Vertrauen ist gut, Kontrolle ist besser

RISIKOMANAGEMENT. Durch Mitarbeiterkriminalität entstehen hohe Schäden. Die Personalabteilung kann entscheidend zur Unternehmenssicherheit beitragen.

Von **Carsten Baeck** und **Marek Weber**

Studien zur Unternehmenskriminalität (siehe PriceWaterhouseCoopers, Wirtschaftskriminalität 2005) zeigen, dass 50 Prozent der Täter aus der eigenen Belegschaft (interne Täter) kommen und sie für mindestens 70 Prozent der Schäden verantwortlich sind. Als Motivation dieser Mitarbeiter gelten mangelhafte Kontrollen, persönliche Probleme und eine falsche Unternehmens-ethik. Die Personalabteilung kann daher einen entscheidenden Beitrag zur Unternehmenssicherheit leisten.

Im Folgenden präsentieren wir die These, dass eine vernünftige und von der Unternehmensspitze effizient umgesetzte Unternehmensstrategie zu einer guten Mitarbeiterorientierung führt. Diese mindert die Mitarbeiterkriminalität, was auch einen guten internen Schutz vor Spionage und Verlust von Know-how darstellt. Mit Hilfe interner Kontrollsysteme können potenzielle oder reelle Abweichungen erkannt und an die Verantwortlichen weitergeleitet werden. So ein internes Kontrollsystem (IKS) sollte organisatorische, technisch-bauliche/informationstechnische, juristische, personelle (und informationsbezogene) Komponenten beinhalten (siehe Abbildung rechts).

Negative Tendenzen, die den Unternehmenserfolg gefährden, können so rechtzeitig erkannt und behoben werden. Dadurch werden die Risiken minimiert und die Chancen für eine erfolgreiche Umsetzung der Unternehmensstrategie erhöht. Dieser Artikel konzentriert sich auf die personelle IKS-Komponente. Wir gehen weiterhin nur auf die Abwehr interner und nicht auf die externer Täter ein, obwohl die aufgeführten Überlegungen sich auch zur Abwehr externer Angreifer eignen.

Der frühere Enron-Chef Kenneth Lay: Im Topmanagement fehlt es oft an Unrechtsbewusstsein.

Wie Mitarbeiter kriminell weren

Nach dem Kriminalitätsrisikomodell von Donald R. Cressey, der sich bereits in den 40er Jahren in seiner Dissertation mit den Entstehungsgründen von Kriminalität beschäftigt hat, tritt Wirtschaftskriminalität dann auf, wenn drei Faktoren gleichzeitig präsent sind (siehe auch das Betrugsdreieck nach Joseph T. Wells):

- Gelegenheit: Es muss eine Gelegenheit für die Tat existieren.
- Motivation: Der Täter muss einen Anreiz für die Tat erkennen.
- Rechtfertigung: Der Täter muss die Tat im Nachhinein vor sich selbst rechtfertigen können (Ethik).

Auf die Kriminalprävention übersetzt heißt das:

1. Rechtfertigung (Ethik) ist das Ergebnis der Corporate Governance.
2. Gelegenheit bedeutet vorrangig das Fehlen oder die Ineffektivität von Kontrollen (Compliance).
3. Motivation ist eine Fehlentwicklung des Mitarbeiters, was eine Ineffektivität der Personalführung oder ein Versagen der Personalüberwachung (ebenfalls Compliance) darstellt.

Was man dagegen tun kann

Forensische Forschungsergebnisse zeigen, dass diejenigen Mitarbeiter, die in veränderten Arbeitssituationen abweichende Verhaltensmuster aufweisen, oft auch in Mitarbeiterkriminalität involviert sind. Deswegen sollten neben Inventurdifferenzen, Krankheitsstand, Stimmung am Arbeitsplatz und Mobbing auch weitere Aspekte zentral erfasst werden. Christine Brand-Noé schlägt in ihrem Artikel „Aufgaben des Personalwesens im Hinblick auf die Prävention von unternehmensschädigendem Verhalten“(erschienen in der Fachzeitschrift ZRFG Risk, Fraud & Governance, 02/2007) die unternehmensweite Auflistung folgender Faktoren vor.

- Mahnungen oder Abmahnungen
- Problemfälle (Spieler, Suchterkrankungen)
- Workaholics
- „Spesentreiberei“
- Drastische Veränderung des Lebensstils von Mitarbeitern
- Mitarbeitereinkommen, die mit Pfändung belegt sind
- Anonyme Hinweise auf das Verhalten von Mitarbeitern
- Mitarbeiter, die bereits von der internen Revision überprüft wurden
- Mitarbeiter, auf die verschiedene Hinweise über Auffälligkeiten zusammentreffen und die in einer bestimmten Organisationseinheit konzentriert sind

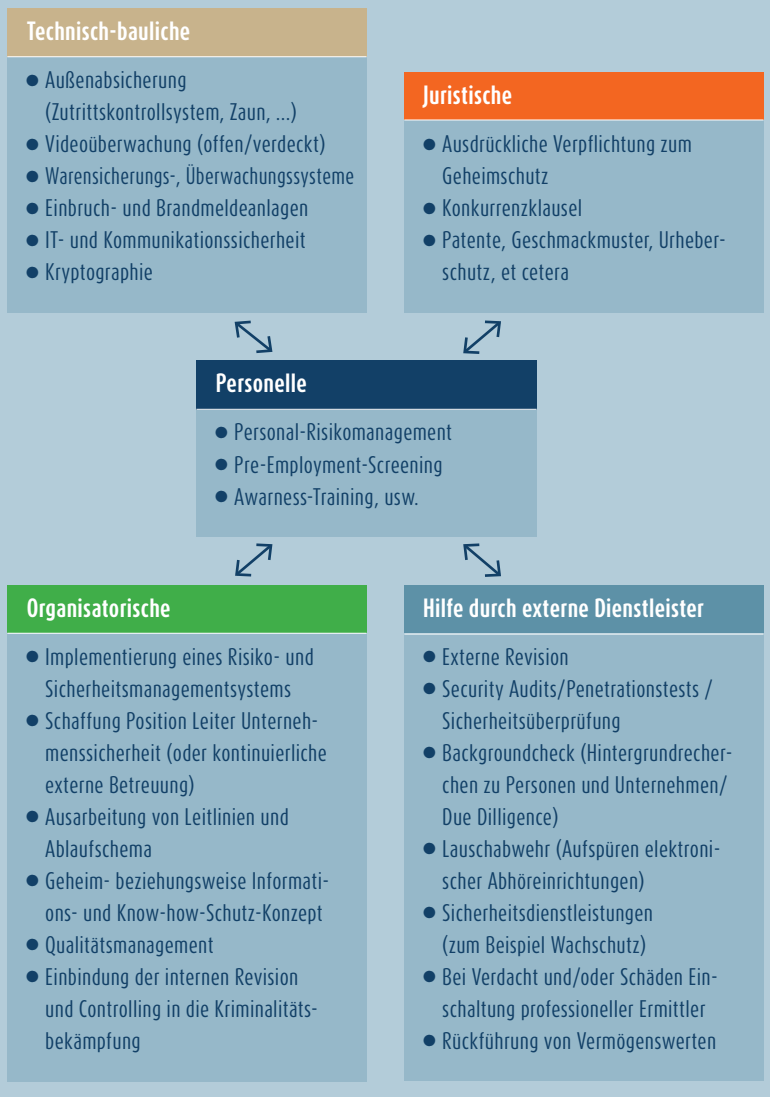
Mit einer derartigen zentralen Datenbank können potenzielle Gründe für mögliche kriminelle Handlungen, wie zum Beispiel ein zu aufwendiger Lebensstill, frühzeitig erkannt werden.

Doch wie sieht es beim Faktor „Anreiz“ beziehungsweise „Motiv“ aus? Laut der eingangs genannten PWC-Studie sind folgende Faktoren als Motivation für kriminelle Handlungen entscheidend: Unzufriedenheit mit dem Unternehmen, berufliche Enttäuschung/Karriereknick und Massenentlassungen.

Der rationale Täter

Daraus resultiert, dass Mitarbeiter in der Regel nicht von einem Tag auf den anderen kriminell werden, sondern in einem schleichenden Prozess. (Eine Ausnahme

Komponenten eines Internen Kontrollsystems (IKS)



Ein internes Kontrollsystem sollte aus mehreren Komponenten bestehen. Die Verantwortung für den personellen Bereich liegt bei der Personalabteilung. Quelle: Deutsche Risikoberatung

sind Täter, die sich gezielt in Unternehmen „einschleusen“. Durch eine gezielte Vorauswahl, inklusive Pre-Employment Screening, können die meisten dieser Täter im Vorfeld identifiziert werden.) Die kriminelle Handlung ist somit das letzte Glied in der Kette einer Abwärts- oder Aufwärtsspirale.

Die Aufwärts- und Abwärtsspirale

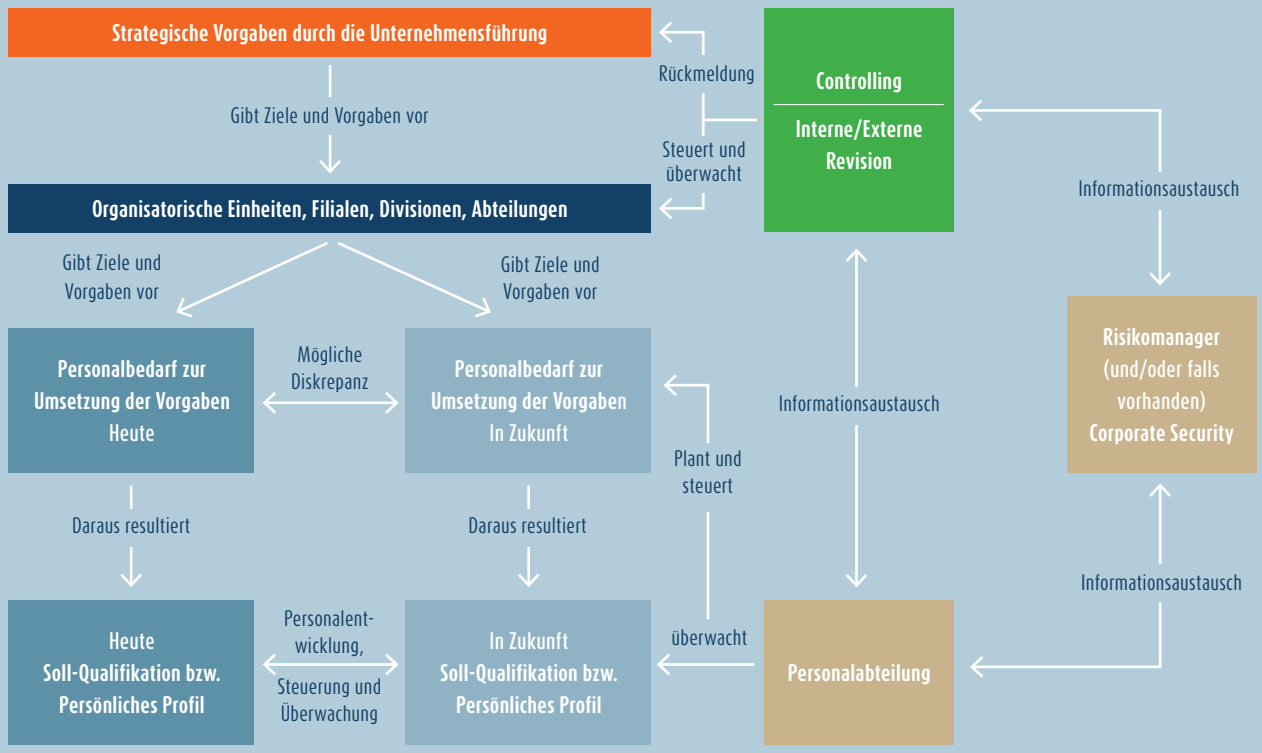
Die Aufwärtsspirale: Mitarbeiter operieren getreu dem Motto „Erfolg rechtfertig die Mittel“. Oft wird dieses Verständnis, vor allem beim Topmanagement, durch eine erfolgsorientierte Vergütung bestärkt, so dass die Manager kein Unrechtsbewusstsein für ihre Taten entwickeln. Ein Beispiel für so ein Verhalten ist die Bilanzfälschung bei Enron.

Die Abwärtsspirale: Mitarbeiter sind aus welchen Gründen auch immer unzufrieden und reagieren mit einem ihrer Meinung nach gerechtfertigtem Verhalten. Das „Exit-Voice-Loyalty-Neglect“ (EVLN)-Modell identifiziert vier Varianten von Verhalten, mit denen Mitarbeiter auf Unzufriedenheit reagieren können.

- Exit: Mitarbeiter meinen, dass sie die Ursache ihrer Unzufriedenheit nicht verändern können und verlassen die Abteilung oder das Unternehmen.
- Voice: Dieses Vorgehen beinhaltet alle Versuche, die Situation zu verändern anstatt vor ihr zu fliehen (Exit).
- Loyalty: Die Mitarbeiter warten ab und dulden die Missstände, bis das Problem sich von alleine löst oder durch Dritte gelöst wird.
- Neglect: Hiermit ist der Dienst nach Vorschrift gemeint. Die Mitarbeiter schränken ihre Anstrengungen ein, kommen zu spät und/oder sind öfters abwesend. Neglect und Loyalty können parallel auftreten, zum Beispiel wenn die Mitarbeiter keine Chance sehen, das Problem zu beheben oder wenn keine Jobalternativen zur Verfügung stehen.

Dabei verursachen die Mitarbeiter Schäden in mehrfacher Hinsicht, zum Beispiel: Abwanderung von Know-how (Exit), Kosten für Neueinstellung und Einweisungs- oder Schulungsphasen; Schäden, die durch die verminderte Arbeitsleistung des Täters entstehen, zum Beispiel „blau machen“ oder der so genannte „Dienst nach Vorschrift“(Neglect); direkte Schä-

Personalplanung und -entwicklung



Stratgisches Personalmanagement, insbesondere die Personalplanung und Personalentwicklung, ist der Kern eines integrierten Risiko- und Sicherheitsmanagements. So kann möglichen Aufwärts- oder Abwärtsspiralen vorgebeugt werden.

Quelle: Deutsche Risikoberatung

den, zum Beispiel Diebstahl, Unterschlagung, Spionage, die durch kriminelle Handlung(en) entstehen, (Beispiel: Nick Leeson und der Bankrott der Barings Bank) und eventuelle Folgeschäden, unter anderem Rufschädigung bei der Entdeckung der Straftat (zum Beispiel bei Korruptionsvergehen).

Vertrauen ist gut, Kontrolle ist besser

Welche Schlussfolgerung können wir aus unseren Überlegungen ziehen? Für die Entwicklung von Präventivmaßnahmen bedeutet dies, dass das Ermittlungs- und Kontrollsystem eines Unternehmens effizient und das Bestrafungssystem transparent sein müssen. Diese Aussage wird unter anderem durch die PWC-Studie bestätigt: Straftaten werden in Deutschland momentan eher durch Zufall als durch interne Kontrollsysteme (IKS) aufgedeckt (siehe auch KMPG: Studie 2006 zur Wirtschaftskriminalität in Deutschland). Es bedeutet aber auch, dass vor der kriminellen Handlung in der Regel eine negative Entwicklung der Produktivität beziehungsweise eine Motivation und Entwicklung der entsprechenden Mitarbeiter steht. Diese Überlegung sollte bei der Kriminalprävention und somit beim Aufbau eines umfassenden IKS nicht fehlen.

Strategisches Personalmanagement ist der Kern eines integrierten Risiko- und Sicherheitsmanagements. Wir wollen uns ein vereinfachtes System zur Steuerung und Überwachung des Personals unter dem Aspekt der Kriminalprävention anschauen. Dabei gehen wir von drei Annahmen aus. Erstens: Menschen verändern sich und entwickeln sich weiter. Zweitens: Unternehmen verändern sich und entwickeln sich weiter. Drittens: Jede Veränderung birgt neben Chancen auch Risiken und Gefahren. Um erfolgreich eine Veränderung umsetzen zu können ist es erforderlich, die Risiken und Gefahren zu kontrollieren.

Aufgaben der Personalabteilung

Die Aufgabe der Personalabteilung ist somit nicht nur, Stellen nach den momentanen Anforderungen zu besetzen und die Mitarbeiter zu bewerten, sondern auch wahrscheinliche Veränderungen zu antizipieren und die Weiterentwicklung der Mitarbeiter zu fördern. Was muss zum Beispiel Mitarbeiter X in der Abteilung Y leisten, um befördert zu werden, oder wie muss sich Mitarbeiter Z weiterentwickeln, um in Zukunft seine ihm vorgesehenen Aufgaben nachzukommen (siehe Dr. Guido Leidig, „Personal-Risikomanagement und Zukunftsherausforderung“, in ZRFG Risk, Fraud & Governance, 03/2007).

Entwickelt und qualifiziert sich der Mitarbeiter nicht weiter oder entspricht er nicht dem neuen und/oder zukünftigen Profil, so kann es passieren, dass er nicht befördert wird, man ihn in eine andere Abteilung versetzt, er innerhalb der Abteilung an Bedeutung verliert oder das Unternehmen verlassen muss (Abwärtsspirale). Wie oben aufgezeigt kann der Mitarbeiter auf diese negative Entwicklung unterschiedlich reagieren, aber in der Regel wird die Reaktion nicht positiv sein, im schlimmsten Fall sogar kriminell – getreu dem Motto: „Wie du mir, so ich dir“. Das bedeutet, dass dieser Mitarbeiter ein Risiko darstellt und vom Risikomanagementsystem erfasst werden muss.

> Ein sinnvolles internes Kontrollsystem sollte sowohl eine Überwachungsfunktion als auch eine Steuerungsfunktion haben.

Ein sinnvolles IKS sollte somit sowohl eine Überwachungsfunktion, aber auch eine Steuerungsfunktion beinhalten. Durch klare Zielvorgaben/Leistungsindikatoren (Key Performance Indicators) können dann für die einzelnen logischen beziehungsweise organisatorischen Einheiten sowie für die dort jeweils tätigen Mitarbeiter Leistungs- und Entwicklungsprofile ermittelt werden. Zusammen mit den zentral erfassten negativen Ereignissen/Entwicklungen der Mitarbeiter lassen sich damit sowohl negative wie auch positive Abweichungen (Trends) feststellen. Man kann überprüfen, in wie weit die momentan ermittelten Profile die Strategie des Unternehmens fördern oder belasten. Gleichzeitig dienen sie auch als Wegweiser, damit die Mitarbeiter wissen, was momentan und in Zukunft von ihnen erwartet wird.

Es sollte offensichtlich sein, dass die Vorgaben für die Richtwerte auch realistisch sein müssen, damit die einzelnen Einheiten und Mitarbeiter – bei gutem Willen, den wir hier voraussetzen – in der Lage sind, erfolgreich zu sein. Das setzt auch eine kontinuierliche Führung voraus, die nicht ständig den Kurs ändert und neue Ziele vorgibt.

Fazit: Keine Insellösungen

Die einzelnen Maßnahmen sollten nicht als Insellösungen betrachtet werden, sondern wie in der Einleitung angedeutet, in ein ganzheitliche Risiko- und Sicherheitsmanagementsystem integriert werden. Dabei ist die Hilfe durch externe Sicherheitsexperten zu empfehlen. Da sie nicht Teil der Organisation sind, können sie den Ist-Zustand unvoreingenommen und unabhängig testieren und beim Aufbau der Sicherheitsmaßnahmen helfen. ■

Carsten Baeck
ist Geschäftsführer der DRB Deutsche Risikoberatung GmbH in Berlin.

Marek Weber
ist Junior Consultant bei der DRB Deutsche Risikoberatung GmbH in Berlin.