Die Motive eines Angestellten, seiner Bank Schaden zuzufügen, sind vielfältig. Die Dunkelziffer der Delikte ist hoch.

BILD: ISTOCKPHOTO

INTERNER BETRUG UND WHISTLEBLOWING

Der Feind in der Bank

Der Faktor Mensch ist nicht vollständig kontrollierbar. Das hat der «Fall Hildebrand» wieder gezeigt. Die beste Prävention ist eine gesunde Mitarbeiterkultur.

JOHANNES J. SCHRANER

Müssen Banken den Feind im eigenen Haus fürchten? Der «Fall Hildebrand» in der Bank Sarasin ist ein Hinweis. Eine Umfrage von Ernst & Young bei 100 deutschen Kreditinstituten bestätigt ihn: 39 Prozent der befragten Banken gehen von einer erhöhten Wahrscheinlichkeit aus, durch Fehler oder Betrug von Angestellten einen Schaden zu erleiden. Bei 11 Prozent der befragten Finanzdienstleister wurde in den letzten zwei Jahren mindestens ein Betrugsfall bekannt. Die Dunkelziffer der tatsächlichen Schadensfälle sei viel höher, vermuten die Studienverfasser. «Unzufriedenheit und das Gefühl, unterbezahlt zu sein beziehungsweise mehr zugut zu haben, können die Motive sein», meint Compliance-Spezialistin Monika Roth, Dozentin am Institut für Finanzdienstleistungen Zug IFZ. Ebenfalls seien Gier, ein überhöhter Lebensstil, ein geringes Selbstwertgefühl und der Wunsch auch dazuzugehören mögliche Triebkräfte für solche Taten.

Soziale Kontrolle ist wichtig

«Nicht immer wollen sich Betrüger persönlich bereichern», bestätigt Dirk Müller-Tronnier, Leiter Bankenberatung von Ernst & Young in Deutschland. Oft versuchten Banker einfach, besser dazustehen, um ihre Stellung innerhalb des Unternehmens zu sichern. Wie aber kann dieser Feind im Haus bestmöglich unter Kontrolle gehalten werden?

«Die soziale Kontrolle spielt in diesem Zusammenhang eine grosse Rolle», betont Roth weiter.

Eine informelle Umfrage der «Schweizer Bank» ergab ein differenziertes Bild, wie in den Banken mit dem heiklen Thema umgegangen wird. «Die Zürcher Kantonalbank erwartet, dass sich die internen und externen Mitarbeitenden aller Stufen untereinander unabhängig von ihrer Funktion, ihres Geschlechts oder ihrer Herkunft taktvoll, respektvoll und verantwortungsvoll begegnen», hält die Pressestelle fest.

Missbrauch am Arbeitsplatz

Das sei ein wichtiger Punkt aus der internen Weisung «Machtmissbrauch am Arbeitsplatz». Die ZKB sei um eine offene und ehrliche Kommunikation zwischen den Mitarbeitenden und ihren Vorgesetzten, aber auch zwischen den Mitarbeitenden untereinander bemüht. Als Ansprechpersonen bei Mobbing oder sexueller Belästigung fungierten jeweils eine Frauenbeauftragte und ein Männerbeauftragter.

«Grundsätzlich erwarten wir, dass allfällige interne Missstände dem direkten Vorgesetzten mitgeteilt werden», beschreibt Franz Würth von Raiffeisen Schweiz den klassischen Dienstweg. Die Mitarbeiter würden in den Mitarbeiter-Gesprächen auch immer wieder aufgefordert, sich diesbezüglich zu äussern. Das setze eine entsprechende Vertrauenskultur voraus, auf die Raiffeisen grossen Wert lege.

Wenn der Draht zum direkten Vorgesetzten nicht funktioniere, könne sich ein Mitarbeiter auch an den übernächsten Vorgesetzten wenden. «Oder in besonderen Fällen auch an die Mitglieder der Geschäftsleitung, den Leiter HR oder den Leiter Legal & Compliance», so Würth. Wirkliche Probleme in dieser Hinsicht seien aber bei Raiffeisen bisher nicht vorgekommen.

Eine besondere Herausforderung den Unsicherheitsfaktor «Mensch» zu beherrschen, haben Grossbanken. «Sämtliche Mitarbeitende können vermutetes rechtliches, regulatorisches, ethisches oder anderes Fehlverhalten jederzeit melden», hält Sprecherin Da-

niela Häsler von der Credit Suisse fest. Melden können die Mitarbeitenden Fehlverhalten beim direkten Vorgesetzten, bei der Rechtsabteilung oder telefonisch und auf Wunsch anonym an eine spezielle Anlaufstelle.

Die Credit Suisse hat einen internen Code of Conduct

Diese Integrity Hotline stehe allen Mitarbeitenden weltweit an allen sieben Wochentagen rund um die Uhr zur Verfügung, heisst es im internen Code of Conduct. Er wurde vom Verwaltungsrat und der Geschäftsleitung der Bank Ende 2010 verabschiedet. Der Code lege die ethischen Grundwerte der Bank und die professionellen Standards fest, ist einleitend festgehalten.

Einer der sieben professionellen Standards lautet: «Wir behandeln unsere Mitarbeiter respektvoll und fair.» Das bedeute für die Bank ein sicheres und gesundes Arbeitsumfeld ohne Diskriminierung, Belästigung oder Repressalien und eine Politik der «offenen Tür». Sie ermögliche allen Mitarbeitenden den Zugang zum Management.

Neben Respekt ist Vertrauen ein wichtiger Anspruch der CS: «Wir wollen professionell und ethisch verantwortungsvoll handeln», heisst es im Code. Das Handeln der Mitarbeitenden müsse stets offen und transparent sein und auch so den Kunden sowie den Kollegen übermittelt werden. «Unsere Reputation ist unser wichtigstes Gut», heisst es abschliessend über die Einhaltung des Codes. Ob und wie er tatsächlich wirkt, kann nicht gemessen werden.

BILD: KEY/PETER KLAUNZER

Der Rücktritt von SNB-Präsident Philipp Hildebrand hat in Sachen Datenmissbrauch sensibilisiert.

Die kriminelle Energie des Faktors Mensch kann nie vollständig ausgeschlossen werden. Ein diesbezüglich besonders heikler Bereich ist die IT (siehe auch Kasten). Der Fall Hildebrand in der Bank Sarasin ist ein entsprechendes Beispiel. Der Fall Zumwinkel beziehungsweise Kieber in der Liechtensteiner Global Trust (LGT) ist ein anderes.

Wie verhindert zum Beispiel die ZKB Datenmissbrauch durch interne IT-Mitarbeitende? «Viel wichtiger als ausgeklügelte Sicherheitssysteme ist die Integrität der Mitarbeitenden», fasst Sprecher Igor Moser zusammen. Bereits bei der Rekrutierung eines Mitarbeitenden setze die Bank alles daran, die charakterliche Neigung durch verschiedenste Mittel zu ergründen. Dazu zählen das persönliche Gespräch, Assessments und der Strafregisterauszug.

IT als besonders heikler Bereich

Trotzdem könne menschliches Fehlverhalten nicht vollumfänglich ausgeschlossen werden. Die ZKB versuche deshalb der Gefahr zu begegnen, indem auch sensible Kundendaten geschützt beziehungsweise für einen möglichst kleinen Benutzerkreis zugänglich gemacht würden.

Konkreter wird in diesem Punkt Raiffeisen. «Bei der IT haben lediglich rund 50 der 700 Mitarbeitenden theoretisch Zugriff auf Kundendaten», stellt Sprecher Würth fest. Die entsprechenden Berechtigungen würden sehr restriktiv durch ein Berechtigungsmanagement vergeben, das ausserhalb der IT angesiedelt sei.

Ein 100-prozentiger Schutz sei nicht möglich, sagt auch Christoph Steiner von der Neuen Aargauer Bank. Die Mitarbeitenden müssten ja mit Daten arbeiten können. Trotzdem gäbe es viele Einzelmassnahmen, um Datenmissbrauch zu vermeiden. Zu den Massnahmen zählten Zugriffsbeschränkungen, Sensibilisierung durch Schulung und Ausbildung der Mitarbeitenden aller Stufen sowie IT-systemtechnische Massnahmen wie gesperrte USB-Ports und CD-Laufwerke sowie physische Massnahmen wie die Platzierung von Servern in besonders gesicherten Räumen. «

BILD: ISTOCKPHOTO

Technische Massnahmen sind das eine, die kriminelle Energie von Mitarbeitern das andere.

Firewalls und Verschlüsselungen reichen nicht mehr

Im Fall des abgetretenen SNB-Präsidenten Philipp Hildebrand stellen sich unter anderem besonders heikle Fragen um die IT-Sicherheit in Banken: Screenshots mit dem Smartphone, zusammengestückelte und nachbearbeitete Kontoauszüge sowie Fragen um die Zugangsrechte von IT-Fachleuten zu höchst sensiblen Kundendaten sind die Stichworte.

«Wir betonen schon lange, dass man bei IT-Security auch den Insidern, und dazu gehören die eigenen Angestellten, ausreichend Aufmerksamkeit schenken muss», sagt Robert Griffin, Chief Security Architect bei RSA, der IT-Security-Sparte von EMC. Fast alltäglich seien Fälle verlorener beziehungsweise gestohlener Laptops ohne Datenverschlüsselung wie beim US-Unternehmen Transcend Capital im Dezember 2011. «Finanzdienstleister sind im Allgemeinen sensibilisiert und unternehmen eine Menge, um Datenverluste zu vermeiden», stellt Griffin fest. Dazu gehörten beispielsweise Technologien, die verhindern, dass Informationen aus Spreadsheets in E-Mails kopiert und verschickt werden können. Aber nicht nur Kundendaten, sondern auch die Algorithmen für den Handel seien für Banken sehr wichtig und schützenswert. Hier versucht man sich laut Griffin zu schützen, indem man prüft, ob diese Algorithmen an denjenigen Orten gespeichert sind, wo sie hingehören – und nicht an einem anderen Ort, wo sie beispielsweise ein Angestellter, der die Firma verlässt, hinkopiert hat.

Für einen effizienten Schutz sind gemäss Griffin nicht nur Technologie, sondern auch geeignete organisatorische Strukturen und Geschäftsprozesse erforderlich. Hierzu zählt die Trennung von unterschiedlichen Rollen und Zugriffsrechten. «Vor allem bei kleinen Banken kann das Probleme geben, wenn mehrere Zuständigkeiten auf eine einzige Person fallen», gibt Griffin zu bedenken. Im Zusammenhang mit Whistleblowers und gegebenenfalls offen gelassenen Überwachungslücken für die absichtliche Weitergabe von Informationen betont Griffin, dass IT ständig in Zusammenhang mit dem gesamten Corporate-Governance-Programm einer Bank betrachtet werden muss. Oft werde Sicherheit als isoliertes Technologieproblem betrachtet und es würden Fragen gestellt, ob Firewalls installiert und die Daten auf Laptops verschlüsselt seien. (mn)