Richtlinie nimmt Banken in die Pflicht

Das Geldwäschegesetz ist ein heißes Eisen. Bei Nachlässigkeit und Gesetzesverstoß drohen harte Strafen – auch für Unternehmen und Finanzinstitute.

Von François Baumgartner

Im Kampf gegen Geldwäsche kommt auf Banken ein Mehraufwand zu. Foto: Edler von Rabenstein - stock.adobe.com

OSTBAYERN. Seit Juni 2017 ist das Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen in Kraft. Die Novelle soll den Kampf gegen Geldwäsche, Terrorfinanzierung und Korruption erleichtern. Vor allem Banken stehen von jetzt an in der Pflicht, die gesamte Transaktionsatmosphäre zu dokumentieren. Der Gesetzgeber will bei jeder verdächtigen Überweisung nicht nur Sender und Empfänger, sondern auch alle wirtschaftlich Berechtigten im Hintergrund kennen. Bankseitige und umfangreichere Verdachtsmeldungen müssen an die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) bei der Generalzolldirektion übermittelt werden.

Helfen soll hierbei ein elektronisches Transparenzregister. „Diese Finanztransaktionsanalysen führen zu mehr Kontrollaufwand“, erklärt Markus Bender, Partner im Bereich Anti Financial Crime bei Capco. Unternehmen und insbesondere Geldhäuser sollten daher ihre IT-Systeme und Anti-Money-Laundering(AML)-Bereiche fortan prüfen, da bei Leichtsinn, Nachlässigkeit oder Gesetzesverstoß vor allem Finanzinstituten harsche Auflagen und hohe Geldbußen drohen. „Bei schwerwiegenden und wiederholten Gesetzesverstößen stehen Strafen von bis zu fünf Millionen Euro oder bis zu zehn Prozent des Jahresumsatzes im Raum“, warnt Bender.

Wer sich zu den neuen regulatorischen Bemühungen des Gesetzgebers sowie zum aktuellen Status quo interner Bankprozesse informieren möchte, stößt bei ostbayerischen Stadtsparkassen und anderen Banken auf wenig Gesprächsbereitschaft. Doch andere wagen sich aus der Deckung: „Es gibt keine eindeutigen Merkmale oder Muster für Terrorfinanzierung. Viele Transaktionen und das damit verbundene Grundgeschäft weisen vordergründig Ähnlichkeiten mit ganz normalen Kauf- und Bezahlvorgängen auf“, moniert Dr. Indranil Ganguli, Leiter der Zentralen Stelle für Betrugs- und Geldwäscheprävention bei der GenoTec GmbH, die zur Genossenschaftlichen Finanzgruppe Volksbanken Raiffeisenbanken gehört. Dr. Ganguli weiter: „Doch das Klagen über eine überbordende Regulatorik hilft nicht. Das Umsetzungsgesetz erwartet ein gewisses Maß an Recherchetätigkeiten von Banken, die durchaus in die Nähe von Vorermittlungen zu rücken sind.“

Das sieht Markus Bender von Capco ähnlich: „Der Gesetzgeber sollte den Kampf gegen Kriminalität nicht allein auf die Banken auslagern, sondern die entsprechenden Aufdeckungsbehörden mit Mitteln ausstatten. Banken können dazu naturgemäß nur einen kleinen Beitrag leisten, denn sie sind nicht die Behörde, die dazu befähigt ist, die wirtschaftlichen Akteure zu überwachen.“ Darüber hinaus nehmen auch Cyberattacken immer mehr zu, was Unternehmen und Finanzinstituten ebenso zu schaffen macht.

Stellt sich die Frage, wie man Geldwäsche, Terrorfinanzierung, Korruption und Cyberkriminalität als ehrbarer Kaufmann frühzeitig erkennen und präventiv handeln kann. Die bankseitige Abgabe der Verdachtsmeldungen scheint auf den ersten Blick ein leichtes Unterfangen zu sein. Doch hier ist Vorsicht geboten. Die pflichtgemäße Erfüllung erfordert intelligente und nachrüstbare IT-Systeme sowie effiziente Prozessabläufe. „Die IT-Infrastruktur muss verdächtige Transaktionen erkennen und Verdachtsmeldungen an die FIU weiterreichen können, und zwar wie von der Regulatorik definiert, also im gesetzlich vorgegebenen Format mit allen Informationen“, betont Bender und ergänzt: „Die Mitarbeiter können durch Trainingseinheiten und klare Arbeitsanweisungen für solche Aufgaben geschult werden.“ Und wie sieht die optimale IT-Infrastruktur aus? „Gefragt sind heute Anwendungen, die sich schnell an neue Anforderungen anpassen lassen. Dieser scheinbare Widerspruch lässt sich durch eine sogenannte bimodale IT respektive eine ‚IT der zwei Geschwindigkeiten‘ lösen. Altbewährte vorhandene Systeme tun weiterhin ihren Dienst, werden aber durch innovative Lösungen, insbesondere an der Kundenschnittstelle, ergänzt und liefern die dringend benötigte Flexibilität“, sagt Dr. Lars Rüsberg, Berater bei afb Application Services AG, einem europaweit agierenden Gesamt-Dienstleister für digitale Prozesse mit Geschäftssitz in München.

Wer sich dagegen vor Cyberkriminalität schützen möchte, sollte darauf achten, dass die vorhandene Hard- und Software über stets aktualisierte Betriebssysteme und Virenschutzprogramme verfügt. Überdies sollten Mitarbeiter zu diesem Thema informiert und dafür sensibilisiert werden. Der Grund: Oftmals gehen die Täter manipulativ vor. Sie geben sich beispielsweise als Vorstand oder Geschäftsführer eines anderen Unternehmens aus, um Überweisungen einzufordern. Deshalb sind nachvollziehbare Arbeitsanweisungen und Prozessbeschreibungen, die Überprüfung von Informationen eines Transaktionspartners, die Aufklärung der Mitarbeiter zu Betrugsmustern sowie klare Abwesenheitsregeln und Kontrollmechanismen unverzichtbar.