



DEUTSCHLAND
EUROJURIS
INTERNATIONAL

Leitfaden zur Verhinderung von Wirtschaftskriminalität

Autor: Michael-Christian Rössner
Rechtsanwalt
Rössner Rechtsanwälte, Höchlstraße 4, 81675 München
Fon: 089/998922-0
Fax: 089/998922-33
E-mail: info@roessner.de
Internet: www.roessner.de

Inhalt:

Inhalt	S. 2
1. Kriminalität im oder gegen das Unternehmen	S. 3
2. Schutzgüter des Unternehmens	S. 4
3. Mögliche Angriffe von innen oder außen	S. 5
4. Wichtigste Grundsätze bei Schadensverdacht	S. 6
5. Richtige Erstmaßnahmen	S. 7
6. Wichtige Beweissicherungsmaßnahmen	S. 7
7. Effektive Problemlösungsstrategien	S. 8
8. Richtiger Umgang im Bereich der Information	S. 9
9. Gezielte Präventionsmaßnahmen	S. 10
10. Fallbeispiele	S. 11
11. Grundabsicherung des Unternehmens	S. 13
12. Notfallmanagement für den Fall des Gefahren Eintritts	S. 13
13. Erstinformation und regelmäßige Fortbildung	S. 15
14. Über den Autor	S. 15
Checkliste für gezielte Präventionsmaßnahmen	S. 16

Leitfaden für Eurojuris

Thema: Wie kann sich ein Unternehmen vor betriebsinterner oder betriebsexterner Kriminalität wirksam schützen?

1. Kriminalität im oder gegen das Unternehmen

Der laut Untersuchungen typische Täter stammt aus dem eigenen Unternehmen und ist meist ein nach außen hin angesehener Manager Anfang Vierzig mit beruflichem Erfolg und soliden wirtschaftlichen und familiären Verhältnissen. Der von diesem Täterkreis angerichtete Schaden liegt nach mehreren in Deutschland und in der Schweiz durchgeführten Erhebungen bei 65 %. Die geschätzten Schäden allein in Deutschland liegen bei 35 Milliarden Euro. Die Dunkelziffer der nicht aufgeklärten Fälle beträgt nach Schätzungen von Fachleuten bis zu 175 Milliarden Euro. Häufig gelingt es den Wirtschaftskriminellen nämlich, die von ihnen verursachten Schäden als Ergebnis unternehmerischer, im Tagesgeschäft getätigter Fehlentscheidungen darzustellen oder völlig zu verheimlichen. Psychologischer Hintergrund und Motive des Managers als Täter bilden vor allem der zunehmende Leistungsdruck, die Erwartung, bereits mit Mitte Vierzig durch jüngere Nachfolger ersetzt zu werden, unzureichende Kontrollsysteme, mangelnde Identifikation mit dem Unternehmen sowie der Verfall gesellschaftlicher Werte.

Aber nicht nur Topmanager, auch Angestellte in allen anderen Ebenen eines Betriebs können dem Unternehmen massiven Schaden zufügen. Ferner gibt es die Angriffe von außen, meist initiiert von Konkurrenzunternehmen. Die schädigenden Attacken können unterschiedlichster Art sein, in allen Fällen ist es für den Erfolg des Unternehmens von äußerster Wichtigkeit, dass Sicherheitsfragen als „Chefsache“ behandelt werden und im Betrieb ein umfassendes Sicherheits- und Kontrollsystem installiert ist, das Kriminalität am besten verhindert, zumindest aber sehr erschwert oder – beim Schadenseintritt – die richtigen Maßnahmen zur Schadensbehebung bereithält. Einzelne Abteilungen im Betrieb können umfassende Sicherheitskonzepte nicht entwickeln, da jeweils immer nur der eigene Bereich übersehen wird - „begrenzter Horizont“.

Eine weitere sehr ernste Tatform liegt im kollusiven Zusammenspiel von unternehmensinternen und –externen Personen. In Frage kommen bei den externen Schadensverursachern oft Lieferanten, Manager von Konkurrenzunternehmen sowie auch Kunden.

Besonders gefährdet sind die Branchen Medien, Dienstleistung, Kreditinstitute, das produzierende Gewerbe, Versicherungen und der Handel.

Hauptdelikte sind Unterschlagung, dicht gefolgt von Wechsel-, Scheck- und Kreditkartenbetrug, sodann Kreditbetrug, Diebstahl, Scheinrechnungen, private Nutzung von Vermögensgegenständen, gefälschte Jahresabschlüsse und Korruption. Im Bereich der Computerkriminalität gibt es auch eine Reihe von Fällen, hier ist es allerdings in der Regel sehr schwer erkennbar, geschweige denn nachweisbar, dass z.B. ein Hacker sich Zutritt zum EDV-System verschafft hat.

In dem am 27.4.1998 erlassenen „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich(KonTraG)“ hat der deutsche Gesetzgeber den Vorständen börsennotierter Aktiengesellschaften die Pflicht auferlegt, für ein angemessenes Risikomanagement in den Unternehmen zu sorgen. Dabei ging der Gesetzgeber davon aus, dass die damit verbundene Erweiterung der Überwachung und Organisationspflicht „auch auf den Pflichtenrahmen der Geschäftsführer

anderer Gesellschaftsformen ausstrahlt“. Deshalb sind Wirtschaftsprüfer auch angehalten, das Vorhandensein und die Tauglichkeit des Risikomanagementsystems in einem Unternehmen bei der Testierung zu überprüfen. Das Transparenz- und Publizitätsgesetz (TransPuG), das nach dem derzeitigen Stand der Gesetzgebung ab 1.1.2003 gelten wird, soll zum Schutz der Aktionäre die Zusammenarbeit zwischen Vorstand, Aufsichtsrat und Wirtschaftsprüfer weiter vertiefen und zudem die Rechnungslegung internationalen Standards anpassen.

In diesem Leitfaden werden die wichtigsten Checkpunkte aufgezeigt, mit denen sich jedes Unternehmen aufmerksam befassen sollte.

2. Schutzgüter des Unternehmens

Gemessen an einem auf die Unternehmensziele und die Unternehmenskultur abgestimmten Sicherheitsbedarf sind folgende wertbildenden Faktoren eines Betriebes durch ein angemessenes Sicherheitssystem zu schützen:

- a) **Personal**
 - **Geschäftsleitung, Management**
 - **Mitarbeiter**
- b) **Materielle Wirtschaftsgüter (insbesondere Sachgüter)**
 - **Produktionsmittel (Gebäude, Anlagen etc)**
 - **sonstige technische Einrichtungen (Computertechnik)**
- c) **Besonders geschützte immaterielle Wirtschaftsgüter**
 - **Geschäfts- und Betriebsgeheimnisse**
 - **Patente, Gebrauchsmuster, Geschmacksmuster, Warenzeichen, Marken**
- d) **Sonstige immaterielle Wirtschaftsgüter**
 - **Know How**
 - **Produktionsverfahren**
 - **Image**
 - **Kundenwertschätzung**

Den Vermögenswert eines Unternehmens bestimmt also nicht nur die materielle Ausstattung im Betrieb; auch andere Kriterien bilden Faktoren für die Gesamtbewertung und stellen somit einen eigenständigen wirtschaftlichen Vermögenswert dar. Dies wird bei der personellen Besetzung allein schon daraus ersichtlich, dass der Kenntnisstand, den ein Mitarbeiter durch die Tätigkeit für das Unternehmen erlangt, nicht vollumfänglich dem Unternehmen zusteht und für dieses gesichert werden kann. Nur an einem Beispiel soll dies verdeutlicht werden: das Gesetz gegen den unlauteren Wettbewerb (UWG) sichert das Unternehmen nur vor einzelnen bestimmten Verhaltensweisen der Ausforschung von außen. Dem Mitarbeiter kann es nicht insgesamt untersagt werden, seine Kenntnisse bei einem Konkurrenten einzubringen. Daher stellt jeder einzelne Mitarbeiter einen eigenen Vermögenswert dar, der gesichert werden muss.

Zum Schutze dieser Güter bedarf es interner Schutzmaßnahmen, bei denen die Mitarbeiter einbezogen sind (sog. innere Revision) und extern von Profis entwickelter Sicherheitsstrategien mit dazugehörigem Controlling (sog. externe Revision).

Es empfiehlt sich, einen professionellen Standard auf der Grundlage einer individuellen Risikoprofilanalyse des Unternehmens einzurichten, vergleiche dazu im Detail unten.

3. Mögliche Angriffe von innen oder außen

Die Angriffe von Straftätern können unmittelbar das Vermögen berühren; in diesem Fall beschränkt sich der Verlust meist auf den betroffenen Vermögensgegenstand selbst. Ein höheres Risikopotential wird durch Straftaten verursacht, bei denen der Angreifer zunächst lediglich Zugriff auf betriebsbezogene Informationen gewinnt, diese aber dann zu eigenen Zwecken verwertet und dabei Gewinne erzielt, die eigentlich dem Unternehmen selbst zugestanden wären. Auch bei Straftaten, die lediglich das Vertrauen in das Unternehmen beeinträchtigen, ohne es unmittelbar zu schädigen, liegt die eigentliche Gefahr für relevante Schädigung erst in der weiteren Entwicklung des Geschehens.

In Betracht zu ziehen sind hier demnach:

a) Straftaten gegen Eigentum des Unternehmens

Bei Straftaten gegen das Eigentum werden dem Unternehmen Sachwerte entzogen, so dass das Unternehmen diese Wirtschaftsgüter nicht mehr benutzen kann bzw. erst neu beschaffen muss. Daraus können sich weitergehende Schäden entwickeln, wenn die Ersatzbeschaffung zeitlichen Aufwand erfordert. Beispiele für solche Straftaten wären:

(Einbruch-)Diebstahl
 Raub
 Unterschlagung
 Sachbeschädigung
 Brandstiftung
 Sabotage

b) Straftaten, die sich unmittelbar gegen das Vermögen des Unternehmens richten

Kennzeichnend für diese Straftatbestände ist nicht der Verlust bestimmter Sachen; vielmehr wird hier das Vermögen des Unternehmens in anderer Weise beeinträchtigt. Anders als bei den oben genannten Straftaten wirken sich diese Straftaten zunächst allein unmittelbar vermögensmindernd aus:

Untreue mit Firmengeldern
 Korruption
 Erpressung
 Spesenbetrug, Abrechnungsbetrug
 Computerkriminalität, insb. auch EDV-Sabotage durch Vireneinschleusung
 Illegale Nutzung von Computerprogrammen
 Steuerstraftaten

c) Straftaten mit mittelbarem Vermögensbezug

Unter diese Gruppe werden Straftaten erfasst, bei denen sich der Vermögensnachteil nicht unmittelbar aus der Straftat ergibt. Das Unternehmen ist zwar Opfer der Straftat geworden, die sich aber nur mittelbar in Wettbewerbsnachteilen oder in Form von Beeinträchtigungen durch staatliche Sanktionen auswirkt:

Betriebsspionage, insbesondere durch Einschleusung von Spionen
 Patent-, Warenzeichen-, Gebrauchs-, Geschmacksmuster- und Markenverletzungen
 Verrat von Betriebs- und Geschäftsgeheimnissen
 Urheberrechtsverletzungen
 Wettbewerbsrechtliche Verstöße
 Ausspähen von Daten bzgl. des Unternehmens-Know-Hows, Verfahrenstechniken, Kundendaten, Werbekampagnen, Personaldaten, bevorstehende Transaktionen
 Verleumdung
 Üble Nachrede
 Beleidigung
 Subventionsbetrug
 Kreditbetrug
 Prozessbetrug
 Fälschung von Urkunden und anderen beweiserheblichen Datenträgern
 Verstoß gegen Umweltschutzvorschriften
 Geldwäsche
 Branchenspezifische Delikte
 Insolvenzstraftaten

d) Sonstige Beeinträchtigungen der Funktionsfähigkeit des Unternehmens

Auch Angriffe von innen und außen ohne strafrechtliche Relevanz können das Unternehmen in eine nachteilige Situation kommen lassen, indem die Funktionsfähigkeit in anderer Weise beeinträchtigt wird:

Mobbing
 head-hunting von Führungskräften
 Bestechung von internen Mitarbeitern oder externen Amtsträgern
 Vertrauensmissbrauch
 Anonyme Briefe
 Abhören
 Insider-Trading zulasten des Unternehmens
 Schaffung einer belastenden Indizienlage
 Imageschädigung des Unternehmens, Diffamierung
 Kartellbildung

4. Wichtigste Grundsätze bei Schadensverdacht

Folgende Fehler sollte die Unternehmensleitung unbedingt vermeiden:

- **Verdrängen, nicht wahrhaben wollen, bagatellisieren, bewusst tolerieren, aufschieben** – so treibt der Täter weiter sein Unwesen und man lockt Nachahmungstäter an.
- **Selbsthilfe trotz Unkenntnis des Umfangs des Schadens sowie der Identität aller Täterpersonen und bei unzureichenden Kenntnissen in diesem Spezialgebiet** – so warnt man den Täter nur, der alle Beweise vernichtet, sich vielleicht sogar unauffindbar ins Ausland absetzt, und verhindert infolge mangelnden Überblicks womöglich den gezielten erfolgreichen Zugriff auf Täter, Mittäter sowie Hinterleute, und auch die Vermögensschadenrückführung oft.

- **Emotionaler Rundumschlag ohne Sach Tatsachen:** Spontankündigung des Verdächtigen – dadurch fordert man diesen erst heraus, unmittelbar oder mit Hilfe der Konkurrenz noch weitaus größeren Schaden anzurichten.

5. Richtige Erstmaßnahmen

a) Geheimhaltungsgebot

Wichtig ist zunächst die Sicherung des Status quo. Es muss verhindert werden, dass Informationen gleich welcher Art an andere Personen weitergegeben werden, die nicht unmittelbar mit der Bekämpfung des Schadensfalles konfrontiert sind. Wegen der Gefahr persönlicher Rücksichtnahmen oder personeller bzw. finanzieller Verstrickungen sollte insbesondere der Firmenanwalt in das weitere Vorgehen nicht eingebunden werden.

b) Kompetenter Rat durch Externe

Vielmehr sollte sofort die Beratung durch eine auf derartige Fälle spezialisierte Anwaltskanzlei erfolgen, die aufgrund ihrer Erfahrung das Krisenmanagement übernimmt und die Sofortmaßnahmen koordiniert.

c) Bildung eines kleinen Krisenstabes

Auf höchster Unternehmensleitungsebene wird in Abstimmung mit der beratenden Kanzlei im engsten Vertrautenkreis unter Leitung der Anwaltskanzlei das weitere Vorgehen abgesprochen. Dabei ist die exakte Projektbeschreibung zu erfassen. Ein zu groß geratener Krisenstab birgt vor allem die Gefahr, dass wegen der Vielfältigkeit der dort vertretenen Interessen eine effektive Bekämpfung unnötig erschwert wird.

d) Weitergabe von Informationen und Festschreibung des Berichtsweges

Um die Gefahr der unbefugten Weitergabe von innerbetrieblichen Informationen möglichst weitgehend auszuschließen, muss festgehalten werden, wer im Unternehmen auf welchem Weg wann von der Anwaltskanzlei ohne Lauschrisiko informiert wird. Andernfalls können mögliche Löcher in der Informationspolitik nicht vermieden werden; es besteht zugleich die Gefahr der Nachahmung durch andere Betriebsangehörige, wenn ein entstandener Schaden nicht in effektiver Weise bekämpft wird.

e) Ausarbeitung von Reaktionsplänen

Für einzelne denkbare Entwicklungen, die aufgrund ihres Schadenspotentials ein schnelles Handeln erfordern, sollten durch den Krisenstab bereits präventiv Strategien entwickelt werden, die eine Ausweitung des Schadens möglichst unterbinden. Andernfalls könnte die gesamte Lage des Unternehmen außer Kontrolle geraten, der bereits eingetretene Schaden würde sich auf diese Weise in exponentieller Weise vergrößern.

6. Wichtige Beweissicherungsmaßnahmen

a) Vollständiges Erfassen der für die Krisenmanagement erforderlichen Informationen

Die Unternehmensleitung stellt schadensbezogen alle sofort verfügbaren Informationen zur Organisation, den Betriebsabläufen, den Mitarbeitern seines Unternehmens und zum konkreten Problembereich zusammen.

b) Firmeninterne Beweissicherung

Aus Gründen des Imageschutzes und der Prüfung des Umfangs des Schadens sollten Beweise zunächst ohne Einschaltung der Polizei gesichert werden. In Frage kommen hier insbesondere Informationen aus der EDV (z.B. email-Verkehr) sonstige Printunterlagen, die am Arbeitsplatz sichergestellt werden können! Die Einschaltung der Polizei führt im ungünstigsten Fall einerseits zu einer Beschlagnahme der entsprechenden Unterlagen im Wege des Strafverfahrens, so dass diese Informationen für eine betriebsinterne Schadensbekämpfung nicht mehr zur Verfügung stehen, andererseits kann das Unternehmen durch die damit häufig verbundene Publizität in den Medien in das Blickfeld einer breiten Öffentlichkeit geraten. Dies führt in vielen Fällen zu einem Imageschaden für das Unternehmen, wenn beispielsweise bekannt wird, dass der Betrieb wegen mangelnder interner Kontrollen zum Opfer von strafrechtlich relevanten Verhaltensweisen geworden ist.

Die Sicherung von Beweisen kann in vielen Fällen nur unter Einbeziehung von Fachleuten geschehen, da die meisten Täter ihre strafbaren Handlungen in engem Zusammenhang mit den von ihnen wahrgenommenen Aufgaben durchführen, so dass diese Handlungen meist „autorisiert und legal“ zu sein scheinen.

c) Weitere Maßnahmen zur professionellen Beweissicherung

Gegebenenfalls sollte eine auf diesen Bereich spezialisierte Detektei für Personenobservationen oder für die Auffindung wichtiger Unterlagen oder verschobener Vermögenswerte eingeschaltet werden, sofern dafür die firmeninternen Möglichkeiten nicht ausreichen.

In jedem Fall müssen falsche Beschuldigungen vermieden werden, da dadurch wiederum die Gefahr einer unerwünschten Publizität besteht, wenn sich ein zu Unrecht in Misskredit gebrachter Mitarbeiter an die Öffentlichkeit wendet. Das Unternehmen kann auch dann noch in einem schlechten Licht erscheinen, wenn die Untersuchung eines Schadensfalles durch hektische, unkoordinierte und nicht zielführende Erstmaßnahmen nach außen hin unprofessionell erscheint.

7. Effektive Problemlösungsstrategien

a) Festlegung der Ziele bei der Problembearbeitung

Primärziel einer Problembekämpfung ist zunächst, den Schaden möglichst zu begrenzen und Möglichkeiten der Schadenskompensation zu prüfen. Bei der Festlegung der Ziele sollte mit berücksichtigt werden, welche Ergebnisse unbedingt zu vermeiden sind.

b) Entwicklung einer geeigneten Strategie zur Problemlösung

An diesen festgelegten Zielen wird anschließend die Strategie entwickelt, in welcher Weise vorgegangen werden soll: hier gibt es jeweils eine Vielzahl von Möglichkeiten, die anhand des jeweiligen Einzelfalles erarbeitet und bis in alle Konsequenzen durchüberlegt werden. In der Regel wird ein Aktionsplan mit genau festgelegten Einzelschritten entwickelt, der die Aufgaben für die einzelnen Beteiligten innerhalb des Unternehmens, auf Seiten der koordinierenden und beratenden Kanzlei und für hinzugezogene externe Dienstleister mit klaren Zeitvorgaben enthält. Es finden täglich mehrmals telefonische Besprechungen mit der Unternehmensleitung statt, meist passieren die entscheidenden Schritte für den Erfolg der Strategie innerhalb weniger Tage. Einzelfallbezogen kreativ wird der beste Weg für das gewünschte Ziel erarbeitet und umgesetzt.

c) Sofortmaßnahmen zur Beschränkung von Schäden

Effektiver Rechtsschutz unmittelbar nach Entdeckung des Schadens kann durch einstweilige Maßnahmen wie z.B. einem Arrest oder einstweiligen Verfügungen erfolgen, die Verfügungsverbote enthalten oder vorläufig Unterlassungsansprüche titulieren.

Die dahinterstehenden Ansprüche auf Herausgabe von Gegenständen oder Schadensersatz sind später in der Hauptsache vor Gericht endgültig durchzusetzen.

Bei der Prüfung von Schadensersatzansprüchen kann auch an eine Inanspruchnahme von Versicherungen (Managerhaftpflichtversicherung, Vertrauensschadenversicherung) gedacht werden.

d) Einschaltung externer Behörden

Sollte ein Schadensfall nicht durch eigene Maßnahmen in hinreichender Weise bekämpft werden können, ist zu überlegen, inwieweit staatliche Behörden wie Polizei, Staatsanwaltschaft und Steuerfahndung, insbesondere aber auch Aufsichtsämter bei externen Angriffen mit ihren Ermittlungsmöglichkeiten dem Unternehmen helfen können, Verluste bei Wirtschaftsgütern auszugleichen. Bei dieser Einschaltung ist aber stets zu berücksichtigen, dass jede staatliche Ermittlungstätigkeit meist zu Einschränkungen bei der Funktionsfähigkeit eines Unternehmens führt und lange dauert. Staatliche Behörden sollten daher nur dann eingeschaltet werden, wenn die zu erwartenden Vorteile die daraus entstehenden Nachteile deutlich überwiegen.

8. **Richtiger Umgang im Bereich der Information**

a) Präventive Informationspolitik

Wichtig ist es auch, parallel zur Problemlösung als solcher geeignete Presseinformation zum richtigen Zeitpunkt mit dem richtigen Inhalt an die Öffentlichkeit zu geben. Bemühungen, einen eingetretenen Schadensfall zu vertuschen, bergen regelmäßig die Gefahr eines um so größeren Imageverlustes, wenn der Schadensfall nachträglich in das Bewusstsein der Öffentlichkeit gerät. Dieser Gefahr kann nur durch eine – wenn im Einzelfall erforderlich – offensive Informationspolitik begegnet werden. Ob eine

solche Information der breiten Öffentlichkeit erforderlich ist, kann nur nach den Umständen der jeweiligen Situation und aufgrund der Erfahrungswerte der Spezialisten in diesem Gebiet festgestellt werden. Maßnahmen der Informationspolitik sollten daher immer erst nach Abstimmung mit der beratenden Kanzlei veranlasst werden.

b) Entschärfung von negativer Presseberichterstattung

Sollte im Einzelfall eine eigentlich vorab notwendige Information unterblieben sein, so sind bei negativer Berichterstattung in der Presse die Vorwürfe transparent zu machen und vollumfänglich aufzuklären. Wichtig ist darüberhinaus, dass ferner alle (!) Mitarbeiter im Unternehmen veranlasst werden, im individuellen Gespräch mit Außenstehenden zugunsten des Unternehmens Partei zu ergreifen und im Interesse des erfolgreichen Fortbestehens des Betriebs und der Erhaltung der Kundenakzeptanz ein positives Bild des Unternehmens zu zeichnen.

9. Gezielte Präventionsmaßnahmen

Das Risiko eines Schadensfalles kann aber vorab bereits erheblich gemindert werden, wenn sich die Unternehmensführung nicht allein auf die Zuverlässigkeit der einzelnen Mitarbeiter verlässt, sondern durch gezielte Maßnahmen der Prävention die Möglichkeiten zur Schädigung einschränkt.

Betriebsintern sollten Regelungen für die Zuständigkeit in Sicherheitsfragen allgemein und aus besonderem Anlass bestehen. Jedem Mitarbeiter muss bewusst sein, dass die Unternehmensführung mit der Möglichkeit eines Schadens rechnet und Vorkehrungen für eine schnelle Reaktion im Falle eines Schadens getroffen hat. Dazu zählen:

- Präventionsmaßnahmen im sachlich-objektbezogenen Bereich
- Erarbeitung und Publizierung von Leitlinien zur Unternehmensphilosophie und zur Unternehmensethik.
- Installation eines Frühwarnsystems mit einer Vielzahl klar beschriebener Indikatoren (z.B. bei Budgetüberschreitungen; Überweisungszweck „Diverses“; Nachvergütungsforderungen bei Beratungsverträgen mit ursprünglichem Festhonorar; plötzliche Verbesserung des Lebensstandards eines Mitarbeiters; plötzliche Übernahme zuständigkeitfremder Aufgaben; unerklärliche Wochenendarbeit im Betrieb; Absonderung, Verschlossenheit eines Mitarbeiters; Kontakte zur Konkurrenzmitarbeitern; Verzicht auf Beförderung; u.v.m.).
- Verbesserung der internen Kontroll- und Steuerungssysteme sowie des externen Unternehmensschutzes insgesamt.
- Festschreibung der offiziellen Kontrollsysteme in einem für alle Mitarbeiter verbindlichen „Sicherheitshandbuch“.
- Folgende firmeninterne Richtlinie bekannt machen: „Verpflichtung aller bei einem Straftatverdacht, die Unternehmensleitung sofort vertraulich zu informieren, dabei kein Risiko einer persönlichen Inanspruchnahme oder von Nachteilen.“ Also Anreiz: interne Kronzeugenregelung.
- Keine Anonymität in den Vorstandsetagen, sondern gute Zusammenarbeit und menschliche Kontakte fördern.
- „Lean management“, also eine schlanke, kostengünstige Struktur im Führungsbereich, darf nicht auf Kosten der Sicherheit gehen.
- Regelmäßiges internes und externes Controlling.
- Anonyme Hinweise ernstnehmen.

- Ständige Weiterentwicklung der Sicherheitsstandards durch interne Gremien und mit Hilfe der Beratung durch externe Dienstleister (Kanzleien, Sicherheitsdienstfirmen).
- Strengeres Auswahlverfahren bei der Personaleinstellung und –beförderung.
- Mitarbeiterschulungen im Sicherheitsbereich, sog. „Sicherheits-Work-shops“.
- Job-/Personalrotation kann vor allem im Bereich der Auftragsvergabe sinnvoll sein, um zu hohe Kompetenz- und Machtkonzentration und damit Bestechlichkeit bei einzelnen Angestellten zu vermeiden.
- Sicherstellung der Mitarbeiterzufriedenheit und der Loyalität der Angestellten durch sensiblen Kontakt und offenes, Kreativität förderndes Gesprächsklima.
- Regelmäßige Management-Meetings zu Fragen der Sicherheitsverbesserung.
- Genauere Recherchen vor der Aufnahme von Geschäftstätigkeit im Ausland.
- Sorgfältige Auswahl von in- und ausländischen Geschäftspartnern.
- Abschluss von Vertrauensschadensversicherungen und Managerhaftpflichtversicherungen

Sollte dann im Einzelfall doch ein Schadensfall Realität geworden sein, sind die oben unter Punkten 4 bis 8 dargestellten Maßnahmen zu ergreifen und mögliche Nachahmungstäter durch eine angemessene Straftatverfolgung wirksam abzuschrecken.

10. Fallbeispiele

Fall 1: Veruntreuung von Firmengeldern durch den angestellten Geschäftsführer

Der Geschäftsführer eines mitteldeutschen Unternehmens zweigte sich privat große Summen ab, die er mit fingierten Rechnungen für angebliche Rohstofflieferungen auf diverse Konten in der Schweiz überwies.

Was tun? Die Unternehmensleitung ging einem anonymen Hinweis nach und schaltete ohne jede weitere Rücksprache mit anderen Betriebsmitarbeitern eine spezialisierte Kanzlei ein. Es wurde gemeinsam überlegt, welche Beweise es schon gab (Rechnungen an unbekanntem angeblichen Zulieferer und damit in Zusammenhang stehende Zahlungsausgänge) und ob ein externer Buchprüfer diskret beigezogen werden konnte (verdeckte Buchprüfung). Es erfolgte dann die Einschaltung einer professionellen Detektei, die nach den näheren Verhältnissen bei der angeblichen Zuliefererfirma recherchierte und die Zahlungsflüsse bis ins Ausland nachvollzog. Da es Anzeichen gab, dass der kriminelle Geschäftsführer sich ins Ausland absetzen könnte, beantragte die Kanzlei einen Arrest im In- und Ausland bezüglich der veruntreuten Gelder und schob kurz darauf eine Strafanzeige an die Staatsanwaltschaft nach. Die veruntreuten Gelder konnten in mehreren Verfahrensschritten zurückgeholt werden, der Täter kam ins Gefängnis und die anderen mittleren Führungskräfte im Unternehmen waren beeindruckt und von derartigen Verhaltensweisen abgeschreckt durch die schnelle und effiziente Problemlösung.

Fall 2: Wirtschaftlicher Schaden durch Verrat von Betriebsgeheimnissen durch einen bestochenen Mitarbeiter an die Konkurrenz

Ein exklusives Modeunternehmen wurde von der Konkurrenz ausspioniert. Die Mitbewerberfirma hatte offenbar einen Spion in das Unternehmen eingeschleust oder einen leitenden Mitarbeiter bestochen. Es war auffällig, dass das Konkurrenzunternehmen mit fast völlig gleichen Entwürfen stets zwei Wochen vorher auf den Markt kam und das Hauptgeschäft machte.

In diesem Fall war der Unternehmensleitung klar, dass die Konkurrenz einen Mitarbeiter bestochen oder einen Spion eingeschleust haben musste, nur kannte niemand dessen Identität. Die diskret eingeschaltete Anwaltskanzlei befragte die Unternehmensleitung detailliert zu allen tatsächlichen Abläufen und es stellte sich heraus, dass nur drei Chefdesigner die Möglichkeit zur Tatausführung hatten, da die Entwürfe unter strengsten Sicherheitsvorkehrungen aufbewahrt wurden.

Es wurde dann ein Detektiv als Beobachter eingeschleust (angeblicher Verwandter des Chefs, der in die Branche hineinschnuppern wollte), ferner wurden Videokameras versteckt am Safe mit den Entwürfen eingebaut. Nach acht Wochen wurde der Täter entlarvt, als er die Entwürfe nachts aus dem Safe nahm und im Betrieb kopieren wollte. Die Aufdeckung erfolgte jedoch erst, nach man den Täter bei der Übergabe der kopierten Entwürfe an einen Mitarbeiter des Konkurrenzunternehmens beobachtet hatte und dies durch Detektivfotos nachweisbar dokumentieren konnte. Nunmehr konnte man gegen den eigenen Mitarbeiter und das Konkurrenzunternehmen erfolgreich zivil- und strafrechtlich vorgehen. Das Konkurrenzunternehmen wurde auf Zahlung von Schadensersatz für die Geschäftseinbußen durch die bereits zuvor gestohlenen Entwürfe verklagt. Zur Vermeidung eines geschäfts-schädigenden Presseskandals zahlte das Konkurrenzunternehmen vergleichsweise eine große Entschädigungssumme.

Die Unternehmensleitung war froh, denn sie hatte die Gefahr weiterer Diebstähle behoben. Außerdem wurden alle anderen Mitarbeiter abgeschreckt. Die internen Sicherheitsstandards wurden durch laufende Videoüberwachung der Entwürfe verbessert und der wirtschaftliche Schaden war größtenteils wiedergutmacht worden. Einen Imageschaden gab es nicht. Das Ansehen der kompetenten Unternehmensleitung ist in der Firma jedoch noch mehr gestiegen.

Fall 3: Entwendete Schecks

Aus der Poststelle eines renommierten Markenartikelherstellers in Bayern wurden laufend Schecks entwendet und bis zur Aufdeckung über dubiose Firmen und Privatpersonen meist im Ausland eingezogen.

Analyse:

- Schwachstellen durch Zeit- (Leih-) Angestellte, Aushilfskräfte
- Fehlen jeglicher Sicherheitsvorkehrungen
- Erhöhter Schaden durch langes Zuwarten

In einem Parallellfall sprach ein angeblicher Firmenangehöriger auf telefonische Anweisung des Täters direkt bei der Post vor und leerte wiederholt Firmenpostfächer und entwendete dabei diverse Schecks.

Fall 4: Gefälschte Überweisungen im Außenwirtschaftsverkehr

Auftraggeber und geschädigter Betrieb war ein schwäbisches Textilunternehmen. Der zeichnungsberechtigte Geschäftsführer hatte deckungsgleich Unterschriften der Mitzeichnungsverpflichteten von korrekten Überweisungsformularen übernommen und Euro 250.000 an eine Gesellschaft spanischen Rechts mit Domizil bei Barcelona und spanischer Bankverbindung leiten wollen.

Analyse:

- Ein Schreibfehler bei der spanischen Bankadresse führte zu Rückfragen durch die angewiesene Bank beim Unternehmen (Zufall).
- Die Recherchen ergaben eine ad-hoc-Gesellschaftsgründung in Spanien mit mittellosem Strohmann als Geschäftsführer, der den Scheck einlösen hatte wollen.
- Ein Schadenseintritt konnte verhindert werden.

Fall 5: Gestohlene Ware wurde durch Privatverkäufe abgesetzt

In einem nordrhein-westfälischen Textilunternehmen wurde gestohlene, beim Warenversand nicht fakturierte und an der Rampe nicht kontrollierte Ware über Hotel- und Privatverkäufe abgesetzt. Der beauftragte Anwalt schaltete eine Detektei ein, die Hintergründe wurden aufgedeckt, die Beweismittel gesichert und der Polizei übergeben. Der Anwalt erwirkte zeitgleich einen Arrest in das gesamte Vermögen der Täter, es kam zur Schadenswiedergutmachung. Den Tätern wurde darüber hinaus gekündigt und sie wurden vor das Strafgericht gestellt und verurteilt.

11. Grundabsicherung des Unternehmens durch die Erarbeitung eines maßgeschneiderten Sicherheitskonzeptes durch eine spezialisierte Kanzlei in fachübergreifenden Kooperationen mit externen Dienstleistern:

- Schaffung einer übersichtlichen Organisationsstruktur mit „Mehr-Augen-Prinzip“ bei sicherheitsrelevanten Entscheidungen.
- Identifizierung der sensiblen Firmenbereiche und Aufdeckung von Sicherheitsschwachpunkten.
- Überprüfung und Implementierung vorbeugender Kontrollsysteme.
- Erarbeitung einer Betriebsphilosophie und Unternehmensethik mit klarem Leitbild und konkreten Verhaltensmaßstäben.
- Ermutigung aller Angestellten zu einer engagierten „Dienstaufsicht“.
- Erkennen, warum solche Straftaten begangen werden, Mitarbeiterzufriedenheit schaffen, Fortbeschäftigung von Managern als Berater auch nach einer aktiven Phase.

12. Notfallmanagement für den Fall des Gefahreneintritts: rasche, kompetente und konkrete fallbezogene Problemlösung in engster Zusammenarbeit einer spezialisierten Anwaltskanzlei mit der Unternehmensleitung:

- Soforthilfe durch Erstmaßnahmenbesprechung.
- Erstellung und Umsetzung eines Krisenplanes.
- Ausführliche persönliche Beratung und Betreuung der Unternehmensleitung zu allen Fragen des Konfliktfalles.
- Schulung und Information derjenigen Mitarbeiter im Unternehmen, die in die Problemlösung ohne Sicherheitsrisiko einbezogen werden sollen.
- Beziehung und Überwachung wichtiger externer Dienstleister.
- Steuerung der Informationspolitik.

- Nachbereitung des Problemfalles u.v.m.

Der Bereich der umfassenden Wahrnehmung der Interessen des Unternehmers bei Fragen der Abwehr von kriminellen Schäden stellt eine Schnittstelle zwischen einer Reihe von wichtigen grundsätzlich getrennten Kompetenzen dar. Es geht um

- Werkschutz,
- Strafrecht,
- Zivilrecht,
- Ausspüren verschwundener Gelder („following the money trail“),
- detektivische Recherchen,
- Wirtschafts-, Steuer- und Bilanzrecht,
- Kriminologie,
- Täterpsychologie,
- konkrete Branchenkenntnisse und um
- Rechtskenntnisse in all diesen Bereichen.

Der auf diese an Unternehmen gerichtete Dienstleistung spezialisierte Anwalt verfügt nicht nur über die erforderlichen Rechtskenntnisse, sondern bringt große Erfahrung mit im Bereich der gerichtsverwertbaren Tatsachenerfassung und Beweissicherung. Das ist besonders wichtig vor dem Hintergrund, dass polizeiliche Ermittlungen oft jahrelang dauern, dass dabei unzählige eigentlich benötigte Unterlagen beschlagnahmt und Mitarbeiter zeitraubend befragt werden und dann obendrein auch noch ein Imageschaden durch Presseveröffentlichungen und somit unter Umständen eine Kundenabschreckung zu befürchten sind. Ein weiterer Schwerpunkt des spezialanwaltlichen Könnens ist die Entwicklung der besten Strategie für den konkreten Einzelfall. Diese wird in enger Zusammenarbeit mit der Unternehmensleitung unter Beachtung aller Besonderheiten zielorientiert erarbeitet und in genau festgelegten Einzelschritten sofort effektiv umgesetzt. Der Unternehmer erhält eine hochkompetente „Komplettberatung und -unterstützung“, in der alle Fragen bis hin zur besten Informationspolitik im und außerhalb des Betriebs beantwortet und die Handlungsabläufe genau festgelegt werden.

Dabei ist es ein großer Vorteil, dass der spezialisierte Anwalt als Externer sein Fachwissen einbringt, da interne Mitarbeiter, ja selbst Justitiare oft „betriebsblind“ und zu wenig bereit zu manchmal auch für sie unbequemen zusätzlichen Sicherheitsmaßnahmen sind. Mitunter liegt sogar ein verdeckter Interessenkonflikt oder ein innerer Abwehrmechanismus vor, wenn der Angestellte sich selbst oder sogar seine Vorgesetzten in einem Konzept strengen Kontrollen unterwerfen soll. Im Falle eines definitiv eingetretenen Schadens besteht darüber hinaus die Ungewissheit, ob der Justitiar nicht den Täter deckt oder gar mit diesem zusammenarbeitet.

Im Bereich der Rückholung von veruntreuten Geldern ist die Hilfe des externen Spezialisten unverzichtbar, da nur bei entsprechend großem Know How und mit den richtigen externen Dienstleistern verstecktes Vermögen aufgespürt werden kann. Sobald Geldmittel entdeckt sind, kann man im Wege eines bei Gericht beantragten Arrestes den Zugriff des Täters auf die entwendeten Summen verhindern. Soweit Gelder bereits ins Ausland transferiert worden sind, wird geprüft, ob der deutsche Arrest im Ausland vollstreckt werden kann oder ob über eine ausländische Anwaltskanzlei weitere Rechtsmaßnahmen erforderlich sind. Hat sich der ungetreue Mitarbeiter ein Haus auf den Namen seiner Ehefrau mit Firmengeldern gekauft, gibt es weitere rechtliche Möglichkeiten, die der darauf spezialisierte Anwalt kennt und ausschöpfen wird. Die Zusammenarbeit mit einer professionellen Kanzlei empfiehlt sich vor allem auch vor dem Hintergrund, dass die Wirtschaftskriminellen von heute immer intelligenter, skrupelloser und raffinierter vorgehen. Die Straftaten sind vom Täter oft in monatelanger Vorberei-

tung präzise geplant und unter Ausnutzung aller Kontrollschwächen des Unternehmens dann durchgeführt worden. Verschachtelte Gesellschaftsstrukturen im Ausland als Geldempfangsstelle erschweren die Spurensuche erheblich. Diesen Umstand sollte die Unternehmensleitung durch die Wahl von dem Täter überlegenen Fachleuten zum Vorteil des Unternehmens ausgleichen.

13. Erstinformation und regelmäßige Fortbildung für Unternehmer zum Thema

Die Sicherheit des Unternehmens gegenüber kriminellen Angriffen ist „Chefsache“. Also ist es unumgänglich, dass sich Mitglieder der Leitung größerer Unternehmen nicht nur ein Basiswissen zugänglich machen, sondern sich auch regelmäßig in diesem Bereich fortbilden – entweder durch eine konkrete Einzelberatung oder durch die Teilnahme an Seminaren zum Thema. Namhafte Kanzleien bieten in diesem Zusammenhang in unterschiedlichem Umfang Veranstaltungen zu den sicherheitsbezogenen Hauptthemen an.

14. Über den Autor

Rechtsanwalt Rössner berät Unternehmen gegen Schäden aus Wirtschaftskriminalität. Seine spezialisierte Kanzlei ist bei der Überprüfung von Verdachtsfällen, der Aufklärung strafbarer Handlungen zum Schaden des Unternehmens und bei der Durchsetzung von Schadensersatz und geeigneten Strategien behilflich.

Die Kanzlei wurde vom heutigen Senior Rechtsanwalt Michael-Christian Rössner, 1976 gegründet und beschäftigt insgesamt 8 Rechtsanwälte. Er spezialisierte sich bereits vor Gründung seiner Kanzlei auf internationale Verfahren im Bereich des Anlegerschutzes sowie auf das Gebiet der internationalen Wirtschaftskriminalität.

Rössner Rechtsanwälte

www.roessner.de

07/02

Anhang: Checkliste

Checkliste für gezielte Präventionsmaßnahmen

Wichtige Sicherheitsfragen:

	Sehr abdeckt uns.	gut bei	Sollten wir vielleicht verbessern!	Muss dringend verbes- sert wer- den, hierzu holen wir uns In- formati- onen ein:
Festlegung der betriebsinternen Zuständigkeit für Sicherheitsfragen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Präventionsmaßnahmen im sachlich-objektbezogenen Bereich	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Erarbeitung und Publizierung von Leitlinien zur Unternehmensphilosophie und zur Unternehmensethik	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Installation eines Frühwarnsystems mit Indikatoren	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Festschreibung der offiziellen Kontrollsysteme in einem für alle Mitarbeiter verbindlichen „Sicherheitshandbuch“	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Regelmäßiges internes und externes Controlling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Strengeres Auswahlverfahren bei der Personaleinstellung und –beförderung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mitarbeiterschulungen im Sicherheitsbereich, sog. „Sicherheits-Workshops“	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sicherstellung der Mitarbeiterzufriedenheit und der Loyalität der Angestellten durch sensiblen Kontakt und offenes, Kreativität förderndes Gesprächsklima	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Erstellung von Kriterien für die Aufnahme von Geschäftstätigkeit im Ausland	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Abschluss von Vertrauensschadensversicherungen und Managerhaftpflichtversicherungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Copyright Rössner Rechtsanwälte