

Krise: Jetzt ist deutsches Know-how in Gefahr

Wirtschaftskriminalität

Erschienen in Produktion - 44/2009

Autor: Michaela Neuner und Annika Mentgen

LANDSBERG. In Zeiten der weltweiten Wirtschaftskrise wiegen sich viele Unternehmen in falscher Sicherheit, wenn es um das Innerste ihres Betriebs geht: ihr Know-how. Denn gerade jetzt werden die eigenen Mitarbeiter immer öfter zum Sicherheitsproblem.



Die finanziellen Schäden, die Unternehmen durch Wirtschaftskriminalität entstehen, haben in den letzten drei Jahren drastisch zugenommen.

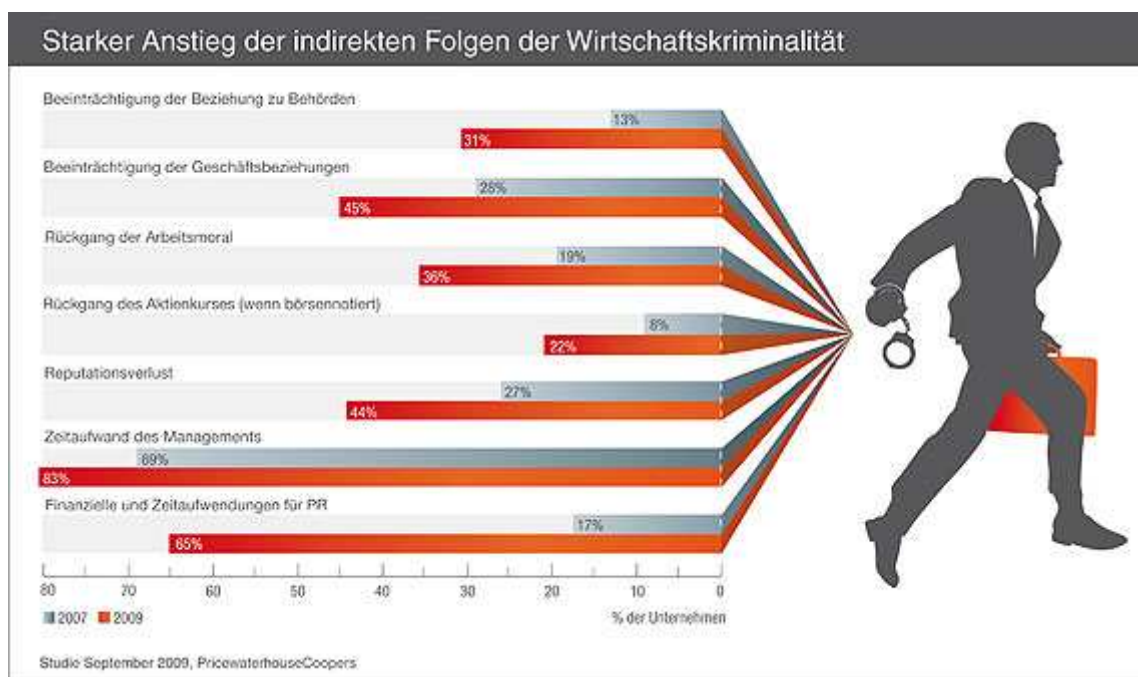
Für die kommenden Jahre erwarten die Unternehmen einen weiteren Anstieg der Wirtschaftskriminalität. Zu diesem Ergebnis kommt die Studie ‚Wirtschaftskriminalität 2009 – Zur Sicherheitslage in deutschen Großunternehmen‘ von PricewaterhouseCoopers (PwC). Gut 40% der Befragten rechnen in ihrer Branche verstärkt mit Wettbewerbsdelikten wie Industriespionage oder Kartellabsprachen. Knapp jedes dritte Unternehmen prognostiziert mehr Straftaten auf Grund von Arbeitsplatzsorgen der Beschäftigten.

Claudia Nestler, Partnerin bei PwC im Bereich Advisory, Forensic Services, verdeutlicht die Problematik der Unternehmen im Rahmen der Wirtschaftskrise: „Unternehmen konzentrieren sich auf kurzfristige Maßnahmen und verständlicherweise stehen Gefahren wie Umsatzeinbußen, Liquiditätsengpässe oder gar die Abwehr der Insolvenz im Fokus.“ Da sich die Marktbedingungen schnell wandeln, bestehe das erhöhte Risiko bei Unternehmensleitungen und Mitarbeitern, Hemmschwellen zwischen Erlaubtem und Gesetzesverstößen zu übertreten. Der Studie zufolge befanden sich die Täter zum Zeitpunkt der Tat bereits acht Jahre auf ihrer Position. Und diese ist häufig eine führende – 29% gehören zum Topmanagement und 38% zum mittleren Management.

Bei kleinen und mittleren Unternehmen sieht es ähnlich aus. Das zeigt eine aktuelle Studie vom Sicherheitsforum Baden-Württemberg (SiFo), die den „Know-how-Schutz in Baden-Württemberg“ unter die Lupe genommen hat. Wenn es um Wirtschaftsspionage, Konkurrenzausspähung oder den Verrat von Geschäftsgeheimnissen geht, kommen die meisten Angriffe von innen: „Vor zehn Jahren war der Täter nur in jedem vierten Fall ein interner Mitarbeiter. Heute trifft das in über 70 Prozent aller Fälle zu“, berichtet Studienleiterin Birgit Galley von der Steinbeis-Hochschule Berlin und zeigt sich alles andere als überrascht: „Das ist bei Know-how-Abfluss eine ganz typische Größenordnung. Über interne

Quellen kommt man leichter und schneller an Informationen heran.“ Nach den Erkenntnissen aus der SiFo-Studie ist der Haupttäter im Schnitt 41 Jahre alt und arbeitete bereits zehn Jahre im Unternehmen. Selbst bei externen Tätern bestand im Durchschnitt seit sechs Jahren eine Geschäftsverbindung.

Die Schäden, die in Deutschland jährlich durch Produktpiraterie oder Spionage entstehen, gehen in die Milliarden. Insgesamt schätzt die Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW), dass deutsche Unternehmen allein durch ungewollten Informationsabfluss jährlich mindestens 20 Mrd Euro verlieren. In ähnlichen Größenordnungen bewegen sich die Schäden durch Marken- und Produktpiraterie. Mit bis zu 50 Mrd Euro rechnet das Fraunhofer-Institut für System- und Innovationsforschung ISI nur für das verarbeitende Gewerbe. Was Großunternehmen noch abfedern können, bricht kleinen und mittleren Unternehmen schnell das Genick. Von den 239 Unternehmen der SiFo-Studie waren in den letzten vier Jahren 38% von Urheberrechtsverletzungen betroffen und 18% von ungewolltem Informationsabfluss durch Fahrlässigkeit, Verrat oder Spionage. Bei jedem fünften Unternehmen lagen die Schäden deutlich über einer halben Million Euro pro Fall. Zu finanziellen Einbußen addieren sich indirekte Schäden – vom angekratzten Image bis zu einem verletzten Vertrauensverhältnis zu Kunden, Geschäftspartnern und Mitarbeitern.



In den Schutz ihres geistigen Eigentums investierten die deutschen Unternehmen 2004 rund 154 Mrd Euro, ermittelte das Fraunhofer ISI. Dennoch reichen „vor allem in kleinen und mittleren Unternehmen die Sicherheitsvorkehrungen oft nicht aus, um dem tatsächlichen Risiko professionell gegenüber zu stehen“, sagt Christian Schaaf, Geschäftsführer des Sicherheitsdienstleisters Corporate Trust. Oft fehlt es an Ressourcen und Erfahrung, Verdachtsfällen nachzugehen.

Grundsätzlich ist es eine Frage der Unternehmenskultur: „Jeder Mitarbeiter muss sensibel genug sein, um mit dem wesentlichen Unternehmens-Know-how verantwortungsbewusst umzugehen“, fordert Schaaf. Ist der Schadensfall trotzdem eingetreten, gilt es schnell und konsequent zu handeln – vor allem, wenn der Täter aus den eigenen Reihen kommt.

Verdachtsfälle auf jeden Fall ausermitteln und die Taten sanktionieren, empfiehlt Galley. Nur so könne man mit dem Verrat fertig werden und mit dem „gefühlten Makel“, dass hier jemand „bis ans Innerste des Unternehmens ganz einfach durch gehen konnte“. Gravierende Verstöße sollten mit einer Strafanzeige geahndet und Instrumente wie Kündigung oder Schadensersatz stärker genutzt werden, raten auch die PwC-Experten.