Artificial Intelligence werden auch im Risikomanagement von Banken genutzt, um das Geschäftsmodell zu digitalisieren und dadurch zu besseren und schnelleren Entscheidungen zu gelangen.

Das ist nicht nur spannende Theorie, sondern ist zunehmend Realität. Dazu einige

Beispiele aus der Praxis des Risikomanagements:

Die Diskussion um die Abgasmanipulation hat die Autoindustrie in Deutschland in Aufruhr versetzt. Sollte man als Bank deshalb das Engagement der ganzen Branche begrenzen? In der Vergangenheit war es Praxis, eine ganze Branche konservativ zu behandeln. Bei ihrer Bedeutung für die deutsche Wirtschaft wäre das ein massiver Einschnitt. Und: die Geschäfte der Zulieferer von Bremsen, Sitzen oder Karosserien laufen unverändert gut.

Die Commerzbank hat deshalb mithilfe von Big Data schnell und gezielt analysiert, welche Lieferanten tatsächlich vom sogenannten Dieseldiebstahl betroffen sind. Pro Automobilhersteller wurde die Anzahl von Zulieferern in der ersten und zweiten Ebene gezählt. Eine zeitnahe manuelle Untersuchung zur Ableitung von Risikoentscheidungen ist hier nicht möglich. Durch eine Auswertung sämtlicher Zahlungsverkehrsströme mit der Koppelung der Daten aus den Jahresabschlüssen konnte die Zahl von Zulieferern mit großer Abhängigkeit stark eingegrenzt werden und lediglich 100 Unternehmen mussten manuell untersucht werden. Am Ende wurden lediglich fünf Unternehmen von rund 12000 Lieferanten als kritisch bewertet. Die Verbindung von Big Data und darauf aufsetzender menschlicher Expertenanalyse erlaubt bei solchen Fragestellungen ein viel präziseres Risikomanagement. Dagegen hätte eine manuelle Auswertung aller Einzelengagements vermutlich Jahre gedauert.

Einsatz selbstlernender Systeme

Auch in der Abwehr von Cybercrime setzt die Bank auf neueste Technologien. Dabei geht es unter anderem auch um den Schutz der Kunden: Die Commerzbank hat bereits frühzeitig das Thema CEO-Fraud erkannt. Hierbei geht es beispielsweise um das Risiko, dass durch eine gefälschte E-Mail des Vorstandsvorsitzenden einem Prokuristen die Anweisung erteilt wird, einen höheren Geldbetrag auf ein bestimmtes Konto zu überweisen.

Dies kann für den Kunden schwere Folgen haben und ultimativ sogar zu einem Kreditereignis führen, wenn der Schaden existenzbedrohend hoch sein sollte.

Bei der Abwehr von Cybercrime arbeitet die Commerzbank aktiv mit Behörden und Organisationen zusammen. Gewonnene Erkenntnisse und entschlüsselte Transaktionsmuster aus Angriffsvektoren wie Wanna-Cry oder Non-Petya fließen permanent in Abwehrmaßnahmen ein. Dieses durch selbstlernende Systeme (Advanced Analytics) erzielte Wissen stellt die Bank auch ihren Kunden zur Verfügung.

So ist die Commerzbank bei der Verhinderung von CEO-Fraud ein angesehener Partner des Mittelstands geworden. Die Erfolgsquote bei der Abwehr von solchen Betrugsversuchen ist mit über 99 Prozent im vergangenen Jahr hervorragend. Dadurch konnten allein 2017 von den Kunden beauftragte Auszahlungen von mehr als 100 Millionen Euro von der Bank gestoppt werden. Das heißt, in diesen Fällen hatte der Betrug aufseiten des Kunden zwar funktioniert, die Commerzbank konnte die Überweisung aber als risikoreich identifizieren und stoppen. Klassische regelbasierte Mechanismen sind hier meist zu grob und unflexibel zur Risikoidentifikation. Vor allem können sie nicht schnell genug auf veränderte Angriffsmuster reagieren. Selbstlernende Algorithmen sind – eingesetzt in eine schnelle und leistungsfähige technische Umgebung – deutlich besser.

Schließlich: Banken werden von der Politik und der Regulierung immer stärker dazu verpflichtet, illegale und unethische Finanztransaktionen, Geldwäsche oder Terrorismusfinanzierung aufzudecken. Das ist wichtig und richtig. Denn für jeden Mitarbeiter wäre es ein Albtraum, wenn beispielsweise ein Terroranschlag über seine Bank finanziert worden wäre. Terrorismus wird eben nicht mehr wie in den siebziger Jahren über Banküberfälle finanziert, sondern über hochkomplexe Geldströme, in denen das Geld gewaschen werden soll. Das gilt es immer und ausnahmslos zu verhindern. Auch für die Bekämpfung und Aufdeckung von sol-

chen kriminellen Systemen werden zunehmend selbstlernende Modelle eingesetzt. Dadurch lässt sich die Zahl von falschen Verdachtsfällen deutlich reduzieren und somit die Kapazität und Energie auf die wirklich kritischen Fälle konzentrieren. Das zeigen schon jetzt die ersten Erfahrungen.

Verlässliche Regeln und klare Wegmarken erwünscht

Digitalisierung ist eine große Chance für Deutschland und Europa. Digitalen Geschäftsprozessen gehört die Zukunft. Das gilt natürlich auch für die Prozesse und Methoden im Risikomanagement von Banken. Doch um das gesamte Potenzial zu nutzen und die Effizienzvorteile zu heben, sind entsprechende technische, regulatorische und rechtliche Anpassungen notwendig. Wichtig ist, dass Politiker und Regulatoren schnell verlässliche Regeln und klare Wegmarken für Europa festlegen, die dem rasanten Wandel der europäischen Wirtschaft gerecht werden. Und dies, bevor zum Beispiel amerikanische Standards sich durchsetzen.

Dazu muss Regulierung aber auch die Chancen der neuen Technologien annehmen. Und das bedeutet unter anderem schnellere und neue Genehmigungsprozesse. Ein Beispiel: Beim Risikomanagement sind Banken verpflichtet, nicht nur eigene, sondern auch komplementäre Datenquellen zu nutzen, sofern der Aufwand ökonomisch vertretbar ist. In der Vergangenheit war die Anbindung neuer Datenquellen eher eine Seltenheit, da der Prozess zu teuer und komplex und mit einem erheblichen Zeitaufwand verbunden war. Durch die neuen, schnellen Programmierschnittstellen (Application Programming Interface, kurz API) verkürzt sich dieser Schritt auf wenige Wochen. Nur: Wenn externe Datenquellen eine wichtige und sinnvolle Quelle für Risikobewertung sein können, dann müssen Regulatoren auch deren Anbindung akzeptieren und schneller genehmigen.

Aber nicht nur das Tempo ist entscheidend. Regulatoren werden auch viel häufiger mit Genehmigungsprozessen kon-

frontiert sein. Denn Banken nutzen für ihre Risikobewertung zunehmend selbstlernende Modelle und verbessern dadurch ihre Modelle stetig weiter. Damit erzeugen sie im Prinzip immer wieder genehmigungspflichtige Modelländerungen.

Hinzu kommt: Aufgrund immer höherer Rechnerleistungen können Banken riesige Datenmengen genauer erfassen und auswerten. Insbesondere bei Portfolios mit zahlreichen Datenpunkten kann das Risikomanagement komplett automatisierte Kreditentscheidungen treffen. Dies ist beispielsweise bei granularen Kreditportfolios wie bei kleineren Mittelständlern, Retailkunden oder Baufinanzierungen der Fall.

Auch können wichtige Aufgaben bei der Kreditgewährung oder Überwachung künftig automatisiert ablaufen. Dazu gehören unter anderem das Ableiten der Haushaltsüberschussrechnung und damit der Kapitaldienstfähigkeit eines Kunden aus den Kontodaten. Das gilt aber auch für die Plausibilitätsprüfung der Unternehmensstruktur und Kennzahlen aus verschiedenen verfügbaren Datenquellen.

Darüber hinaus können Unstimmigkeiten zwischen verschiedenen Datenquellen schnell aufgezeigt werden. Durch automatisches Einlesen (Optical Character Recognition) können auch solche Dokumente, die nur papierhaft vorliegen, für die automatisierte Bonitätsbeurteilung, Betrugsabwehr und laufende Überwachung herangezogen werden.

Deshalb sollte das Kriterium, welchen Kredit man wie oft und mit wie vielen Mitarbeitern überprüfen muss, nicht an einer Pauschalgröße festgemacht werden. Entscheidend sollte vielmehr die relative Größe des Kredits sein, die Tatsache, wie viele Fallzahlen zur jeweiligen Forderungskategorie verfügbar sind oder welche zusätzlichen Daten zur Früherkennung und Plausibilisierung genutzt werden können.

Versandhändler wie Zalando oder Amazon können seit Jahren die Bonität ihrer

Kunden dank modernster Analysemethoden mit internen Modellen beurteilen und so in Sekundenschnelle über die Vorauszahlung eines Kunden entscheiden. Da möchten und müssen die Banken auch hinkommen, auch um dem Wettbewerb von Fintechs standhalten zu können. Regulierung muss den Banken dafür aber die Voraussetzungen bieten.

Umgang mit Wahrscheinlichkeiten

Klar ist: Es darf dabei keine Modellartefakte stattfinden und die Einhaltung von bestimmten Prinzipien muss gewahrt sein. Ein über viele Jahre angelegter Prozess zur Überprüfung der Modelle (TRIM) ist dabei fundamental. Wenn der Regulator sich aber nicht nur mit theoretischen Risiken beschäftigen möchte, sondern mit realen Anwendungsfällen, dann dürfen sich regulatorische Risikobewertungsmodelle nicht von den ökonomischen Entscheidungsmodellen wegentwickeln.

Wie wird künftig mit Wahrscheinlichkeiten umgegangen? Bei klassischen manuellen Prozessen beispielsweise beobachtet man im Nachhinein immer eine gewisse Fehlerrate, selbst in Prozessen, die nach dem Vier-Augen-Prinzip erfolgen. Durch den Einsatz von Big Data und Advanced Analytics kann man heute im Voraus einschätzen, wie hoch der Fehleranteil ist. Und die Quote ist meistens niedriger als in manuellen Prozessen.

Besteht aber die Bereitschaft, die Untersuchung von Geldwäscheverdachtsfällen einem selbsterkennenden Algorithmus zu überlassen? Auch wenn bekannt ist, dass der Algorithmus in einem Prozent der Fälle nicht gesehen wird, aber die Quote wesentlich besser ist als in der manuellen Analyse?

Big Data und Advanced Analytics als Motor für Strategie und Effizienz

Mit Big Data und Advanced Analytics gelingt es deutlich schneller und besser, kritische Fälle zu identifizieren und falsche Positivbefunde, die unnötig Kapazität



Foto: Commerzbank AG, Alexandra Lechner

Dr. Marcus Chromik

Mitglied des Vorstands, CRO,
Commerzbank AG, Frankfurt am Main

Die Bandbreite der Risiken, die die zuständigen Vorstände in der Kreditwirtschaft heute im Auge haben müssen, hat sich aus Sicht des Autors weit über klassische Felder wie beispielsweise das Kreditrisiko ausgeweitet. Seinem Verständnis nach muss ein zukunftsweisendes Risikomanagement alle verfügbaren Daten auswerten, vernetzt denken und handeln. Als Voraussetzung für diese Innovation sieht er aber auch eine zeitgemäße Regulierung an, beispielsweise eine deutlich schnellere und flexiblere Genehmigung von Risikomodellen. Vor allem angesichts des exponentiellen Wachstums verfügbarer Daten hält er extrem schnelle Modellanpassungen für erforderlich. Seine Botschaft: Auch die Regulierung muss den technologischen Wandel positiv begleiten und darf keineswegs in der analogen Welt stehenbleiben. (Red.)

binden, signifikant zu reduzieren. Im Sinne der Sicherheit für das Finanzsystem sollte der wesentliche Vorteil einer schnelleren Verdachtsmeldung überwiegen.

Big Data und Advanced Analytics werden im digitalen Zeitalter zum Motor eines jeden Unternehmens. Sie sind nicht nur entscheidend für Stabilität und Compliance, sondern sind in der heutigen Zeit wesentlicher Teil der Strategie und Effektivität einer Bank. Wünschenswert wäre, dass auch Regulierung diese Ziele stützt und fördert: Banken benötigen dringend eine Regulierung 4.0.