

Aktuell. Detailliert. Fundiert.

Wirtschaft Konkret Nr. 302



EULER HERMES
Kreditversicherung

Gewappnet für den Ernstfall

Rechtzeitige Vorsorge ist ein guter Schutz gegen Vertrauensschäden

Inhalt

302 Gewappnet für den Ernstfall

3	Editorial	9	Worauf es ankommt	16	Checkliste: Wie sicher ist Ihr Unternehmen?
4	Die Dimension der Wirtschaftskriminalität	9	Die Fakten sprechen für sich	18	Weiterführende Links
4	Gefahr für alle Unternehmen	10	Auch Topmanager als Täter		
6	Wer sind die Täter?	10	Auf Warnsignale achten		
7	Lücken in der betrieblichen Sicherheit	11	Wirtschaftskriminalität im Datennetz		
8	Welche Unternehmen sind betroffen?	11	Daten sind beweglich		
8	Die Gefahr wird verdrängt	12	Risiken eingrenzen		
8	Risiken im Mittelstand	13	Nicht Sparen an der IT-Sicherheit		
8	Risiken in großen Unternehmen	14	Im Ernstfall konsequent handeln		
		14	Den Fall aufklären		
		14	Schutz vor Veruntreuung		
		15	Kasten: Was ist versichert?		

Impressum

„Wirtschaft Konkret“ ist eine Veröffentlichung der Euler Hermes Kreditversicherungs-AG, Friedensallee 254, 22763 Hamburg.

Verantwortlich: Hans Joachim Kasperski, Euler Hermes Kreditversicherungs-AG. **Redaktion:** Rainer Hupe Kommunikation, Hochallee 77, 20149 Hamburg.

Layout: Type Art Team Detlef Rögner GmbH, Kieler Straße 1, 25451 Quickborn.

Informationen nach bestem Wissen, jedoch ohne Gewähr. Nachdruck (auch auszugsweise) nur mit Genehmigung des Herausgebers.

Stand: Februar 2008

Editorial



Vertrauensschäden

Wenn Grenzen überschritten werden

Die Klage ist häufig zu hören: Der allgemeine Werteverfall schreitet unaufhaltsam voran, Loyalitäten gegenüber Mitarbeitern, Vorgesetzten und der eigenen Firma spielen eine immer geringere Rolle; Vertrauen und die Bedeutung von Anstandsregeln schwinden. Hinzu kommt andererseits der immer schärfere Wettbewerb in der internationalen Wirtschaft – sowohl zwischen Unternehmen als auch zwischen den Mitarbeitern in den Firmen.

Die Folgen werden regelmäßig mit einschlägigen Statistiken belegt: Wirtschaftskriminalität nimmt zu, Unternehmen sind immer größeren Risiken ausgesetzt – extern wie intern. Korruption, Bestechlichkeit, Industriespionage sind immer häufiger zu beklagen genauso wie Diebstahl oder Unterschlagung durch Mitarbeiter, private Nutzung von Unternehmenseigentum oder Computerkriminalität.

Auch wenn die Unternehmen die Gefahr grundsätzlich erkennen, in Bezug auf ihre eigene Situation sind sie überraschend arglos. Wirtschaftskriminalität gilt meistens nur als Risiko bei den anderen, so das Ergebnis von einschlägigen Umfragen und Studien. Und dies obwohl die große Mehrzahl der Manager gleichzeitig glaubt, dass die Wirtschaftskriminalität weiter ansteigen wird.

Dabei kann man sich wirksam auf vielfältige Weise schützen – auch durch geeignete Versicherungen. Voraussetzung ist allerdings, die eigene Lage realistisch zu analysieren. Dabei will die vorliegende Broschüre helfen.

*Rainer Hupe
Chefredakteur*



Die Dimension der Wirtschaftskriminalität

Gefahr für alle Unternehmen

Täglich kommt es in deutschen Unternehmen zu Schäden durch Wirtschaftskriminalität. Die Gefahr ist praktisch allgegenwärtig, dies ergab eine von der Euler Hermes Kreditversicherungs-AG in Auftrag gegebene Untersuchung. Sie erfasst alle Unternehmen in Deutschland mit einem Umsatz von mehr als einer Million Euro und ist damit repräsentativ für den Mittelstand. Danach sind für 86 Prozent der Befragten wirtschaftskriminelle Handlungen in Betrieben ein ernsthaftes Problem. Ein Drittel der Unternehmen wurde innerhalb der letzten drei Jahre tatsächlich Opfer von Wirtschaftskriminalität, wovon wiederum drei Viertel durch eigene Mitarbeiter oder zumindest deren Beteiligung geschädigt wurden.

Bemerkenswert sind sowohl die Häufigkeit als auch die Höhe der Schäden, denn jedes von Wirtschaftskriminalität betroffene Unternehmen wurde im Durchschnitt nicht nur sechsmal innerhalb von drei Jahren Opfer externer Delikte, sondern hatte auch noch einen Schaden von durchschnittlich 296.000 Euro zu beklagen. Siebenmal

im Schnitt wurden die Betriebe sogar im gleichen Zeitraum von eigenen Mitarbeitern geschädigt, mit einem mittleren Schaden von 73.000 Euro.

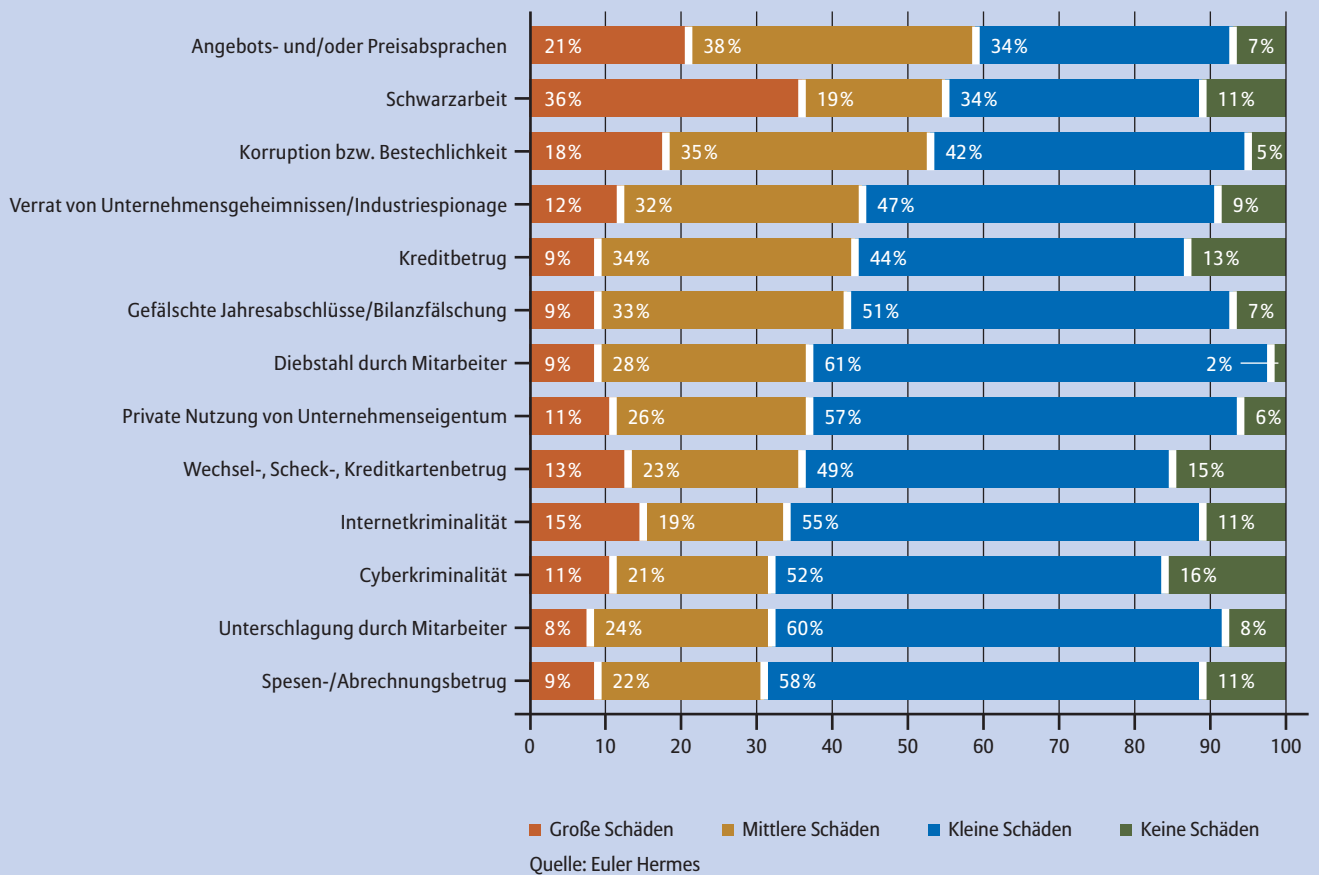
Insgesamt schätzen die Befragten in der Euler Hermes-Studie den gesamtwirtschaftlichen Schaden auf bis zu 100 Milliarden Euro im Jahr.

Mehr als die Hälfte der Unternehmen geht davon aus, dass die Wirtschaftskriminalität weiter zunehmen wird. Darin drückt sich nicht nur der allgemeine Pessimismus aus, sondern vor allem auch die Ansicht, der wirtschaftliche Existenzkampf werde sich noch verschärfen.



Für wie groß halten Sie das Ausmaß der Schäden, die in Ihrer Branche verursacht werden durch...

(Einschätzung der Schäden insgesamt)



Wer sind die Täter?

Immer häufiger müssen Arbeitgeber die Erfahrung machen, dass unredliche Machenschaften von Beschäftigten Schäden im eigenen Betrieb verursachen. Es gibt offensichtlich so etwas wie die alltägliche Veruntreuung, über die Unternehmer nicht gern sprechen. Versicherungen, die einen gezielten Schutz gegen innerbetriebliche Kriminalität bieten, verzeichnen allerdings seit Jahren gute Zuwächse (siehe Grafik).

Allein der polizeilich registrierte Gesamtschaden für Betrugs-, Untreue- und Unterschlagungsdelikte belief sich 2006 auf 4,0 Milliarden Euro. Euler Hermes schätzt, dass 40 Prozent dieser Fälle von eigenen Arbeitnehmern verursacht wurden. Ernst & Young kommt in seiner Umfrage sogar zu dem Ergebnis, dass über die Hälfte der Täter aus

den eigenen Reihen kommen. Betrug und Unterschlagungen finden häufig in Unternehmen und Abteilungen statt, in denen Buch- und Bargeld umgesetzt wird. Auch alle Bereiche, die direkt mit Waren oder mit der Buchhaltung zu tun haben, gelten als besonders gefährdet.

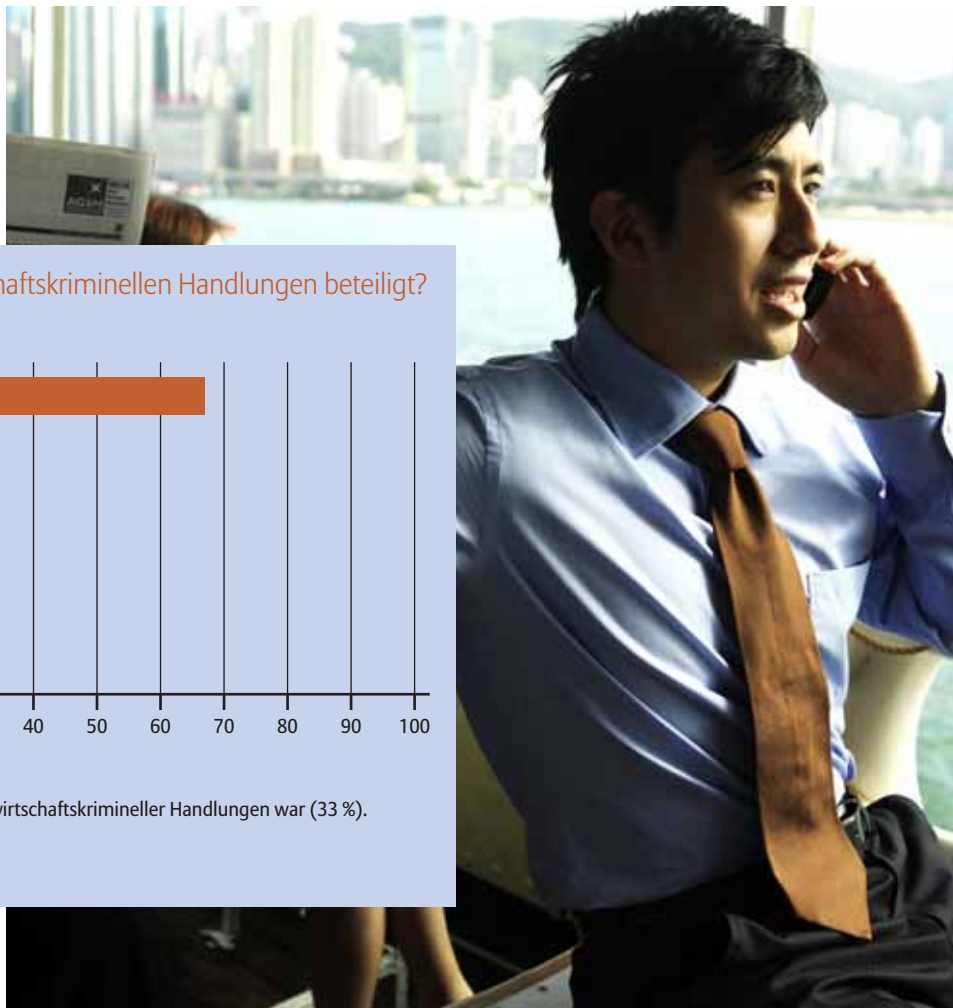
Immerhin sieben Prozent der von Euler Hermes Befragten nennen auch das Management als Gefahrenquelle, was besonders bemerkenswert ist, weil genau diese Personengruppe befragt wurde. Doch auch das erscheint plausibel, denn es sind vor allem die Mitarbeiter mit großem internen Wissen, die einem Unternehmen erheblichen Schaden zufügen können.

Was aber ist der Grund dafür, dass Wirtschaftskriminalität und auch Bestechlichkeit seit Jahren zunehmen und auch in Zukunft steigen werden,

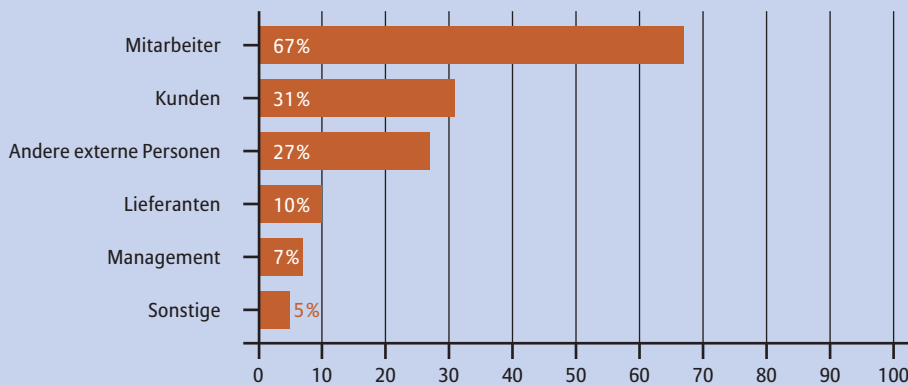
wie alle einschlägigen Untersuchungen mehr oder weniger deutlich belegen? Der allgemeine Werteverfall ist ein beliebtes Argument, nahezu 90 Prozent aller Unternehmen sehen im schwindenden Unrechtsbewusstsein einen Grund für die ansteigende Wirtschaftskriminalität.

Doch ohne Zweifel spielen auch persönliche Motive eine wichtige Rolle:

- Immer mehr Menschen leben über ihre Verhältnisse, geraten in finanzielle Engpässe und in Gefahr, sich zu überschulden.
- Materielle Güter und das eigene Fortkommen gewinnen für den Einzelnen deutlich an Bedeutung.
- Wirtschaftliche Unsicherheiten wie die Angst vor Entlassung senken die Loyalität gegenüber dem Unternehmen zusätzlich.



Welcher Personenkreis war an den wirtschaftskriminellen Handlungen beteiligt?



Frage wurde nur gestellt, wenn das Unternehmen Opfer wirtschaftskrimineller Handlungen war (33 %).

Quelle: Euler Hermes

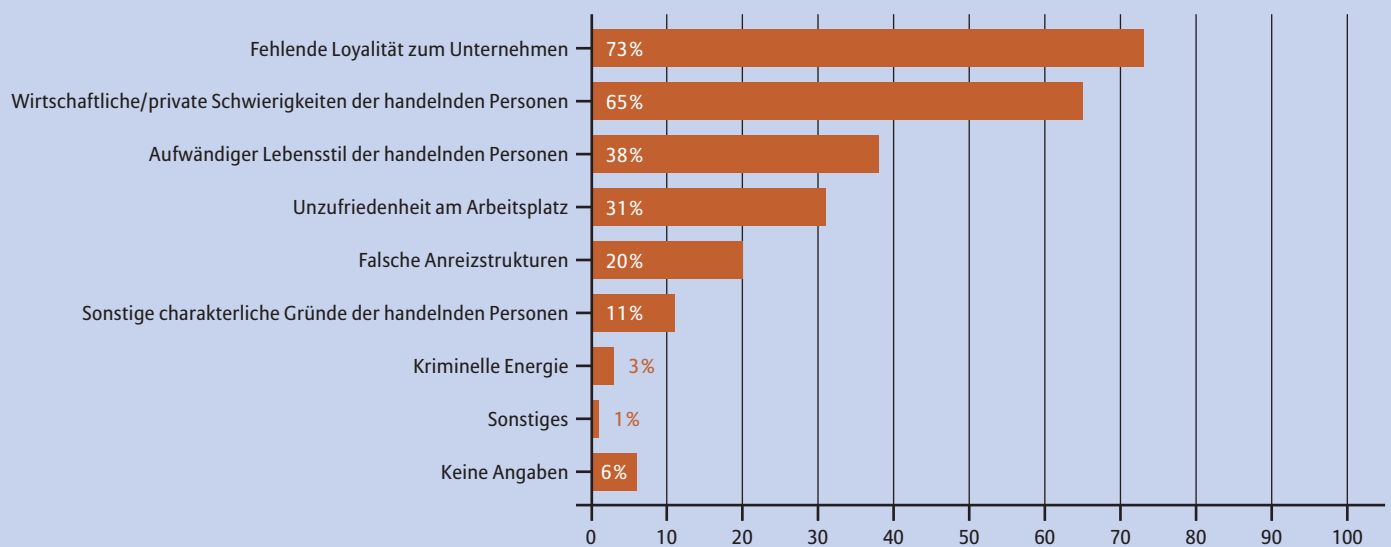
Lücken in der betrieblichen Sicherheit

Veränderungen im Unternehmen führen gleichfalls oft zu Sicherheitslücken, denn dadurch werden oft bewährte Organisationen und Kontrollmechanismen geschwächt. Das fängt mit Re- oder Neuorganisationen an, Stichwort Lean Management, und endet bei Firmenfusionen. Die daraus resultierenden Auswirkungen auf die Ablauforganisation schaffen mindestens vorübergehend Unsicherheit bei den Mitarbeitern und damit Lücken in der Sicherheit. Sie bilden Risiken, die ein betriebliches Kontroll- und Sicherheitssystem zwar eingrenzen, aber nicht sicher ausschalten kann.

Hinzu kommen vernetzte DV-Arbeitsplätze, die es erleichtern, Firmendaten zu manipulieren und in die eigene Tasche zu wirtschaften. Die Gefahr wächst also – gerade in Zeiten zunehmender Anonymisierung der Arbeitsverhältnisse, steigenden Arbeitsvolumens und erhöhten Termindrucks.



Welche Umstände waren mit ursächlich für die in Ihrem Unternehmen begangenen wirtschaftskriminellen Handlungen?



Mehrfachnennungen möglich.

Quelle: KPMG 2006



Welche Unternehmen sind betroffen?

Die Gefahr wird verdrängt

Veruntreuung kann jedes Unternehmen treffen, unabhängig von Branche und Größe. Die Ergebnisse der Umfrage von Euler Hermes belegen sogar eindeutig, dass Wirtschaftskriminalität viel mehr kleine und mittlere Unternehmen trifft als große: Über 80.000 Firmen mit einem Umsatz bis zu zehn Millionen Euro waren in den vergangenen drei Jahren Opfer gesetzeswidriger Handlungen, aber nur 13.700 in der nächsten Gruppe mit Umsätzen bis zu 50 Millionen und nur gut 3.700 mit darüber liegenden Umsätzen.

Im Kern sind die Ursachen für Veruntreuung sowohl in mittelständischen als auch in großen Unternehmen die bereits genannten: Verfall gesellschaftlicher Werte sowie veränderte Arbeitsbedingungen. Die Art der Risiken unterscheidet sich jedoch nach Unternehmensgröße.

Risiken im Mittelstand

In mittelständischen Unternehmen mit relativ überschaubaren Mitarbeiterzahlen ist die Arbeitsatmosphäre häufig noch durch eine persönliche, vertrauensvolle Unternehmenskultur geprägt. Mitarbeiter werden flexibel eingesetzt und nehmen häufig mehrere Funktionen wahr.

Lösen sich die betrieblichen Hierarchien auf und gewinnen Mitarbeiter unabhängig von ihrer Position Einblicke in vertrauliche administrative Prozesse und Betriebsinterna, ist allerdings Vorsicht geboten. Denn diese Kenntnisse können zu Fehlverhalten verleiten. Fazit: Vertrauen ist notwendig und richtig, einen ausreichenden Schutz vor Veruntreuung bietet es nicht.

Risiken in großen Unternehmen

In großen Unternehmen sind die Verantwortlichkeiten eindeutiger verteilt. Nur wenige Mitarbeiter sind autorisiert, mit sensiblen Firmendaten umzugehen. Schäden entstehen eher aus der steigenden Anonymität und Komplexität der Unternehmensstrukturen. In der Folge sind Kontrollen schwieriger und Sicherheitslücken bleiben oft unentdeckt.

Als strukturelle Faktoren, die Risiken bergen, sind vor allem zu nennen:

- Neuorganisationen und fortschreitende Dezentralisierung.
- Wachsende Kompetenzen für den einzelnen Mitarbeiter.
- Abbau von Kontrollinstanzen.
- Bündelung von Funktionen zur ganzheitlichen Bearbeitung von Geschäftsabläufen.

Worauf es ankommt

Aufmerksamkeit ist angebrachter als Entwarnung. Alle Marktstudien deuten auf einen starken Anstieg der Wirtschaftskriminalität hin. Diametral im Gegensatz dazu aber steht das Bewusstsein für die eigene Gefährdung.

Die Fakten sprechen für sich

In vielen Führungsetagen wird das eigene Risiko wesentlich geringer eingeschätzt als das allgemeine Risiko. Grundsätzlich glaubt ohnehin nur ein zehntel der Firmen, so das Ergebnis der Euler Hermes Umfrage, selbst einem erhöhten Risiko ausgesetzt zu sein, ganz im Gegensatz zur allgemeinen Einschätzung. Kleine und mittlere Firmen sehen das Risiko darüber hinaus vor allem bei großen Firmen – ein eklatanter Widerspruch zur Realität.

Denn die Fakten sind eindeutig, wie auch eine im Jahre 2006 veröffentlichte Umfrage der Wirtschaftsberatung KPMG belegt. Danach

- meinen 62 Prozent der Unternehmen, dass die Wirtschaftskriminalität in nächster Zeit steigen wird,
- wurde von Einzelschäden in einer Höhe von über 1 Milliarde Euro berichtet,
- halten 77 Prozent die eigenen Präventionsmaßnahmen allerdings für ausreichend, obwohl lediglich 18 Prozent die eigene Kenntnis wirtschaftskrimineller Handlungsmuster als gut bezeichnen.

Die befragten Unternehmen schätzen, dass auf jeden entdeckten Fall fünf nicht entdeckte Fälle von Wirtschaftskriminalität kommen. Das geschätzte Dunkelfeld beträgt also nach Einschätzung der Unternehmen über 80 Prozent.

Zeichen für Veruntreuung

- Auffallende Inventurdifferenzen.
- Veränderung im Verhalten oder Lebensstil von Mitarbeitern.
- Abweichende finanzielle Entwicklung des Unternehmens.
- Hinweise von Mitarbeitern.



Auch Topmanager als Täter

Der typische Täter ist – auch wenn es auf den ersten Blick nicht plausibel erscheint – meist gut in ein Unternehmen eingebunden. Ein Viertel der Schäden geht auf Täter im Management zurück. Fast jeder zwanzigste Täter gehört zur Geschäftsleitung. Angesichts des vergleichsweise geringen Anteils der Manager an der gesamten Firmenbelegschaft eine bemerkenswert hohe Zahl. Zudem verursachen Manager mit weitreichenden Befugnissen und Verantwortlichkeiten wesentlich höhere Schäden.

Vertrauensschäden werden am häufigsten durch interne Kontrollsysteme wie die Revision aufgedeckt oder durch die eigenen Mitarbeiter. Gleich danach folgt der Faktor Zufall (siehe Grafik). In einer Vielzahl der Fälle spielt er eine weitaus bedeutendere Rolle bei der Aufklärung als interne und externe

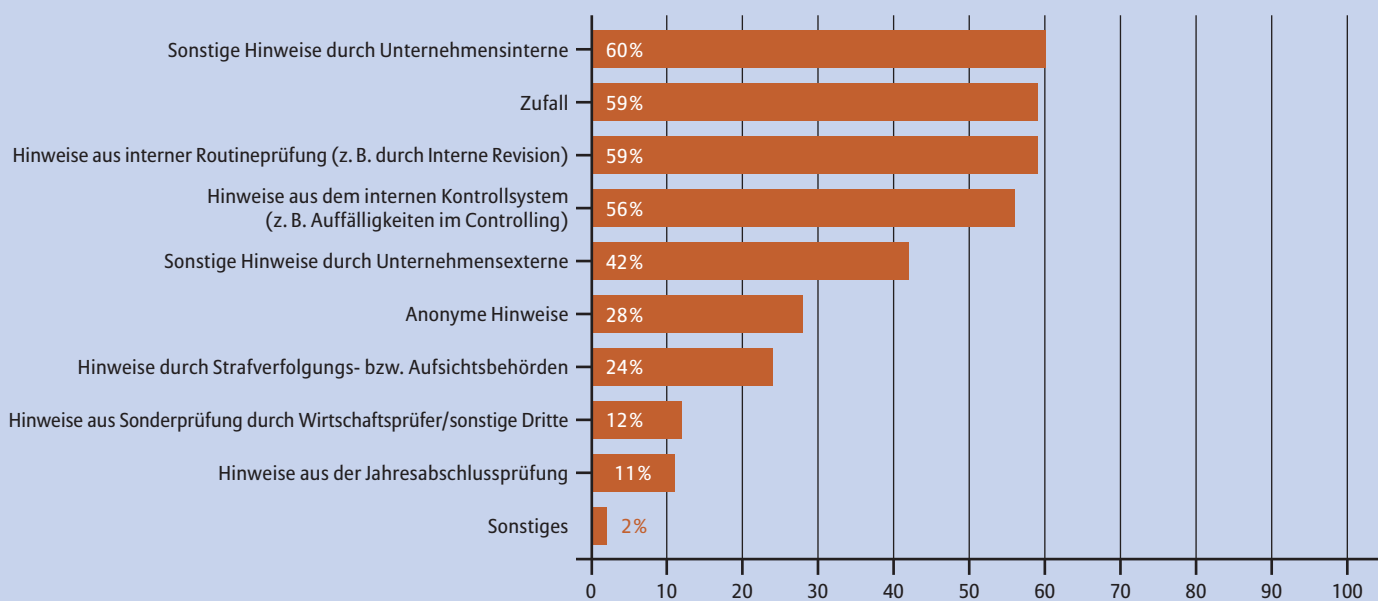
Hinweise oder Polizei und Staatsanwaltschaft. Ist ein Schaden begrenzt und der Schadenersatz geregelt, spielt die Klärung der Ursachen oft nur eine untergeordnete Rolle. Veruntreuungsschäden gelten als Image schädigend und werden deshalb oftmals nicht publik gemacht. Obwohl das Problem bekannt ist, möchte kein Unternehmen in den Ruf geraten, Mitarbeiter zu haben, die sich am Geld des Unternehmens oder der Kunden bereichern.

Auf Warnsignale achten

Umso wichtiger ist es, frühzeitig Warnsignale zu erkennen und zu beachten. Laut der KPMG-Marktforschung sind 58 Prozent der geschädigten Unternehmen der Ansicht, dass die Fälle wirtschaftskrimineller Handlungen durch höhere Sensibilität der Mitarbeiter hätten vermieden werden können.



Wodurch sind Sie auf die in Ihrem Unternehmen begangenen wirtschaftskriminellen Handlungen erstmalig aufmerksam geworden?



Mehrfachnennungen möglich.

Quelle: KPMG 2006



Wirtschaftskriminalität im Datennetz

Elektronische Medien und Datenverarbeitung sind heute in Unternehmen selbstverständlich und unverzichtbar – bei Lohnbuchhaltung, Kommunikation, Auftragsbearbeitung und im Zahlungsverkehr. Der Einsatz intelligenter Datenverarbeitungssysteme birgt eigene Risiken. Dennoch schätzen die Unternehmen mehrheitlich die Gefahr von Delikten im IT-Bereich zu niedrig ein.

Daten sind beweglich

Angriffe auf E-Mail- und Internet-Systeme nehmen zu, Datenbanken werden manipuliert und eingeschleuste Viren zerstören Informationen. Der ungehinderte Zugriff auf Daten ist für den Täter oft ein Kinderspiel, denn sie liegen konzentriert vor und sind deshalb schnell und in großem Umfang ebenso verfügbar wie veränderbar. Gleichzeitig ist der Zugriff auf Speichermedien wesentlich schwerer zu kontrollieren als auf Akten aus Papier. Die Daten können in Sekundenbruchteilen

unbemerkt eingesehen und modifiziert werden. Und das nicht nur von jedem intern vernetzten Arbeitsplatz aus – sondern auch von außen durch Hacker.

Das Personal in Schlüsselpositionen wie der EDV, der Systemadministration und den IT-Abteilungen sollte deshalb höchst sorgfältig ausgewählt werden. Denn auf den Einsatz dieser Spezialisten muss sich ein Unternehmen verlassen können, insbesondere wenn es um komplexe Softwarelösungen für spezielle Probleme geht.



Risiken eingrenzen

Die hohe Präzision und Funktionalität der IT-Systeme verleitet dazu, in der Alltagsroutine die Notwendigkeit wirksamer Schutzmaßnahmen zu unterschätzen. Über 90 Prozent der Unternehmen gehen davon aus, dass beispielsweise die Gefahr, über das Computersystem ausspioniert zu werden, gering ist (Ernst & Young). Die Tatsachen widersprechen dieser Einschätzung. Bei der internen Kontrolle sollten alle Sicherungsmöglichkeiten genutzt werden, die ein IT-System bietet.

Dennoch bleiben Risiken – aber sie lassen sich eingrenzen. Ein effektives Risk Management erfordert keinen hohen Aufwand, sondern vor allem Aufmerksamkeit an den entscheidenden Punkten:

- Neue Mitarbeiter sorgfältig auswählen: Der persönliche Eindruck und das fachliche Können reichen als Kriterien nicht aus. Arbeitszeugnisse und Papiere sollten ebenfalls gründlich geprüft werden. Auf Lücken im Lebenslauf muss es eine plausible Antwort geben.
- Doppelt absichern: Das Vier-Augen-Prinzip sollte konsequent eingehalten werden. Die zweite Unterschrift darf also keinesfalls nur dekorativen Charakter haben. Das Risiko verringert sich deutlich, wenn eine kontrollierende Instanz vorhanden ist. In sensiblen Bereichen sollten außerdem Zeichnungsberechtigte immer persönlich unterschreiben.
- Geldflüsse organisieren: Im Umgang mit Geld gilt die Regel: wenn möglich keine Schecks. Denn diese Zahlungsform ermöglicht es, Einträge zu ändern oder Vordrucke mit gefälschter Unterschrift auszufüllen.
- Arbeitsbereiche klar definieren: Bestimmte Unternehmensbereiche sollten getrennt sein. Dies gilt sowohl für die Finanz- und Debitorenbuchhaltung als auch für die Kasse und den Verkauf. Wichtig sind auch exakt ausgearbeitete Arbeitsplatzstrukturen. Kompetenzen und Funktionen müssen klar aufgeteilt, Jobs genau beschrieben und Arbeitsabläufe eindeutig definiert sein.
- Atmosphäre bereinigen: Auch der Führungsstil spielt eine nicht unbedeutende Rolle. Ist das Betriebsklima angenehm und die Entlohnung angemessen, sinkt das Risiko. Mit steigender Entfremdung vom Arbeitgeber sinkt andererseits die Hemmschwelle. Missstimmungen im Betrieb können Ausdruck von Konflikten mit schwerwiegenden Folgen sein.
- Ungewöhnliche Entwicklungen erkennen: Ein wichtiges Stichwort der Gefahrenvorsorge heißt soziale Kontrolle. Damit ist keineswegs Überwachung gemeint, sondern ein sensibler Blick für die Stimmigkeit im Lebensstil der Mitarbeiter. Nicht jede Veränderung der Lebensverhältnisse ist gleich ein Anzeichen für Veruntreuung. Ungewöhnlich große Abweichungen sind aber Alarmzeichen.
- Bestände regelmäßig prüfen: Inventuren sind ein geeignetes Mittel, um Versuchungen im Keim zu ersticken und Abweichungen schnell festzustellen. Zudem ist eine tägliche Kontrolle der Kassenbestände zu empfehlen.

Nicht Sparen an der IT-Sicherheit

Datensicherheit steht und fällt mit dem Engagement des Managements. Es muss sich dazu bekennen und entsprechende Grundsätze und Richtlinien aufstellen (Wirtschaft Konkret Nr. 301 „Ein sicheres Netz“). Ein ganzheitliches System, das höchstmögliche und effektive Datensicherheit im Unternehmen gewährleistet, ist genauso Chefsache wie Absatz, Produktion oder Kostenmanagement. Im Aktiengesetz ist festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die ein Risiko für das Unternehmen sein können, nicht mit dem geeigneten Risikomanagement überwacht.

Dies erfordert neben den organisatorischen und software-technischen Voraussetzungen auch eine ausreichende finanzielle Ausstattung. Einer der häufigsten Fehler in Betrieben, fast unabhängig von der Größe, ist aber, dass Sicherheit nur als Kostentreiber gesehen wird und besonders bei Neuanschaffungen die Sicherheitseigenschaften des Systems vernachlässigt werden.

Eine Umfrage von Ernst & Young bei 1.400 IT-Verantwortlichen und Geschäftsführern in 66 Ländern ergab, dass die Unternehmen weltweit an ihrer IT-Sicherheit sparen und damit ihre strategischen Geschäftsziele gefährden. Als wichtigsten Grund für bestehende Sicherheitslücken nannten 16 Prozent der Unternehmen unausgereifte Technologien, immerhin 55 Prozent aber verweisen auf Budgetbeschränkungen.

Rund die Hälfte der Befragten nennt Viren und Würmer als große Gefahr, immerhin ein Drittel aber sieht auch in leichtsinnigem oder absichtlichem Fehlverhalten von Mitarbeitern ein enormes Risiko. Dennoch geben 83 Prozent der Unternehmen das meiste Geld für die Anschaffung neuer Hard- und Software aus, aber nur 29 Prozent investieren nennenswerte Summen in die Aus- und Fortbildung der Mitarbeiter und damit in deren Sensibilisierung für Gefahren.





Im Ernstfall konsequent handeln

Trotz aller Vorsichtsmaßnahmen lassen sich Veruntreuungen nicht vermeiden. Wichtig ist, in solchen Fällen richtig und schnell zu reagieren. Bei Eintritt eines Schadens muss zunächst die Sicherheitslücke großflächig geschlossen werden, damit weitere Schäden vermieden werden können. Beim EDV-Netzwerk bedeutet dies unter Umständen nicht nur neue Passwörter, sondern das Passwortssystem insgesamt umzustellen.

Den Fall aufklären

Auf jeden Fall müssen die Verantwortlichen ermittelt oder zumindest der Kreis der eventuell in Frage kommenden Personen eingegrenzt werden. Manchmal sind es nur wenige, die in der Lage sind, eine unerlaubte Handlung auf eine bestimmte Weise zu verüben.

Ist der Fall aufgeklärt, dürfte eine fristlose Kündigung die beste Lösung sein. Ein möglichst notariell beurkundetes Schuldanerkenntnis erleichtert den Haftungsnachweis und die Rechtsverfolgung. Ist der Mitarbeiter nicht bereit, seine Schuld schriftlich anzuerkennen, muss die Haftungsfrage gerichtlich geklärt werden. Auch eine Strafanzeige kann sinnvoll sein, denn aus dem Strafverfahren können sich ggf. zusätzliche Anhaltspunkte für die Schadenhöhe ergeben.

Schutz vor Veruntreuung

Wirksame Kontrollen können helfen, eventuellen Vermögensverlusten vorzubeugen und entstandenen Schaden frühzeitig zu erkennen und zu begrenzen. Einen ausreichenden Schutz bieten sie allerdings nicht. Eine sinnvolle Absicherung besteht aus dem Zusammenwirken dreier Komponenten:

- Vertrauen zu den Mitarbeitern,
- Regelmäßige Optimierung des betrieblichen Sicherheitssystems,
- Vorkehrungen für den Fall der Fälle, zum Beispiel durch eine Vertrauensschadenversicherung.



Was ist versichert?

Eine Vertrauensschadenversicherung schützt vor Vermögensschäden, die von Betriebsangehörigen und anderen Vertrauenspersonen vorsätzlich verursacht werden. Gedeckt sind die finanziellen Folgen von Schäden durch Diebstahl, Unterschlagung, Betrug (einschließlich Computerbetrug), Untreue, Geheimnisverrat oder sonstige vorsätzliche unerlaubte Handlungen, die zum Schadenersatz verpflichten – wie zum Beispiel Sachbeschädigung oder Sabotage.

Dabei sind nicht nur eigene Vermögensschäden versichert, sondern auch Schäden, die Dritten vorsätzlich zugefügt werden. Zusätzlich sind Hackerschäden durch unmittelbare und rechtswidrige Eingriffe in die elektronische Datenverarbeitung des Versicherungsnehmers versichert. Der Versicherungsschutz gilt weltweit. Es sind alle Unternehmen, an denen der Versicherungsnehmer mit mehr als 50 Prozent beteiligt ist, mitversichert.

Der Versicherungsschutz gilt für alle Arbeitnehmer, Angestellten, Aushilfen, Praktikanten und Zeitarbeitskräfte sowie für Geschäftsführer und Vorstandsmitglieder mit maximal 20 Prozent Anteilsbesitz. Die Versicherung zahlt, wenn der Täter namentlich ermittelt wurde oder sich aus dem Sachverhalt ergibt, dass der Schaden mit überwiegender Wahrscheinlichkeit durch eine Vertrauensperson vorsätzlich verursacht worden ist.



Checkliste:

Wie sicher ist Ihr Unternehmen?

	Ja	Nein
1. Risikofaktor Unternehmensstruktur		
Sind die Arbeitsabläufe und -prozesse in Ihrem Unternehmen klar definiert?	<input type="checkbox"/>	<input type="checkbox"/>
Sind die Kompetenzen und Verantwortlichkeiten der Mitarbeiter eindeutig schriftlich festgelegt?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es in Ihrem Hause Verantwortliche, die sich über notwendige und mögliche Sicherheitsvorkehrungen auf dem Laufenden halten?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es Verantwortliche für die Planung, Durchführung und Kontrolle von Sicherheitsmaßnahmen?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Sicherheitsmaßnahmen in der Aufbau- und Ablauforganisation berücksichtigt?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es Katastrophenpläne im Unternehmen?	<input type="checkbox"/>	<input type="checkbox"/>
2. Risikofaktor Personalbeschaffung		
Werden von Bewerbern alle Zeugnisse der letzten drei Jahre verlangt und Lücken im Beschäftigungsnachweis geklärt?	<input type="checkbox"/>	<input type="checkbox"/>
Wird bei Bewerbern mit ungewöhnlichen Kündigungsterminen oder häufigem Stellenwechsel die Ursache ergründet?	<input type="checkbox"/>	<input type="checkbox"/>
Werden bei Bewerbern für Schlüsselpositionen weitergehende Prüfungen (Referenzen) vorgenommen?	<input type="checkbox"/>	<input type="checkbox"/>

	Ja	Nein
Sind sämtliche Mitarbeiter schriftlich zur Geheimhaltung der Firmeninterna verpflichtet?	<input type="checkbox"/>	<input type="checkbox"/>
Wird durch Job-Rotation die Abhängigkeit von Spezialisten gemindert?	<input type="checkbox"/>	<input type="checkbox"/>
Hat das Management ein Krisenszenario für Vertrauensschadenfälle?	<input type="checkbox"/>	<input type="checkbox"/>
3. Risikofaktor EDV		
Wurden für die Entwicklung und Wartung von Programmen Richtlinien aufgestellt, die allen Sicherheitsaspekten Rechnung tragen?	<input type="checkbox"/>	<input type="checkbox"/>
Sind die Bereiche EDV-Entwicklung und EDV-Produktion getrennt?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es ein geregeltes Programm-übernahmeverfahren?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es für Ihr EDV-System ein Sicherheitskonzept?	<input type="checkbox"/>	<input type="checkbox"/>
Nutzen Sie alle Sicherheitspotenziale, die Ihr EDV-System bietet?	<input type="checkbox"/>	<input type="checkbox"/>
Klassifizieren Sie sämtliche Daten nach ihrer Schutzwürdigkeit und treffen entsprechende Schutzmaßnahmen?	<input type="checkbox"/>	<input type="checkbox"/>
Ist Ihre EDV gegen Angriffe von außen geschützt?	<input type="checkbox"/>	<input type="checkbox"/>

	Ja	Nein
Gibt es ein Berechtigungskonzept?	<input type="checkbox"/>	<input type="checkbox"/>
Werden alle Zugriffsrechte nach dem „Need-to-know-Prinzip“ vergeben und Passwörter regelmäßig geändert?	<input type="checkbox"/>	<input type="checkbox"/>
Ist ein periodischer Passwortwechsel vorgesehen?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es im Unternehmen ungesicherte Internetanschlüsse?	<input type="checkbox"/>	<input type="checkbox"/>
Sind Online-Verbindungen zur Hausbank ausreichend geschützt?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es einen Verantwortlichen für EDV-Sicherheit?	<input type="checkbox"/>	<input type="checkbox"/>
Existiert ein Sicherungskonzept für alle Daten?	<input type="checkbox"/>	<input type="checkbox"/>
4. Risikofaktor Zahlungsverkehr		
Sind Buchhaltung und Kasse streng getrennt?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Scheckvordrucke unter Verschluss gehalten, und werden Nummernkreise kontrolliert?	<input type="checkbox"/>	<input type="checkbox"/>
Verzichtet das Unternehmen soweit wie möglich auf Schecks?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es in Ihrem Unternehmen Unterschriftenfaksimiles?	<input type="checkbox"/>	<input type="checkbox"/>
Sind dabei vorgelagerte Kontrollen vorgesehen?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es Verfahren/beschriebene Arbeitsabläufe für Scheckverkehr, Überweisungen und Zahlungsverkehr?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Schriftstücke mit rechtlich bindendem oder verpflichtendem Inhalt jeweils von zwei Personen unterschrieben (4-Augen-Prinzip)?	<input type="checkbox"/>	<input type="checkbox"/>
Wird der Kassenbestand mindestens einmal monatlich von einer anderen Person als dem Kassierer überprüft?	<input type="checkbox"/>	<input type="checkbox"/>
5. Risikofaktor Post		
Wird die eingehende Post mit einem Eingangsstempel versehen?	<input type="checkbox"/>	<input type="checkbox"/>

	Ja	Nein
Werden eingehende Schecks in einem Eingangsbuch notiert?	<input type="checkbox"/>	<input type="checkbox"/>
6. Risikofaktor Einkauf/Verkauf		
Sind verschiedene Personen jeweils verantwortlich für		
– die Auftragserteilung,	<input type="checkbox"/>	<input type="checkbox"/>
– die Registrierung eingehender Waren,	<input type="checkbox"/>	<input type="checkbox"/>
– die Genehmigung der Bezahlung von Waren?	<input type="checkbox"/>	<input type="checkbox"/>
Werden regelmäßige Inventuren des Warenbestandes durchgeführt?	<input type="checkbox"/>	<input type="checkbox"/>
Erfolgt unmittelbar bei Anlieferung eine Kontrolle der Zugänge auf Übereinstimmung mit der Bestellung hinsichtlich Art, Qualität und Menge?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Retouren gesondert erfasst?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Mitarbeiter im Umgang mit Lieferanten, Banken und Behörden besonders geschult?	<input type="checkbox"/>	<input type="checkbox"/>
Werden Zweitrechnungen (z.B. bei Verlust) als solche kenntlich gemacht?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es klare Richtlinien für die Einholung mehrerer Angebote oder die Durchführung von Ausschreibungsverfahren?	<input type="checkbox"/>	<input type="checkbox"/>
Hat das Unternehmen einen Verhaltenskodex für Einkäufer?	<input type="checkbox"/>	<input type="checkbox"/>
Gibt es eindeutige Anweisungen für die Identifizierung und Behandlung von Ausschussproduktionen?	<input type="checkbox"/>	<input type="checkbox"/>
7. Risikofaktor Revision/Kontrollen		
Haben Sie eine eigene Revisionsabteilung?	<input type="checkbox"/>	<input type="checkbox"/>
Prüft diese bzw. ein Wirtschaftsprüfer regelmäßig alle Bereiche Ihres Unternehmens?	<input type="checkbox"/>	<input type="checkbox"/>
Ist das 4-Augen-Prinzip durchgehend in Ihrem Unternehmen implementiert?	<input type="checkbox"/>	<input type="checkbox"/>



Weiterführende Links*

www.bka.de/pks/
Kriminalstatistik

www.bsi.bund.de
Bundesamt für Sicherheit
in der Informationstechnik (BSI)

www.mcert.de
Spezielle Hilfe für den Mittelstand

*Für den Inhalt der Seiten ist die
Euler Hermes Kreditversicherungs-AG
nicht verantwortlich.

Bei weiteren Fragen helfen Ihnen gern:

Hans Peter Kröber
Euler Hermes Kreditversicherungs-AG
Tel.: +49 (0) 40/88 34-50 15
Fax: +49 (0) 40/88 34-50 25
E-Mail: hans-peter.kroeber@eulerhermes.com

Dr. Jan-Lubomir Heidinger
Euler Hermes Kreditversicherungs-AG
Tel.: +49 (0) 40/88 34-50 32
Fax: +49 (0) 40/88 34-50 50
E-Mail: jan-lubomir.heidinger@eulerhermes.com

Rüdiger Kirsch
Euler Hermes Kreditversicherungs-AG
Tel.: +49 (0) 40/88 34-50 14
Fax: +49 (0) 40/88 34-50 29
E-Mail: ruediger.kirsch@eulerhermes.com

Anhang

In der Reihe „Wirtschaft Konkret“ sind außerdem erschienen:

Schutz vor Forderungsausfall

Nr. 100	Liefern unter Vorbehalt – Wie Unternehmen ihre Eigentumsrechte durchsetzen können
Nr. 103*	Vertrauen durch Transparenz – Internationale Standards der Rechnungslegung
Nr. 104*	Im sicheren Hafen – Die richtige Finanzierung für hohe Risiken im Auslandsgeschäft
Nr. 105	Auf der sicheren Seite – Der richtige Schutz vor Forderungsausfall und seinen Folgen

Avale

Nr. 201	Sicherheiten im Baugeschäft – Wie sich Auftraggeber gegen Ausfälle und Mängel schützen
----------------	--

Schutz vor Veruntreuung

Nr. 301*	Ein sicheres Netz – Computerrisiken sind Chefsache
-----------------	--

Allgemeine Themen

Nr. 401	Zensuren für die Firma – Rating setzt sich auch in Deutschland durch
Nr. 404*	Erfolgreich neue Märkte erobern – Worauf es bei der Expansion ins Ausland wirklich ankommt
Nr. 412*	Wissen richtig managen – Das Know-how der Mitarbeiter ist das Kapital für künftigen Erfolg
Nr. 414	Ursachen von Insolvenzen – Gründe für Unternehmensinsolvenzen aus der Sicht von Insolvenzverwaltern
Nr. 416	Fair Trade und Umwelt – Handel(n) ohne Grenzen
Nr. 417	Die Zukunft Deutschlands – Bildung und Demografie im Wandel
Nr. 418	Rettung aus der Insolvenz – Chancen, Barrieren und die besondere Rolle von Private Equity

* Nur im Internet abrufbar.

Diese Broschüren liegen als Druckstücke nur unter Vorbehalt vor. Zu beziehen über Euler Hermes Kreditversicherungs-AG, Hamburg. Alle Ausgaben sind auch im Internet verfügbar unter www.wirtschaft-konkret.de

Euler Hermes
Kreditversicherungs-AG
Friedensallee 254
22746 Hamburg
Tel. + 49 (0) 40/88 34-0
Fax + 49 (0) 40/88 34-77 44
info.de@eulerhermes.com
www.eulerhermes.de

Sie finden uns ganz in Ihrer Nähe

Hauptverwaltung

22763 Hamburg
Friedensallee 254
Postanschrift
22746 Hamburg
Tel. +49 (0) 40/88 34-0
Fax +49 (0) 40/88 34-77 44
info.de@eulerhermes.com

Niederlassungen und Geschäftsstellen

12435 Berlin
An den Treptowers 1
Tel. +49 (0) 30/20 28 43-00
Fax +49 (0) 30/20 28 43-01
nl.berlin@eulerhermes.com

33602 Bielefeld
Zimmerstraße 8
Tel. +49 (0) 5 21/9 64 56-0
Fax +49 (0) 5 21/9 64 56-50
gs.bielefeld@eulerhermes.com

28195 Bremen
Martinistraße 34
Tel. +49 (0) 4 21/1 65 97-0
Fax +49 (0) 4 21/1 65 97-49
gs.bremen@eulerhermes.com

44137 Dortmund
Westfalen-Center
Lindemannstraße 79
Tel. +49 (0) 2 31/1 82 99-0
Fax +49 (0) 2 31/1 82 99-99
gs.dortmund@eulerhermes.com

01129 Dresden
Rieser Straße 5
Tel. +49 (0) 3 51/8 53 77-0
Fax +49 (0) 3 51/8 53 77-10
gs.dresden@eulerhermes.com

40472 Düsseldorf
Kanzlerstraße 4
Tel. +49 (0) 2 11/9 65 76-0
Fax +49 (0) 2 11/9 65 76-99
gs.duesseldorf@eulerhermes.com

60311 Frankfurt
Große Gallusstraße 1–7
Tel. +49 (0) 69/13 48-0
Fax +49 (0) 69/13 48-1 70
nl.frankfurt@eulerhermes.com

79100 Freiburg
Rehlingstraße 6e
Tel. +49 (0) 7 61/4 00 79-0
Fax +49 (0) 7 61/4 00 79-50
gs.freiburg@eulerhermes.com

20251 Hamburg
Straßenbahnring 11
Tel. +49 (0) 40/2 36 36-0
Fax +49 (0) 40/2 36 36-1 66
nl.hamburg@eulerhermes.com

30159 Hannover
Georgstraße 36
Tel. +49 (0) 5 11/3 64 01-0
Fax +49 (0) 5 11/3 64 01-70
nl.hannover@eulerhermes.com

50672 Köln
Hohenzollernring 31–35
Tel. +49 (0) 2 21/9 20 60-0
Fax +49 (0) 2 21/9 20 60-1 59
nl.koeln@eulerhermes.com

04157 Leipzig
Landsberger Straße 23
Tel. +49 (0) 3 41/9 08 23-0
Fax +49 (0) 3 41/9 08 23-10
gs.leipzig@eulerhermes.com

68259 Mannheim
Hauptstraße 161
Tel. +49 (0) 6 21/1 29 05-0
Fax +49 (0) 6 21/1 29 05-99
gs.mannheim@eulerhermes.com

80339 München
Ridlerstraße 35
Tel. +49 (0) 89/5 43 09-0
Fax +49 (0) 89/5 43 09-1 66
nl.muenchen@eulerhermes.com

90429 Nürnberg
Spittlertorgaben 3
Tel. +49 (0) 9 11/2 44 05-0
Fax +49 (0) 9 11/2 44 05-30
gs.nuernberg@eulerhermes.com

66111 Saarbrücken
Bahnhofstraße 80
Tel. +49 (0) 6 81/3 89 96-0
Fax +49 (0) 6 81/3 89 96-99
gs.mannheim@eulerhermes.com

70597 Stuttgart
Löffelstraße 44
Tel. +49 (0) 7 11/9 00 49-0
Fax +49 (0) 7 11/9 00 49-70
nl.stuttgart@eulerhermes.com

Exportkreditgarantien des Bundes Büro Berlin

10117 Berlin
Friedrichstadt-Passagen
Quartier 205
Friedrichstraße 69
Tel. +49 (0) 30/20 94-53 10
Fax +49 (0) 30/20 94-53 30
aga-berlin@eulerhermes.com