Banken gehen gegen Terroristen vor

Die Bekämpfung von Terrorfinanzierung, Geldwäsche und Korruption wird seit Juni strenger gesetzlich geregelt. Bei Nachlässigkeit oder gar Verstößen drohen Kreditinstituten hohe Geldbußen. Sie müssen nun regelmäßig ihre IT-Systeme und Anti-Money-Laundering-Prozesse prüfen.

François Baumgartner

Die 4. Geldwäscherichtlinie der Europäischen Union (EU) schreibt vor, dass sich Unternehmen für zweifelhafte Finanztransaktionen rechtfertigen müssen. Zwar ist der Strafrahmen für Terrorfinanzierung relativ neu, allerdings kann ein Tatbestand seither zwischen sechs Monaten und zehn Jahren Haft zur Folge haben.

Zurzeit ist die Deutsche Bank, zu deren Kunden die Marxistisch-Leninistische Partei Deutschlands (MLPD) gehören soll, dem Vorwurf der Terrorfinanzierung ausgesetzt. Die potenzielle Verbindung der MLPD zu einer terroristischen Vereinigung, der Volksfront zur Befreiung von Palästina (PFLP), sorgte jüngst für Unmut bei New Yorker Behörden. Ein weiteres Beispiel ist der Zementhersteller Lafarge Holcim, der in Syrien bewaffnete Extremisten bezahlt haben soll, damit ein Werk in Dschalabija im Norden des Landes in Betrieb bleiben konnte. Nun ermitteln drei Untersuchungsrichter gegen das Unternehmen wegen Terrorfinanzierung und Gefährdung des Lebens anderer.

Kontrollaufwand in Instituten steigt

Die Gesetzesnovelle soll Terrorfinanzierung, Geldwäsche und Korruption entgegenwirken, und zwar mithilfe eines elektronischen Transparenzregisters, das auch von Unternehmen aus der Finanzwirtschaft gefüllt werden soll. „Banken stehen von nun an in der Pflicht, die gesamte Transaktionsatmosphäre zu dokumentieren. Der Gesetzgeber will bei jeder verdächtigen Transaktion nicht nur Sender und Empfänger, sondern ebenso alle wirtschaftlich Berechtigten im Hintergrund kennen“, erläutert Andreas Peters, Partner im Bereich Financial Crime beim Software-Dienstleister Capco.

© Phase4Photography/Fotolia

Kompakt

- Geldhäuser müssen die neuen gesetzlichen Vorgaben gegen Straftaten wie Terrorfinanzierung erfüllen.
- Dazu kommen Cyber-Angriffe auf Banken, bei denen neben Datenklau und Vermögensdelikten auch terroristische Motive möglich sind.
- Die IT-Systeme müssen auf ihre Widerstandsfähigkeit überprüft werden.
- IT-Mitarbeiter müssen zur Abwehr von Attacken regelmäßig und umfassend geschult werden.

„Sowohl bei der Ermittlung der wirtschaftlich Berechtigten als auch bei Kundeninvestigationen geht es darum, sich aller öffentlich zugänglichen Informationen zu bedienen, um die wahre Identität des Kunden und der wirtschaftlich Berechtigten herauszufinden. Dazu gehört unter anderem auch, eine Gesamtrisikoeinschätzung des Kunden vorzunehmen." Verdachtsmeldungen müssen Banken und Sparkassen an die Zentralstelle für Finanztransaktionsuntersuchungen (FIU) bei der Generalzolldirektion übermitteln. Gesetzesverstöße können bis zu fünf Millionen Euro Strafe kosten.

Solche Finanztransaktionsanalysen führen zu mehr Kontrollaufwand und stellen für die zum Teil veralteten IT-Systeme in Deutschlands Geldhäusern eine große Herausforderung dar. Die neuen regulatorischen Bemühungen stoßen deshalb auf Kritik. „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", sagt Indranil Ganguli, Leiter der Zentralen Stelle für Betrugs- und Geldwäscheprävention bei der zur genossenschaftlichen Finanzgruppe gehörenden Genotec. „Wie wollen Sie beurteilen, ob das Zelt für den Urlaub gedacht ist oder etwa im Ausbildungscamp in Syrien genutzt werden soll?" Für Banken sei es jedenfalls sehr schwierig, wenn nicht sogar unmöglich, die wahren Hintergründe der Transaktionen aufzudecken. Den Instituten fehlten Informationen, Ermittlungskompetenzen und Ressourcen. Deshalb seien externe Spezialisten und deren Wissen für Banken nahezu unverzichtbar.

Das sieht Lars Rüsberg, Berater bei AFB Application Services, ähnlich. „Eine Auffälligkeitsanalyse des Zahlungsverkehrs sowie beobachtbare Anomalien bei Bargeldzahlungen bilden die Basis für eine Gesamtbeurteilung einer Kundenbeziehung, die bei Bedarf zur einer Kündigung der Kontoverbindung führen kann. Hierbei können spezialisierte Services von Dienstleistern unterstützen, die nahtlos in den bestehenden Systemkontext der Bank eingebunden werden", sagt Rüsberg. Terroristen sind seiner Meinung nach in gewisser Weise Pioniere im negativen Sinne, sobald es um den Missbrauch neuer Technologien geht.

Die Unterschiede zwischen Terrorfinanzierung, Geldwäsche, Korruption und Cyber-Crime hat der Gesetzgeber zwar genau definiert, doch die Übergänge sind fließend, wie ein neuer Vorschlag der Europäischen Kommission zeigt. Demzufolge soll der illegale Handel mit Kulturgütern und deren Einfuhr in die Europäische Union (EU) vollständig unterbunden werden. Denn laut Einschätzung der Brüsseler Behörde sind unter anderem die Plünderung archäologischer Stätten sowie der illegale Verkauf der Beute eine weitere Finanzierungsquelle für Terroristen.

Schutzschilder gehen hoch

Die pflichtgemäße Erfüllung der Gesetzeslage erfordert intelligente und nachrüstbare IT-Systeme sowie effiziente Prozessabläufe in Banken und Sparkassen. „Die Infrastruktur muss verdächtige Transaktionen effektiv erkennen. Ferner muss sie in der Lage sein, Verdachtsmeldungen an die FIU weiterreichen zu können. Und zwar wie von der Regulatorik definiert, sprich im gesetzlich vorgegebenen Format mit allen Informationen", erklärt Peters von Capco. Um gravierende Fehlentscheidungen der Mitarbeiter zu vermeiden, sei es überdies sehr wichtig, dass in der Prozesskette die Funktionstrennung zwischen Organisationseinheiten zur Vermeidung von möglichen Interessenkonflikten vorgenommen wird und bei Bedarf ein Vier-Augen-Prinzip konsequent zur Anwendung kommt. Peters betont: „Die Mitarbeiter können durch Trainings und klare Arbeitsanweisungen, die auch Dilemma-Situationen beinhalten, für neue Aufgaben befähigt werden." ■

Autor: François Baumgartner ist freiberuflicher Journalist, Kommunikationsmanager und Berater für Unternehmen aus der Finanzwirtschaft sowie der Technologie- und Medienindustrie.

Neue Gesetzeslage

Terrorismusfinanzierung § 89c StGB	Geldwäsche § 261 StGB	Korruption § 299 StGB	Cyber-Crime § 202b und c StGB
■ Gefährdung des demokratischen Rechtsstaats ■ Politische und ideologische Aspekte im Vordergrund	■ Verdecktes Einschleusen illegal erworbener Vermögenswerte in den legalen Wirtschaftskreislauf ■ Persönliche und ökonomische Faktoren im Vordergrund	■ Bestechlichkeit und Bestechung im geschäftlichen Verkehr ■ Persönliche und ökonomische Faktoren im Vordergrund	■ Angriffe auf Daten- oder Computersysteme ■ Typ I: Phishing, Vermögensdelikte ■ Typ II: unter anderem Erpressung, Manipulation, Spionage, Planung und Durchführung von Terroranschlägen

Quelle: Strafgesetzbuch (StGB), Deutschland