


Grenzenlose Bedrohung



Viele Unternehmen sind schlecht darauf vorbereitet, Betrugsdelikten rasch und effektiv nachzugehen, wenn diese außerhalb des Landes vorkommen, in dem der Hauptsitz liegt. Nur wenige Unternehmen scheinen wirklich vor Wirtschaftsdelikten im Ausland geschützt. Durch verstärkte Aktivität in High Growth Markets wird das Problem keineswegs kleiner.

Beinähe monatlich liefern die Medienschlagzeilen neue Beispiele: zu spät entdeckt eine in Asien ansässige Fluggesellschaft, dass ein in mehreren Ländern operierendes Reisebüro ihr Reservierungssystem missbraucht hat, um mindestens fünf Millionen US-Dollar abzuzweigen. Ein internationaler Energiekonzern mit Sitz in Afrika findet heraus, dass einer seiner leitenden Mitarbeiter widerrechtlich ein firmeneigenes Produkt aus einem Land in ein anderes und in ein Unternehmen überführt hat, an dem der Angestellte beteiligt ist. Ein in Europa ansässiger Finanzdienstleister

kommt einem Geldwäscheskandal internationaler Tragweite auf die Spur, der nun seinen guten Ruf bedroht.

Wer ernsthafte Betrugsabsichten hat, für den stellen nationale Grenzen nur selten ein Hindernis dar. In einer Zeit, wo im Zuge des globalen Handels Geld und geistiges Eigentum in Sekundenschnelle digital über Kontinente hinweg übertragen werden können, stellt das Verhindern, Erkennen und Reagieren auf grenzübergreifende Betrugsdelikte, Korruption und unethisches Verhalten eine immer größere Herausforderung dar. Das gilt vor allem für die dynamischen High Growth Markets.

In diesen Märkten investierende multinationale Konzerne unterschätzen nicht selten die möglichen Risiken für sich und den Markt. Die Herausforderungen in diesen Ländern sind größer und weisen andere Schwerpunkte auf als im Heimatland des jeweiligen Unternehmens.

Angesichts der verschiedenen Rahmenbedingungen wäre es fahrlässig, ein inländisches Kontrollsystem ohne jede Anpassung auf den Geschäftsbetrieb im Ausland zu übertragen. Asien, Osteuropa oder Lateinamerika haben ganz andere kulturelle Traditionen, verschiedene Geschäftspraktiken

tiken und Rechtssysteme. Und vom Land des Unternehmenssitzes aus eine Untersuchung zu internationalen Betrugsdelikten zu leiten, dürfte ebenfalls kaum von großem Erfolg gekrönt sein. Zu starre Regeln könnten dem Erfolg der Untersuchung einen Riegel vorschieben. Stattdessen braucht man eine breite Basis, die von einem Land auf das andere übertragbar ist.

Wichtig ist auch eine länderspezifische Anpassung von Präventions- und Schutzmechanismen. Zu einem aussichtsreichen Ansatz gehört die Darstellung der allgemeinen Prinzipien sowie der Do's und Dont's über zu ergreifende Maßnahmen. Außerdem sollte klar sein, wer für die Untersuchung, für Decision-Making und Reporting verantwortlich ist.

Dennoch haben nicht einmal 50 Prozent aller Unternehmen wirklich effektive Maßnahmen zum Schutz gegen Wirtschaftsdelikte im Ausland ergriffen. Aus einer Untersuchung von KPMG International geht hervor, dass die Mehrheit der Unternehmen (56 Prozent) unzureichend auf eine rasche und effektive Untersuchung von Betrugsdelikten vorbereitet ist, wenn sich diese in Ländern ereignen, die nicht Unternehmenssitz sind. Wie aus der englischsprachigen Studie „Cross-Border Investigations – Effectively meeting the Challenge“ hervorgeht, verfügen die Unternehmen nicht über umfassende Protokolle, um solchen Untersuchungsprozessen auf internationaler Ebene nachzugehen.

„Bei Prävention, Entdeckung und Verfolgung internationaler Betrugsdelikte einfach untätig zu bleiben, ist wie eine Einladung für die Täter, die sich

sich greift. Offiziellen Zahlen aus dem chinesischen Finanzministerium zufolge deckten die Behörden im Jahr 2006 im Finanzsektor 8233 Bestechungsfälle auf – drei Mal so viel wie im Vorjahr. Die Schadensschätzung stieg um 60 Prozent auf 144 Millionen Euro. Und die Gesamtzahl der Wirtschaftsdelikte stieg auf 2,28 Millionen Fälle. Fachleute gehen davon aus, dass die Dunkelziffer in diesem Bereich noch deutlich höher ist.

Ein weiterer Aspekt: in vielen Ländern achtet der Gesetzgeber jetzt verstärkt auf ethisch korrektes Verhalten im Geschäftsleben. Die Unternehmen stehen damit noch stärker in der Pflicht, bessere Praktiken in den Bereichen in Corporate Governance, Corporate Disclosure und Risk Management umzusetzen. Es ist daher wichtig, dass Unternehmen sich die Betrugsrisiken klar vor Augen führen, denen sie momentan ausgesetzt sind.

Die im Sommer 2008 veröffentlichte, jüngste Ausgabe des „Fraud Survey Report“ von KPMG liefert am Beispiel des High Growth Market Indien grundlegende Einblicke in das Maß an Betrugsbewusstsein sowie in die aktuellen Trends und Betrugsformen in indischen Unternehmen. Sie erörtert aber auch die Wege, die eingeschlagen werden, um die Risiken zu verringern.

Der Bericht stellt fest, dass Betrugs- und Wirtschaftsdelikte in Indien in den letzten Jahren zugenommen haben – Tendenz weiter steigend. Im Vergleich zum „India Fraud Survey Report“ des Jahres 2006 waren mehr

Global Corruption Perceptions Index (CPI) 2008

Der CPI misst den Grad der Wahrnehmung öffentlicher Korruption auf Basis von Untersuchungen und Analysen. Die Skala reicht von 0 (hoch korrupt) bis 10 (hoch integer).

Stelle	Land	Punktzahl
4	Singapur	9,2 von 10
12	Hongkong	8,1 von 10
40	Korea	5,6 von 10
54	Südafrika	4,9 von 10
58	Türkei	4,6 von 10
72	China	3,6 von 10
80	Saudi-Arabien	3,5 von 10
85	Indien	3,4 von 10
121	Nigeria	2,7 von 10
121	Vietnam	2,7 von 10
147	Russland	2,1 von 10

Quelle: Transparency International, Auswahl aus insgesamt 180 Staaten

stungssektor als überdurchschnittlich betrugsanfällig, gefolgt von den Sektoren Immobilien/Infrastruktur und IT.

Betrug in Form von Lieferantenschmiergeldern, Korruption und Bestechung gehört derzeit zu den größten Risiken in indischen Unternehmen. Die Befragten gehen allerdings davon aus, dass sich die Betrugsformen im Lauf der nächsten Jahre ändern. Man nimmt an, dass die verbreitetste Betrugsform der Zukunft Diebstahl von geistigem Eigentum (Intellectual Property/IP) oder Betrug in den Bereichen e-Commerce und IT ist.

Die für Indien festgestellten Ergebnisse zu verschiedenen Betrugsformen werden von einer ähnlichen Studie der KPMG-Mitgliedsfirma in Singapur untermauert. Nach Aussage des „Singapore Fraud Survey Report 2008“ erhöht sich in Unternehmen, die Opfer von Betrugsdelikten waren, die Wahrscheinlichkeit, dass Technologie mit im Spiel war, um dramatische 300 Prozent. Schlussfolgerung: Betrug im Zusammenhang mit Informationstechnologie (IT) ist die derzeit am schnellsten wachsende und am weitesten verbreitete Betrugsform in Unternehmen.

Die starke Zunahme technologiebezogener Betrugsdelikte ist

Wer ernsthafte Betrugsabsichten hat, für den stellen nationale Grenzen nur selten ein Hindernis dar

– im Gegensatz zu den Unternehmen – von nationalen Grenzen nicht beeindruckt lassen“, warnt Adam Bates, Leiter Global Forensic bei KPMG.

Zahlen aus China und anderen High Growth Markets belegen, wie schnell das Problem der Wirtschaftsdelikte in der globalisierten Weltwirtschaft um

Befragte Opfer von Betrugsdelikten geworden als noch vor zwei Jahren. Über 80 Prozent der Befragten räumen ein, dass Betrug in indischen Unternehmen ein Problem darstellt. Die Betrugsrisiken wurden branchenübergreifend als weit verbreitet eingestuft. Dabei gilt der Finanzdienstlei-

Betrug in Form von Lieferantenschmiergeldern, Korruption und Bestechung gehört derzeit zu den größten Risiken in indischen Unternehmen.

How it Works

Zehn Regeln der Prävention

Welche Maßnahmen unsere Forensic-Spezialisten zum Schutz gegen Industriespionage empfehlen.

- | | | | |
|----------|--|-----------|---|
| 1 | Informationsschutz ist ein strategischer Erfolgsfaktor sowie wichtiger Bestandteil der Firmenphilosophie und -strategie. | 6 | „Frühwarnsystem“ zur Erkennung von Know-how-Verlusten einrichten. |
| 2 | Mitarbeiter stehen im Mittelpunkt des Informationsschutzes und der zu treffenden Maßnahmen. | 7 | Sicherheitsstandards regelmäßig analysieren und aktualisieren. |
| 3 | Schutzmaßnahmen auf die entscheidenden, zukunftsichernden Informationen konzentrieren. | 8 | Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren. |
| 4 | Ganzheitliches Sicherheitskonzept etablieren und permanent fortschreiben. | 9 | Aktuelle Hintergrundinformationen zu wesentlichen Stakeholdern bei kompetenten Partnern einholen (z.B. Business Partner Screening, Pre-Employment Screening). |
| 5 | Restriktiven Zugang zu sensiblen Informationen für Mitarbeiter installieren. | 10 | Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen. |

darauf zurückzuführen, dass sich Unternehmen immer mehr auf Technologie verlassen. Dabei hat KPMG einen wichtigen Trend ausgemacht: die Effektivität von Kontrollmechanismen für komplexe IT-Systeme scheint den spektakulären Wachstumsraten hinterherzuhinken.

In Indien erhält dieses Problem angesichts der zahlreichen dort angesiedelten IT-Unternehmen zusätzliche Brisanz. Mit über vier Millionen hoch qualifizierten, englischsprachigen Technikprofis (eine Zahl, die nur von den USA überboten wird) und weltweit

führenden Software-Unternehmen hat sich Indien zum Software-Land Nr. 1 entwickelt. Es exportiert Software in 95 Länder weltweit. In einer neueren Umfrage steht Indien bei 82 Prozent der US-Unternehmen ganz oben auf der Liste, wenn es um Outsourcing der Software-Produktion geht. Es ist daher sehr wichtig, dass IT-bezogene Probleme baldmöglichst angegangen werden.

Da Indien und andere BRIC-Länder auf dem besten Weg in die Wissenswirtschaft sind, sind die Vermögenswerte des Landes zunehmend auch

im nichtmateriellen Bereich zu finden. Ideen, Marken, Content und Software von in Indien oder Korea angesiedelten Unternehmen verzeichnen im Vergleich zu ihren materiellen Pendanten eine stetig steigende Nachfrage. Mit diesem wirtschaftlichen Paradigmenwandel geht aber auch eine exponentielle Steigerung der Betrugsdelikte beim geistigen Eigentum einher.

Abgesehen haben es Betriebsespione vor allem auf technische Innovationen und das Know-how der Unternehmen. Informationen machen etwa 70 Prozent aller immateriellen Vermögenswerte aus. Betriebs- und Geschäftsgeheimnisse sind essenzielle Grundlagen der Wertschöpfung.

Der Verlust wichtiger Informationen stellt daher den größten Schaden für die Unternehmen dar. Meist bietet aber nicht die IT, sondern der Mitarbeiter die größte Angriffsfläche für das Unternehmensgut Information. Ein systematischer Schutz der Information beginnt daher beim Personal.

Unternehmen verkennen oftmals die eigene Anfälligkeit für Betrugsdelikte und unethisches Verhalten. Bis sie selbst Opfer solcher Delikte werden. Die Täter sind nicht selten vertrauenswürdige Mitarbeiter, geschätzte Geschäftspartner oder sogar Vertreter der Geschäftsleitung.

Organisationen wie Transparency International haben Länder-Rankings auf Grundlage von Korruption und der Tendenz zum Einfordern von Bestechungszahlungen erstellt. Indien erzielte beim „Corruption Perception Index 2008“ einen niedrigen, das bedeutet negativen Wert (3,4 von 10 möglichen Punkten) und den niedrigsten Wert auf dem Bestechungsgeld-Index (30/30). Das deutet darauf hin, dass sich die Menschen des hohen Ausmaßes der Korruption im Lande bewusst sind.

Diesen Eindruck unterstrichen die Ergebnisse des „India Fraud Survey“: 84 Prozent der Befragten glaubten,

dass indische Unternehmen Bestechungsgelder fließen lassen, um sich geschäftliche Vorteile zu verschaffen. Außerdem war ein eher dürftiges Wissen um das Vorhandensein einschlägiger Gesetze (wie z.B. des „US Foreign Corrupt Practices Act“ von 1977 und des „Indian Prevention of Corruption Act“ von 1988) festzustellen. Das könnte ein Grund sein, warum sich Unternehmen so wenig an geltendes Recht halten.

Die Nichtbeachtung von Anti-Korruptionsgesetzen kann Unternehmen schwerwiegende Konsequenzen bescheren. Da das US-Justizministerium und die „Securities Exchange Commission“ (SEC) nun verstärkt auf die Einhaltung des „Foreign Corrupt Practices Act“ (FCPA) pochen, müssen US-Unternehmen, die in Indien investieren oder geschäftlich tätig sind, sicherstellen, dass die entsprechenden Gesetze auch eingehalten werden. Ein ähnliches Bild in Europa: der „U.K. Anti-Terrorism, Crime, and Security Act“ von 2001 wurde als Abschreckung erlassen. Ziel des Gesetzes: Unternehmen aus dem Vereinigten Königreich und anderen Ländern sollen auf die Zahlung von Bestechungsgeldern im Ausland verzichten.

Und dennoch: Betrug in High Growth Markets bleibt ein Dauerthema für Unternehmen. Dabei lauert das größte Betrugsrisiko im Unternehmen selbst. Lieferanten-Schmiergelder, das heißt geheime Absprachen zwischen Mitarbeitern und Lieferanten, sind die am weitesten verbreitete Betrugsform. In Zukunft werden aber Betrugsformen rund um die Bereiche IP und IT zunehmen. Unternehmen neigen dazu, auf Betrug lediglich zu reagieren und sind nicht ausreichend auf die Risiken vorbereitet. Außerdem halten viele ihre Kontrollmechanismen nicht für robust genug, um Betrugsdelikten wirksam entgegenzutreten.

Die Kosten, die Betrug in Unternehmen verursacht, sind schwer zu beziffern. Erstens, weil nicht alle Fälle von Betrug und Missbrauch ans Licht kommen. Zweitens, weil nicht alle aufgedeckten Betrugsfälle gemeldet, und drittens, weil nicht immer zivil- und strafrechtliche Schritte eingeleitet werden. Doch die Kosten, die Betrug nach sich zieht, enden nicht mit einer Zahl mit einer Reihe von Nullen. Betrug geht noch tiefer und nagt zerstörerisch an den Wurzeln jeder Geschäftsbeziehung: Zuversicht und Vertrauen. ■

In einer verstärkt auf Wissen basierenden Wirtschaft hat sich die Zahl der Betrugsdelikte beim geistigen Eigentum exponentiell gesteigert.

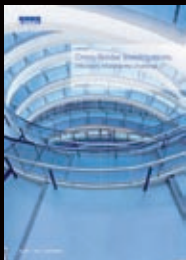
KPMG-Studien

Mehr Informationen zum Thema finden Sie unter anderem in diesen KPMG-Publikationen:

Global anti-money laundering survey 2007
KPMG INTERNATIONAL



Cross-border Investigations
KPMG INTERNATIONAL



India Fraud Survey Report 2008
KPMG, INDIEN



Fraud: Prevent, Detect, Respond – KPMG Singapore's Fraud Survey Report 2008
KPMG, SINGAPUR



2008 GCC Fraud Survey
For Gulf Cooperation Council (GCC) Countries
KPMG GULF STATES



Kostenloser PDF-Download und Bestellmöglichkeiten unter www.kpmg.de oder per E-Mail an highgrowthmarketsmag@kpmg.com