Wenn die Kontrollen versagen

SCHWEIZ Fehlverhalten und Kriminalität beschäftigen Unternehmen und ihre Prüfer. Auch aufwendige Compliance kann den Schaden nicht immer verhindern.

EFLAMM MORDRELLE



BILD: MALTE MUELLER/FSTOP/PLAINPICTURE

Compliance-Richtlinien durchzusetzen und zu kontrollieren ist aufwendig . Bei vorsätzlichem Fehlverhalten kommt auch eine umfassende Risiko-Überwachung an ihre Grenzen.

Nur die spektakulärsten Fälle schaffen es in die Nachrichten. Aber die haben es in sich. Im Januar erregte der Fall des Schatzmeisters bei der südkoreanischen Niederlassung von ABB für Aufsehen: Er veruntreute 103 Mio. $. Pharmamulti Novartis sah sich zuletzt in Griechenland, in der Türkei, Südkorea und den USA mit Korruptionsvorwürfen konfrontiert. Auch Zementriese LafargeHolcim sorgte in den letzten Monaten für viele Schlagzeilen. Der Konzern musste eingestehen, terroristischen Gruppen in den Wirren des syrischen Bürgerkriegs indirekt Schutzgeld gezahlt zu haben, um eine Anlage weiter betreiben zu können. CEO Eric Olsen musste gehen. Über den juristischen Dauerkrieg, in dem sich zahlreiche Schweizer Finanzinstitute in Steuerfragen befinden, ganz zu schweigen.

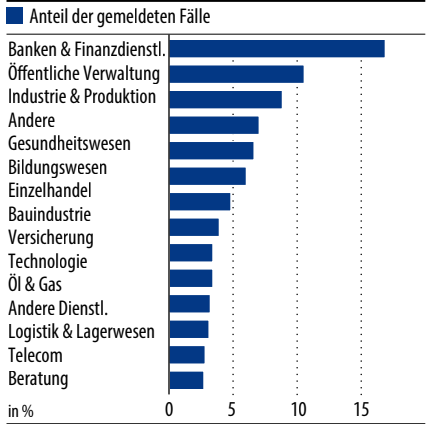
Dabei bemühen sich die meisten Unternehmen, durch interne Kontrollmechanismen Fehlverhalten zu verhindern – mit gemischtem Erfolg. «Das ist nur die Spitze des Eisbergs», sagt Matthias Kiener vom Wirtschaftsprüfer KPMG zu den bekannten Fällen. «Die allermeisten Vergehen dringen nie an die Öffentlichkeit», erklärt der Forensik-Experte, der im Auftrag betroffener Unternehmen interne Ermittlungen durchführt. So lande eine Mehrheit der Fälle in der Schweiz nicht vor Gericht. «Täter werden oft weder zivilrechtlich noch strafrechtlich verfolgt.»

Ein globales Problem

Gemäss einer Studie des Wirtschaftsprüfers verursachten schwere Wirtschaftsdelikte im vergangenen Jahr in der Schweiz allein einen Schaden von 1,4 Mrd. Fr. (vgl. Kasten). Besonders Betrugsdelikte («Fraud») sind stark verbreitet, weltweit wie in der Schweiz. Die Association of Certified Fraud Examiners (ACFE) schliesst aus einer Umfrage, dass Organisationen durchschnittlich 5% ihres Jahresumsatzes wegen betrügerischer Handlungen einbüssen. Die Unternehmen sind am häufigsten Opfer von Veruntreuung. «Der Griff in die Kasse ist verbreitet», bestätigt KPMG-Experte Kiener. Ein Drittel der Fälle betrifft gemäss ACFE Korruption, ein Zehntel Bilanzmanipulation. Wobei letztere Art des Betrugs den grössten finanziellen Schaden anrichtet. Eine weitere Spielart ist die Urkundenfälschung.

Von Betrug betroffene Branchen

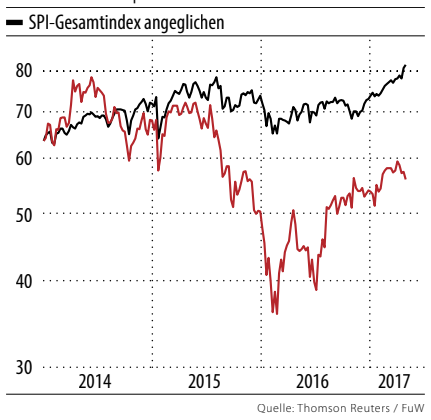
Anteil der gemeldeten Fälle



Quelle: ACFE / Grafik: FuW, sb

– LafargeHolcim N

Kurs: **56.45 Fr.** | Valor: 1221405



Quelle: Thomson Reuters / FuW

– ABB N

Kurs: **24.76 Fr.** | Valor: 1222171



Quelle: Thomson Reuters / FuW

Es gibt grosse Unterschiede zwischen den einzelnen Branchen. Daten gibt es wenig, doch die Finanzindustrie fragt mit Abstand am meisten Dienstleistungen im Bereich Betrugsbekämpfung nach. Das dürfte auf ein entsprechendes Branchenproblem hinweisen (vgl. Grafik). Den Fällen in der Schweiz wie im Ausland ist eines gemein – oft sind die Chefs die Täter: «Je mehr Verfügungsgewalt ein Manager hat, desto schwieriger ist es, ihn zu kontrollieren», sagt Flemming Ruud, Professor für interne Revision und Risikomanagement an der HSG. So rapportierte der Treasurer, der das Vermögensdelikt bei ABB in Südkorea beging, Oh Myung-se, an den lokalen Finanzchef, gehörte also dem höheren Management an. Er hatte privilegierten Zugang zu Systemen und Berechtigungen. Er war fünfundzwanzig Jahre beim Unternehmen, jetzt wird er von Interpol gejagt.

Die Unterscheidung zwischen einer kriminellem Handlung und einem Fehlverhalten ist nicht trennscharf. Was kriminell ist, wird vom Strafgesetzbuch vorgegeben. Doch es gibt einen Graubereich, etwa im regulatorischen, steuerlichen oder ethischen Bereich, wie er etwa von einem Code of Conduct definiert wird (vgl. Glossar).

Löcher im System

In diesem Licht ist es heikel, den LafargeHolcim-Fall als nur von krimineller Energie getrieben zu qualifizieren. Die Verletzung internationaler Sanktionen ist inakzeptabel. Dennoch können Entscheidungen, die in einem ausserordentlichen Umfeld wie Krieg gefällt werden, nicht mit gleichen ethischen Standards beurteilt werden. Dass grobes Fehlverhalten vorliegt, ist trotzdem unbestritten.

Um dem vorzubeugen, betreiben Konzerne umfassende interne Kontroll- und Compliance-Systeme. Sie sollen die Auswirkungen von Fehlverhalten minimieren; besonders die Konsequenzen auf die Rechnungslegung. In der Schweiz sind Unternehmen seit 2002 durch das Obligationenrecht verpflichtet, ein internes Kontrollsystem (IKS) anzulegen. In den USA kotierte Unternehmen wie Novartis müssen sich zudem an die Sarbanes-Oxley-Richtlinien halten (vgl. Glossar).

Trotzdem haben etwa im Fall von ABB in Südkorea die Kontrollsysteme versagt. Eine Untersuchung des Wirtschaftsprüfers E&Y kommt zum Schluss, dass das IKS von ABB eine «Material Weakness», also eine wesentlich Schwäche, aufweise. Das kann letztlich heissen, dass auch die Jahresrechnung nicht korrekt ausgewiesen ist. «Ein solches Testat möchte kein kotiertes Unternehmen im Geschäftsbericht haben», sagt Forensiker Kiener.

«Wir haben es hier mit einer sehr ausgeklügelten kriminellen Aktion zu tun, die jedes Unternehmen treffen könnte», sagt ein ABB-Sprecher zum Südkorea-Fall. Der Konzern hat Massnahmen getroffen, um das Risiko solcher Vorfälle künftig zu reduzieren: Zugangsrechte zum Buchhaltungssystem wurden angepasst, die Aufsicht der Finanzabteilung verschärft, der lokale CEO und CFO ausgewechselt.

Auch LafargeHolcim zieht Konsequenzen aus dem Syrien-Skandal: Striktere Hintergrundprüfungen für Partner, ein Compliance-Team klopft Beschaffung, Zulieferung, Produktion und Verkauf auf Beziehungen zu problematischen Gruppen ab, ein Risikoausschuss entsteht. Was bleibt, ist geschädigte Reputation, und die lässt sich kaum quantifizieren.

Steuern statt kontrollieren

In komplexen Organisationen wie ABB oder Novartis, die in Dutzenden Jurisdiktionen aktiv sind, muss das Compliance-System umfassend sein. Entsprechend aufwendig und teuer sind Durchsetzung und Kontrolle. Für IKS-Experte Flemming Ruud ist deshalb die Steuerung von Risiken wichtiger als ihre Kontrolle – und das muss im Alltag geschehen. «Die Sicherstellung der Qualität der Geschäftsprozesse ist Aufgabe das Managements», sagt Ruud. Compliance und ein übergeordnetes IKS wirkten bloss unterstützend.

Ob ein IKS seiner Aufgabe gewachsen ist, ist von aussen kaum zu beurteilen. «In der Schweiz muss gemäss Obligationenrecht lediglich bestätigt werden, dass ein IKS existiert, nicht dass es auch funktioniert», sagt Ruud. Das sei kein sinnvoller «Swiss Finish». Unter Sarbanes Oxley wird zwar eine Prüfung der Effektivität des IKS verlangt. Doch auch wenn dies geschieht, gibt es keine Sicherheitsgarantie. Das zeigt der Fall ABB. Denn «wasserdicht ist kein System», macht Ruud klar.

Glossar

Code of Conduct
Der Code of Conduct oder Verhaltenskodex ist eine Sammlung spezifischer Richtlinien und Regeln, die ein Unternehmen für sich definiert. Diese Richtlinien haben keinen Rechtscharakter, sie sind also nur freiwillig bindend. Die Regeln dienen als Handlungsanleitung für Mitarbeitende und sollen unethisches Verhalten vermeiden. Die Formulierung und Kommunikation eines Code of Conduct gilt als Standard im Sinne einer modernen Corporate Governance.

Compliance
Auf Englisch heisst Regeltreue «Compliance». Der Begriff steht für die Einhaltung der Grundsätze, regulatorischen Standards und gesetzlichen Richtlinien, die ein Unternehmen beachten muss oder sich selbst auferlegt. Compliance ist keine rein juristische Disziplin. Sie umfasst auch freiwillige Kodizes wie den Code of Conduct.

IKS
Ein internes Kontrollsystem (IKS) ist ein umfassendes Führungsinstrument im Rahmen des Risikomanagements. Es soll insbesondere finanzielle Schäden bei internen Prozessen mit Kontrollen und Vorgaben verhindern oder minimieren. Es soll zudem die Prozesse, die zu einer ordnungsgemässen Buchführung und Berichterstattung führen, sicherstellen. Seit 2008 sind ein IKS und Risikobericht durch das Obligationsrecht für alle Unternehmensformen vorgeschrieben (Art. 728a). In der Schweiz prüft eine Revisionsstelle die Existenz eines IKS.

Sarbanes-Oxley-Act
Im Nachgang zu den US-Finanzskandalen wie Enron um die Jahrtausendwende erliess der US-Kongress 2002 das Sarbanes-Oxley-(SOX-)Rahmengesetz zum besseren Schutz der Anleger. Implementiert und überwacht werden die Massnahmen durch die US-Börsenaufsicht SEC. SOX entfaltet sich über Richtlinien für die Wirtschaftsprüfung. Auch für Schweizer Unternehmen mit einer Kotierung in den USA sind die SOX-Vorgaben bindend. Darunter fallen unter anderem ABB, Novartis oder Logitech. Gemäss Abschnitt 404 muss der Jahresbericht eine externe Beurteilung der Wirksamkeit des IKS für die Rechnungslegung enthalten.

Finanzsektor und Industrie im Fokus

Wirtschaftskriminalität und Betrugsdelikte kosten die Betroffenen viel Geld. **Gemäss 2016 veröffentlichten Daten der Association of Certified Fraud Examiners (ACFE) verursachten 23% der Betrugsfälle weltweit einen Verlust von je über 1 Mio. $.** Zwei Drittel der Fälle betrafen privat gehaltene oder kotierte Unternehmen. Die Branchen Finanzdienstleistungen und verarbeitende Industrie waren demnach am stärksten betroffen.

In der Schweiz wurden im vergangenen Jahr gemäss dem «Forensic Fraud Barometer» von KPMG gesamthaft 1,4 Mrd. Fr. als Schadensumme registriert. Das ist im Vergleich zu den Vorjahren aussergewöhnlich hoch. 2015 waren es 282 Mio. Fr. (91 Fälle), 2014 waren es 537 Mio. Fr. (77 Fälle) und im Jahr davor 830 Mio. Fr. (58 Fälle).

Der Grund: Das Jahr 2016 berücksichtigt den sogenannten Fall Behring – eine Anlagebetrugsaffäre, die 2004 aufflog. Der Fall soll allein einen Schaden von rund 800 Mio. Fr. verursacht haben. Entsprechend waren private und institutionelle Anleger 2016 in der Schweiz die am stärksten betroffene Gruppe von Geschädigten.

Global hatten laut KPMG zwei Drittel der Täter in den Unternehmen eine Management-Funktion oder waren Mitglied des Kaders. In der Schweiz waren es 55% der Täter. Betrug erfolgt oft nicht einmalig. In zwei Drittel der weltweit analysierten Fälle dauerte das Delikt über eine Spanne von bis zu fünf Jahren.

Schweizer Täter waren in vier von fünf Fällen männlich und zwischen 36 und 55 Jahre alt. Von ihnen war über ein Drittel mehr als sechs Jahr beim Unternehmen. Zwei Drittel handelten aus Motiven der persönlichen Bereicherung, 27% aus Opportunismus. **Ein Viertel der Fälle wurde durch Hinweise von Mitarbeitenden aufgedeckt. Lediglich ein Fünftel meldete Fehlverhalten über eine offizielle Whistleblowing-Hotline.**

Eine neue Betrugsart geschieht über das Internet und wird von jüngeren Mitarbeitenden verübt. Verlässliche Daten zu dieser Form von Cyber-Kriminalität fehlen.

Effektive Compliance kann einen wichtigen Unterschied machen. In 64% der Schweizer Fälle waren gemäss Untersuchung die internen Kontrollen schwach.