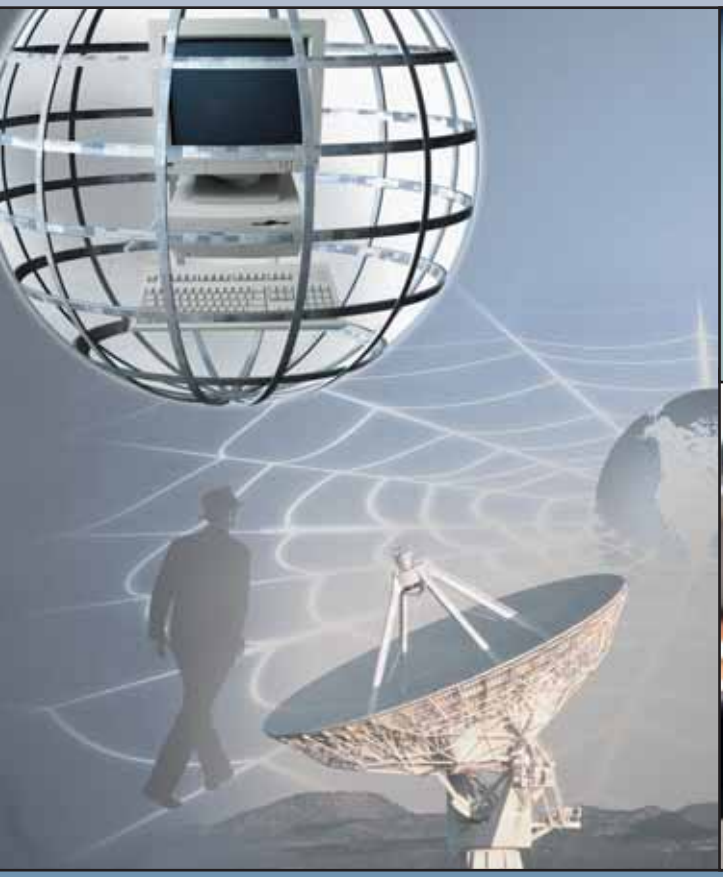
Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

SiFo-Studie 2009/10

Know-how-Schutz in Baden-Württemberg



Steinbeis-Edition

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet.

Impressum

Sicherheitsforum Baden-Württemberg (Hrsg.)
SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg

Die Studie wurde erstellt durch das Ferdinand-Steinbeis-Institut in Kooperation mit der School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin.

1. Auflage 2010, Steinbeis-Edition Stuttgart
ISBN 978-3-941417-20-5

Satz: Steinbeis-Edition
Titelbild: USB © photocase.com/idaho
Druck: RöslerDruck GmbH, Schorndorf

www.steinbeis-edition.de | 135750-2010-01

SiFo-Studie 2009/10

Know-how-Schutz in Baden-Württemberg

Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

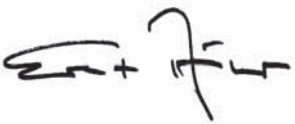
Vorwort

Mit der „SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg“ hat das Sicherheitsforum Baden-Württemberg seine Aktivitäten zum Schutz der heimischen Wirtschaft vor Wirtschaftsspionage und Konkurrenzausspähung um einen weiteren Baustein erweitert. Denn seit über zehn Jahren bietet das Sicherheitsforum besonders kleinen und mittleren Unternehmen Unterstützung beim Schutz ihres Wissens und ihrer Innovationen. Es hat eine Informationsplattform im Internet eingerichtet, gibt Info-Material heraus und wirkt an Veranstaltungen mit. Seit 2007 verleiht das Sicherheitsforum im zweijährigen Turnus den Sicherheitspreis Baden-Württemberg für herausragende Projekte der betrieblichen Sicherheit.

Das Sicherheitsforum hat sich im Jahr 1999 auf Initiative des Innenministers und des Wirtschaftsministers gegründet. Sie haben seither auch die Schirmherrschaft über das unabhängige Gremium aus Unternehmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden des Landes Baden-Württemberg übernommen. Alle haben erkannt, dass die Säulen unseres Wohlstands – die im Land ansässigen Unternehmen und Forschungseinrichtungen – durch mangelhaften Wissensschutz bzw. ungewollten Abfluss von Know-how gefährdet sind. Das Forum verfolgt keine geschäftlichen Interessen und ist politisch nicht gebunden.

Die im Auftrag des Sicherheitsforums vom Ferdinand-Steinbeis-Institut gemeinsam mit der School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin erarbeitete Studie leistet Grundlagenarbeit. Sie hat die Ermittlung statistischer Daten zur Industrie- und Wirtschaftsspionage, zu Urheberrechtsverletzungen und Wirtschaftskriminalität zum Gegenstand und untersucht die Auswirkungen auf die Unternehmen. Die Studie schafft damit die Voraussetzungen, um Defizite beim Wissensschutz der Unternehmen genauer zu erkennen und darauf abgestimmte Handlungsempfehlungen geben zu können. Sie ergänzt und aktualisiert zugleich die Ergebnisse einer vom Sicherheitsforum bereits im Jahr 2004 in Auftrag gegebenen Studie der Universität Lüneburg.

Die „SiFo-Studie 2009/10“ wird zu einem verbesserten Schutz unserer Unternehmen vor ungewolltem Abfluss von Know-how beitragen. Zu dieser verdienstvollen Arbeit gratulieren wir dem Sicherheitsforum und dem Ferdinand-Steinbeis-Institut sowie der School of Governance, Risk & Compliance Berlin. Wir wünschen dem Sicherheitsforum Baden-Württemberg weiterhin viel Erfolg bei seinen Bemühungen, die heimische Wirtschaft vor den Folgen von Wirtschaftsspionage und Konkurrenzausspähung zu schützen.



Heribert Rech MdL
Innenminister

Ernst Pfister MdL
Wirtschaftsminister

Inhaltsverzeichnis

1 Einführung

„Bei uns passiert so etwas nicht“ – so oder so ähnlich lauten die Antworten, wenn man Unternehmen nach Fällen von Know-how-Abfluss durch Wirtschaftsspionage oder Konkurrenzausspähung im eigenen Unternehmen fragt. Tatsächlich passiert so etwas – bei jedem?! Wenn etwas passiert, wissen es die Betroffenen dann, und wenn sie es wissen, reden sie darüber? Wenn man den entstandenen Schaden kennt, ist es zu spät!

Durch die hohe Dunkelziffer der Schadensfälle sind die Schäden in den Unternehmen nur sehr schwer abschätzbar. Es wäre fatal, das Problem aufgrund dieser unsicheren Quantifizierbarkeit zu vernachlässigen und das Risiko gar zu ignorieren, insbesondere bei der rasanten Zunahme der „Brainware“ in Wertschöpfungsprozessen und Produkten sowie Dienstleistungen.

Die Studie und die separat veröffentlichten Handlungsempfehlungen[1] sollen dazu beitragen, dass Unternehmen durch Sensibilisierung, Risikobewusstsein und geeignete Maßnahmen wissentlich sagen können: **„Wir haben alles Mögliche getan, damit bei uns so etwas nicht passiert!“**

Nicht nur die großen Unternehmen sind von Spionage- und Ausspähungsangriffen betroffen. Ziel sind oftmals gerade auch kleine und mittlere Unternehmen mit hoher technologischer Kompetenz, die nicht über geeignete Sicherungsvorkehrungen verfügen, um den Diebstahl und ungewollten Abfluss ihres Know-hows verhindern zu können.

Das Sicherheitsforum Baden-Württemberg als Zusammenschluss von Vertretern aus Unternehmen, Kammern, Verbänden, Forschungseinrichtungen und Behörden des Landes Baden-Württemberg nimmt sich seit zehn Jahren dieser wichtigen Problematik an, um vor allem kleine und mittlere Unternehmen beim Schutz ihres Wissens und ihrer technologischen Kompetenz zu unterstützen.

1 Die Handlungsempfehlungen sollen Unternehmen zusätzlich sensibilisieren und ihnen insbesondere helfen, Netzwerke zum Schutz vor Schäden zu bilden und ihre eigenen Präventivmaßnahmen zu optimieren. Sie sollen auch dazu beitragen, dass gerade kleine und mittlere Unternehmen ihre technologische Kompetenz auch weiterhin im immer stärker werdenden Wettbewerb sicher einsetzen können.

Bereits im Jahr 2004 hat das Sicherheitsforum erstmals eine Studie in Auftrag gegeben, die das Gefährdungspotenzial für Produktideen und Produktions-Know-how analysierte und damit Grundlagenarbeit leistete.

Ziel der aktuellen „SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg" war es, aktuelle Fallzahlen zur Industrie- und Wirtschaftsspionage in Baden-Württemberg zu ermitteln und zu untersuchen, welche Auswirkungen diese Ereignisse auf die betroffenen Unternehmen haben. Das Sicherheitsforum Baden-Württemberg hat das Ferdinand-Steinbeis-Institut und die School of Governance, Risk & Compliance an der Steinbeis-Hochschule Berlin mit der Erarbeitung, Durchführung und Auswertung der Studie beauftragt. Die beiden Institute wurden dabei vom Baden-Württembergischen Industrie- und Handelskammertag, der Steinbeis-Stiftung sowie dem Sicherheitsforum selbst unterstützt.

Von den über 4.000 befragten baden-württembergischen Unternehmen flossen die Angaben von 239 Unternehmen in die Studie ein. Im Folgenden werden diese, wenn nicht anders erwähnt, als „Unternehmen" bezeichnet. In Bezug auf die Branchen stellt diese Studie ein repräsentatives Bild der Bedrohungslage für Unternehmen in Baden-Württemberg dar. Damit ist die „SiFo-Studie 2009/10" eine der größten empirischen Untersuchungen zum Thema Know-how-Schutz in Deutschland. Das Besondere an dieser Studie stellt die Auswertung von Einzelschadensfällen dar, die konkrete Einblicke in die individuelle Schadenshöhe und das Täterverhalten geben.

Drei zentrale Ergebnisse der Studie „Know-how-Schutz in Baden-Württemberg":

- Spionage und ungewollter Know-how-Abfluss in Unternehmen sind realistische Bedrohungen/Risiken, die noch immer unterschätzt werden.
- Nicht technische Angriffe und Außenstehende, wie weithin vermutet, sondern Unternehmensangehörige sind es hauptsächlich, welche die Unternehmen durch Know-how-Verrat schädigen.
- Die Unternehmen könnten (und müssten) selbst mehr tun, um ihr Know-how zu schützen.

Der Verrat von Know-how wird typischerweise von unternehmensnahen Tätern begangen. Dennoch schätzen die Unternehmen ihr Risiko, dass ihre Geschäfts- und Betriebsgeheimnisse ausgespäht oder verraten werden, durch technische Angriffe (24 %) weitaus höher ein als durch Unternehmensangehörige (9 %) oder externe Personen/Unternehmen (8 %). Fast zwei Drittel (64 %) halten es sogar für unwahrscheinlich, dass Unternehmensangehörige betroffen sein könnten. Dies ist eine folgenschwere Fehleinschätzung, wie die Studie belegt.

Über 70 % der Täter kommen laut der „SiFo-Studie 2009/10" aus den Reihen des geschädigten Unternehmens. Das Durchschnittsalter eines Haupttäters beträgt 41 Jahre. Er gehört dem Unternehmen etwa seit zehn Jahren an. Bei externen Tätern bestand im Durchschnitt seit sechs Jahren eine Geschäftsverbindung. Dieses Profil gilt ebenso für Fälle mit Verstößen gegen das Urheberrecht als auch mit Verrat oder Ausspähen von Geschäfts- und Betriebsgeheimnissen.

Die Ergebnisse der Studie zeigen, dass knapp 38 % der Unternehmen in den letzten vier Jahren Urheberrechtsverletzungen ausgesetzt waren und 18 % durch den Verrat von Geschäfts- und Betriebsgeheimnissen Schäden erlitten. Produkt- und Markenpiraterie traf vor allem Unternehmen, die eine intensive Forschung und Entwicklungsarbeit betreiben. Fast zwei Drittel dieser Unternehmen (65 %) hatten hierdurch mindestens einen Schadensfall in den letzten vier Jahren.

Etwa 40 % der betroffenen Unternehmen hatten aufgrund von Urheberrechtsverletzungen mit gravierenden Umsatzeinbußen (37 %), Beeinträchtigungen von Geschäftsbeziehungen (40 %) oder strategischen Vorteilen für Wettbewerber (44 %) zu kämpfen. Die finanziellen Schäden aus Urheberrechtsverletzungen können erheblich sein. So dokumentieren Unternehmen ihre erlittenen Schäden zwischen unter 10.000 bis über zwei Millionen Euro je Vorfall. Die mit Abstand höchsten Schäden erlitten forschungsintensive Unternehmen: im Durchschnitt über eine halbe Million Euro (540.000 Euro), bei 23 % lagen die Schäden deutlich oberhalb dieses Mittelwerts.

Unternehmen könnten sich teilweise aus eigener Kraft präventiv besser schützen. Nur jedes zweite der befragten Unternehmen stellt sicher, dass sensibles Wissen nur relevanten Mitarbeitern bekannt ist. Genauso wenige Unternehmen nutzen ethische Richtlinien oder Verhaltenskodizes, um mangelndem Wertebewusstsein entgegenzuwirken und den Mitarbeitern den Umgang mit sensiblen Informationen zu verdeutlichen. Betroffene Unternehmen decken in der Regel die Vorfälle nicht durch ihre Sicherheits- und Kontrolleinrichtungen auf. Die Entdeckung der meisten Fälle (73 %) erfolgte durch Hinweise von internen (42 %) oder externen (31 %) Tippgebern.

Die nachfolgende Dokumentation ist wie folgt aufgebaut:

- In einem ersten Teil wird, insbesondere für die Zielgruppe, die noch über kein tieferes Fachwissen verfügt, auf die **theoretischen Grundlagen** der Studie mit den Schwerpunkten Urheberrechtsverletzungen, Verrat von Geschäfts- und Betriebsgeheimnissen sowie Wirtschaftskriminalität eingegangen. **(S. 17–34)**
- Nach einer kurzen Erläuterung zur Bedeutung des Problembereichs für Unternehmen wird das **Studiendesign** vorgestellt. **(S. 35–38)**
- Anschließend folgen die **ausführlichen Ergebnisse der Studie**, in der Reihenfolge Urheberrechtsverletzungen, Verrat von Geschäfts- und Betriebsgeheimnissen, Wirtschaftskriminalität, Täterprofile, mittelfristige Risikoeinschätzung sowie Beratungsangebote. **(S. 39–86)**
- Eine **Zusammenfassung** finden Sie am Ende mit anschließendem **Glossar**. **(S. 87–92)**

Im Januar 2010

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

2 Theoretische Grundlagen der Studie

Auf welche Art und Weise unternehmensinterne, vertrauliche Informationen an Wettbewerber oder die Öffentlichkeit gelangen, erfährt man aus den Medien selten. Die Tatsache, dass geheime und vertrauliche Unterlagen oder Daten das Unternehmen unerlaubt verlassen haben, wird kurzerhand einer wirtschaftskriminellen Handlung zugeordnet. Die folgenden theoretischen Grundlagen sollen Abgrenzungen zwischen den Begrifflichkeiten ermöglichen, um strafrechtlich relevantes Handeln mit unterschiedlichen Täterstrukturen zu unterscheiden. Die Methoden der Informationsbeschaffung werden unter dem Blickwinkel der relevanten Unternehmensrisiken betrachtet.

2.1 Urheberrechtsverletzungen

Terminologie Urheberrechte

Unter *Urheberrecht* oder gewerblichem Rechtsschutz werden die Normen zusammengefasst, die Erfindungen, Kennzeichen und Werke der Literatur, Wissenschaft und Kunst schützen. Die wichtigsten gewerblichen Schutzrechte sind:

- Patente,
- Gebrauchsmuster,
- Geschmacksmuster (Design) und
- Marken.

Werden gewerbliche Schutzrechte verletzt, um Gewinn zu erzielen, spricht man häufig von Produkt- oder Markenpiraterie. Hierbei werden Produkte imitiert, wobei sich das Imitieren vor allem auf den Namen, bestimmte Markenzeichen oder Symbole sowie auf das Design des Produkts und der Verpackung bezieht.

Patent

Als *Patent* definiert der Gesetzgeber im Patentgesetz (PatG) ein zeitlich begrenztes Schutzrecht für die alleinige wirtschaftliche Nutzung einer technischen Erfindung. Die Erfindung muss neu sein, d. h. nicht zum Stand der Technik gehören und auf einer erfinderischen Tätigkeit beruhen. Man unterscheidet zwischen Erzeugnispa-

tenten (z. B. auf Maschinen, Vorrichtungen, Stoffe) und Verfahrenspatenten, d. h. auf die zeitliche Reihenfolge von Abläufen.

Gebrauchsmuster

Das *Gebrauchsmuster* ist ein dem Patent sehr ähnliches gewerbliches Schutzrecht für kleinere technische Erfindungen. Es soll einen wirtschaftlichen Anreiz bieten, an Gegenständen des täglichen Lebens durch kleinere Erfindungen, also technische Ideen mit geringerem Fortschritt oder geringerer Erfindungshöhe, Verbesserungen vorzunehmen. Es wird deshalb auch als „kleines Patent" bezeichnet. Auch Gebrauchsmuster müssen neu und gewerblich anwendbar sein. Der Schutz von Gebrauchsmustern ist im Gebrauchsmustergesetz (GebrMG) geregelt.

Geschmacksmuster

Während Patente und Gebrauchsmuster technische Erfindungen schützen, befasst sich das *Geschmacksmuster* mit der äußeren, wahrnehmbaren ästhetischen Form eines Gegenstandes. Es handelt sich um eine Form des Designschutzes, der seine Bedeutung dadurch gewinnt, dass das Produktdesign für eine Kaufentscheidung eine immer größere Rolle spielt. Durch das Geschmacksmustergesetz (GeschmMG) werden Muster geschützt, die neu sind und eine Eigenart haben, d. h. sich von dem Gesamteindruck anderer Erzeugnisse unterscheiden. Hierzu zählen:

- zwei- oder dreidimensionale Erscheinungen, die sich durch Linie, Konturen, Farbe, Gestalt, Oberflächenstruktur oder Werkstoff auszeichnen,
- industrielle oder handwerkliche Erzeugnisse, einschließlich Verpackung, Ausstattung, grafische Symbole und typografische Schriftzeichen, und
- komplexe Erzeugnisse, d. h. Erzeugnisse aus mehreren Bauelementen, wie z. B. Fahrzeuge.

Marken

Marken sind Kennzeichen, die im Geschäftsverkehr zur Unterscheidung von Waren und Dienstleistungen eines Unternehmens von denen anderer verwendet werden und durch das Markengesetz (MarkenG) geschützt sind. Es wird zwischen Wort-, Bild-, Farb-, Hör-, Geruchs-, Geschmacks-, Tastmarken sowie dreidimensionalen, eingetragenen und notorisch bekannten Marken unterschieden.

Täterprofil Urheberrechtsverletzungen
Die Täter von Produkt- oder Markenpiraterie kommen häufig aus Asien, aber auch in vielen Ländern in Europa, z. B. in Tschechien, in der Türkei und in Georgien, werden Produktfälschungen hergestellt. Hierbei kann es sich um unternehmensexterne Täter handeln, die sich die Produktinformationen auf Messen, Konferenzen oder Werksbegehungen aneignen, oder um interne Täter mit direktem oder indirektem Zugang zu Produktinformationen.

Schutz vor Urheberrechtsverletzungen
Unternehmen schützen sich vor Produkt- und Markenpiraterie selbst in Form von eigenen Werkschutz- oder Sicherheitsabteilungen. Diese Abteilungen beschäftigen sich mit dem Schutz des immateriellen Unternehmensbesitzes, z. B. Patente, Lizenzen, Know-how im Allgemeinen, und des materiellen Unternehmensbesitzes, z. B. Gebäude, Betriebseinrichtungen, Produkte etc. Des Weiteren spielen die hauseigenen Rechtsabteilungen oder externe Dienstleister eine entscheidende Rolle beim Schutz der unternehmenseigenen Urheberrechte, da sie häufig die Eintragung und Überwachung der Rechte vornehmen oder darauf aus unterschiedlichen Gründen verzichten. Zudem unterstützen verschiedene Interessensverbände, Universitäten, höhere Bildungseinrichtungen oder auch Behörden Unternehmen bei ihren Bemühungen um Schutz ihrer Urheberrechte.

2.2 Verrat von Geschäfts- und Betriebsgeheimnissen

Terminologie Geschäfts- und Betriebsgeheimnis
Als *Geschäfts- und Betriebsgeheimnis* bezeichnet das Bundesverfassungsgericht in seinem Urteil vom 14. März 2006: „[...] alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge [...], die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Betriebsgeheimnisse umfassen im Wesentlichen technisches Wissen im weitesten Sinne; Geschäftsgeheimnisse betreffen vornehmlich kaufmännisches Wissen. Zu derartigen Geheimnissen werden etwa Umsätze, Ertragslagen, Geschäftsbücher, Kundenlisten, Bezugsquellen, Konditionen, Marktstrategien, Unterlagen zur Kreditwürdigkeit, Kalkulationsunterlagen,

Patentanmeldungen und sonstige Entwicklungs- und Forschungsprojekte gezählt, durch welche die wirtschaftlichen Verhältnisse eines Betriebs maßgeblich bestimmt werden können."[2]

Terminologie Wirtschaftsspionage

Unter *Wirtschaftsspionage* wird die staatlich gelenkte oder gestützte Ausforschung von Wirtschaftsunternehmen und Betrieben verstanden, die von Nachrichtendiensten fremder Staaten durchgeführt wird[3]. Die Schwerpunkte nachrichtendienstlicher Beschaffungsaktivitäten orientieren sich an aktuellen politischen Vorgaben oder volkswirtschaftlichen Prioritäten der jeweiligen Staaten. Die Aufklärungsziele ausländischer Dienste sind die Informationsbeschaffung aus den Bereichen Wirtschaft, Wissenschaft und Forschung, aber auch Politik und Militär.

Zweck der Wirtschaftsspionage ist es, die Wirtschaftskraft bzw. das wirtschaftliche Potenzial der eigenen Volkswirtschaft zu verbessern. Technisch und wirtschaftlich hoch entwickelte Staaten verfolgen mit der Wirtschaftsspionage das Ziel, die technologische Führerschaft und die ökonomische Spitzenposition zu erreichen und zu sichern.

Staaten mit niedrigem technologischen Stand versuchen eher, vordergründig ihre Volkswirtschaft zu optimieren, indem sie sich technisches Know-how beschaffen und dadurch Kosten für eigene Entwicklungen und Lizenzgebühren sparen. Sie beschaffen sich Informationen über Fertigungstechniken, um auf dem Markt mit kostengünstiger gefertigten Nachbauten wettbewerbsfähig zu sein. Täter der Wirtschaftsspionage planen und handeln langfristig und achten auf ihre Tarnung.

Schwerpunkte der Informationsbeschaffung in den Unternehmen selbst sind zukunftssichernde und strategisch bedeutsame Hoch- und Querschnittstechnologien, und zwar nicht nur solche mit direktem militärischen Bezug.

2 BVerfG, 1 BvR 2087/03 vom 14. März 2006, http://www.bverfg.de/entscheidungen/rs20060314_1bvr208703.html, 22.01.2010.

3 Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden in Bund und Ländern: Wirtschaftsspionage – Risiko für Ihr Unternehmen, Vereinigte Verlagsanstalten, Düsseldorf, 2008.

Schutz vor Wirtschaftsspionage

Für die Abwehr von *Wirtschaftsspionage* sind vor allem staatliche Organisationen zuständig, wobei natürlich jede Einrichtung oder jedes Unternehmen sich durch Schutzmaßnahmen im eigenen Haus vor Angriffen nachrichtendienstlich geführter Spionage schützen kann. Wie im Bundesverfassungsschutzgesetz festgelegt, obliegt den Verfassungsschutzbehörden die Abwehr von „geheimdienstlichen Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht“[4]. Verfassungsschutzbehörden sind das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz. Darüber hinaus ist in diesem Bereich auch der Militärische Abschirmdienst (MAD) tätig. Den Polizeibehörden und Staatsanwaltschaften obliegt es, konkrete Gefahren abzuwehren und begangene Straftaten zu verfolgen.

Terminologie Industriespionage

Mittels *Industriespionage* werden Unternehmen durch Wettbewerber ausgeforscht. Daher wird bei der Industriespionage auch oft von Konkurrenzausspähung, Wettbewerbsspionage oder Konkurrenzspionage gesprochen. Die ausforschenden Unternehmen haben verstärktes Interesse an:

- Informationen über den Wettbewerb, Märkte, Technologien und Kunden,
- aktuellem Know-how zu Produktentwicklungen und Produktionstechniken,
- Preisinformationen,
- Kalkulationen,
- Designstudien.

Wie bei der Wirtschaftsspionage ist auch bei der Industriespionage eine Unterscheidung nach dem Grad der Entwicklung des spionierenden Unternehmens zu treffen. Die hoch entwickelten Unternehmen – meist auch aus technologisch hoch entwickelten Ländern – spionieren primär, um mit ihren Wettbewerbern auf dem gleichen Wissensstand zu bleiben. Technologisch weniger entwickelte Unternehmen sind eher an Basistechnologien oder an Wissen zum Nachbau, z. B. von Plagiaten, interessiert. Bei der Industriespionage sind die Aktionen eher impulsiv und kurzfristig, da die kurzen Produktlebenszyklen den Innovationsrhythmus und somit den Wettbewerb beeinflussen.

4 Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 6 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586) geändert worden ist.

Täterprofil Industriespionage

Bei der Industriespionage gehören zu den Tätern vor allem mit guten Zugängen ausgestattete Unternehmensangehörige, die entweder aus eigener Motivation zum Täter werden, durch Außenstehende angeworben oder durch Social Engineering manipuliert werden. Aber auch Mitarbeiter von unternehmensbezogenen Dienstleistern können zu Tätern werden und/oder solche einschleusen.

Eine weitere Gruppe von Tätern bilden die sogenannten *Intelligence Trader*, d. h. Unternehmen, die sich als Informationshändler, „Sicherheitsberater" oder „Detekteien" bezeichnen. Sie werden entweder von Unternehmen beauftragt, Informationen auf dem illegalen Weg zu beschaffen, oder sie beschaffen sich Informationen aus eigener Motivation und bieten sie dann den konkurrierenden Unternehmen an. Neben diesen Leistungen bieten die gleichen Unternehmen auch noch z. B. legale Sicherheitsberatungen, Implementierungen von Sicherheitskonzepten, aber auch die Beschaffung von Informationen mit Hilfe eigener bzw. freier Mitarbeiter an, die ebenfalls aus dem Nachrichtendienst kommen und über spezielle Kenntnisse und Fähigkeiten, wie z. B. Abhörtechniken, verfügen.

Durch die zunehmende Bedeutung von Informations- und Kommunikationstechnologien bei der Informationsbeschaffung hat sich eine weitere Gruppe von Tätern, die *Information Technology Experts*, in den letzten Jahren etabliert. Diese Täter sind beispielsweise versierte Computer-Hacker bzw. arbeiten mit solchen zusammen und beschaffen Informationen aus fremden Systemen. Die dabei eingesetzten Methoden sind analog zu den heute vorhandenen Informationssystemen weit gefächert.

Schutz vor Industriespionage

Den Tätern gegenüber stehen Personen, Einrichtungen und Unternehmen, die sich mit der Abwehr von Konkurrenzspionage beschäftigen. Die staatlichen Organisationen mit Abwehraufgaben sind in Deutschland die Polizeibehörden, insbesondere das Bundeskriminalamt und die Landeskriminalämter.

Wie gegen die Wirtschaftsspionage schützen sich die Unternehmen darüber hinaus auch gegen die Industriespionage, z. B. durch eigene Werkschutz- oder Sicherheitsabteilungen. Je nach Größe des Unternehmens und nach Branche differieren

Organisation und Ausstattung der Abteilungen stark. Unternehmen, die aus Kosten- und/oder Effizienzgründen keine eigene Sicherheitsabteilung haben, nutzen externe Dienstleister, die teilweise oder ganz Sicherheitsaufgaben übernehmen.

Des Weiteren werden Unternehmen im Bedarfsfall auch hier von einschlägigen Verbänden und Interessengemeinschaften unterstützt. Hierzu gehören beispielsweise das Sicherheitsforum Baden-Württemberg (SiFo BW), die Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V. (ASW) und die regionalen Sicherheitsverbände wie z. B. der Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V. (VSW). Sie beraten Unternehmen und interessierte Dritte zur Sicherheit in der Wirtschaft und stellen darüber hinaus eine Schnittstelle zwischen Politik, Wirtschaft, Verbänden und der Wissenschaft dar.

Ferner nutzen Unternehmen auch das Know-how von Universitäten und höheren Bildungseinrichtungen. Neben Netzwerken und Forschungsprojekten – wie z. B. die Durchführung dieser oder weiterer themeneinschlägiger Studien – bieten sie Seminare, Schulungen, Trainings und umfassende Ausbildungen an.

Strafbarkeit

Einen strafrechtlichen Schutz gegen Wirtschafts- und Industriespionage geben die Straftatbestände des Abschnitts „Landesverrat und Gefährdung der äußeren Sicherheit“ des Strafgesetzbuches, insbesondere § 94 StGB (Landesverrat) und § 99 StGB (Geheimdienstliche Agententätigkeit). Der Verrat von Geschäfts- und Betriebsgeheimnissen sowie von Vorlagen oder von Vorschriften technischer Art und ihre unbefugte Verwertung durch Dritte sind auch nach den Straftatbeständen der §§ 17 bis 19 des Gesetzes gegen den unlauteren Wettbewerb (UWG) mit Strafe bedroht.

2.3 Wirtschaftskriminalität

Terminologie Wirtschaftskriminalität

Die Wirtschaftskriminalität ist ein komplexes Gebiet, da es sich nicht um einzelne feststehende Straftaten handelt, sondern um alle Straftaten, die einen wirtschaftlichen Bezug aufweisen. Überwiegend sind diese im Strafgesetzbuch (StGB) geregelt. Privatpersonen, ein Unternehmen oder die Allgemeinheit können Opfer der Tat sein.

Die vorliegende Studie beschränkt sich auf die folgenden Delikte:

- Korruption,
- Betrug,
- Untreue und
- Unterschlagung.

Terminologie Korruption

Kennzeichnend für *korrupte Praktiken* sind vor allem der Missbrauch einer Funktion und das Erlangen bzw. Anstreben von (persönlichen) Vorteilen unter gleichzeitiger Verschleierung dieser Handlungsweisen. Als klassische Korruptionsdelikte gelten:

- Vorteilsnahme (§ 331 StGB) und Vorteilsgewährung (§ 333 StGB),
- Bestechung (§ 334 StGB) und Bestechlichkeit (§ 332 StGB),
- Bestechlichkeit und Bestechung im geschäftlichen Verkehr (§ 299 StGB).

Terminologie Betrug, Untreue und Unterschlagung

Die Tatbestände des Wirtschaftsstrafrechts *Betrug* (§ 263 StGB) und *Untreue* (§ 266 StGB) setzen einen Vermögensschaden oder zumindest eine Vermögensgefährdung voraus. Die *Unterschlagung* (§ 246 StGB) setzt nicht unbedingt einen Vermögensschaden voraus. Es wird bestraft, wenn sich jemand eine fremde bewegliche Sache rechtswidrig aneignet.

Täterprofil Wirtschaftskriminalität
Als Täter kommen bei wirtschaftskriminellen Handlungen sowohl Unternehmensangehörige als auch Externe in Frage. Oft ist sogar ein kollusives Zusammenwirken beider Akteure für den Erfolg der Tat entscheidend.

Unterschieden wird zwischen unbewusst und passiv agierenden (Innen-)Tätern und bewusst und aktiv agierenden Tätern. Der unbewusst und passiv agierende Täter befindet sich anfänglich häufig in einer „Opferrolle". Durch das bekannte „Anfüttern" gelangt er in eine solche Situation bzw. wird in diese gedrängt. Dieser spätere interne Täter (z. B. der Angestellte eines Auftraggebers) wird in der Regel von Dritten (meist externen Tätern, die an dem internen Mitarbeiter zur Umsetzung ihrer geplanten Taten interessiert sind) mit Vergünstigungen versorgt, die anfangs geringwertig sein können, in ihrer Stetigkeit oder wachsenden Wertigkeit jedoch zu einer Form der Abhängigkeit führen können.

Der aktiv und bewusst vorgehende Täter bedarf keiner „Anfütterungsanreize", er ist meist planvoll und strukturiert. Er analysiert die im Unternehmen bestehenden oder fehlenden Kontrollmechanismen und richtet sein Tun danach aus, möglichst lange an den erlangten Vorteilen zu partizipieren. Bei betrügerischen Handlungen agieren diese Täter oft allein, bei korrupten Handlungen überwiegend mit ihnen kriminell vertrauten Partnern.

2.4 Risiken aus Know-how-Abfluss für Unternehmen

Bei der Informationsbeschaffung ist nicht nur das fertige Produkt für den Spion von Interesse, sondern alle Unternehmensbereiche und -angehörige mit ihrem Know-how können für ihn zum Zielobjekt werden.

Das Landesamt für Verfassungsschutz Baden-Württemberg und das Bayerische Landesamt für Verfassungsschutz führen die ausspähungsgefährdeten Unternehmensbereiche mit ihren Funktionsträgern und die möglichen Informationsarten auf (siehe Tab. 1, S. 26).

Der Verrat von Geschäftsgeheimnissen kann ebenso auf allen Hierarchiestufen erfolgen. Wird das Know-how durch Personen verraten, die Zugang zu sensiblen Informationen haben, wie beispielsweise Fach- und Führungskräfte, kann dies zu einem hohen Schaden mit drastischen Folgen führen.

Organisationseinheiten	Ausspähungsinhalte	Gefährdete Funktionsträger/ Bereiche
Aufsichtsorgane	strategische/taktische Entscheidungen	Gesellschafter, Beirat, Aufsichtsrat
Unternehmensleitung	strategische/taktische Entscheidungen	Geschäftsführer, Vorstand, Sekretariat, Controller, Revisoren
Verwaltung, Personalabteilung, Betriebsrat	personenbezogene Daten, strategische Entscheidungen	Telefonzentrale, Arbeitnehmervertretung/ Wirtschaftsausschuss
Forschung, Entwicklung	Produktideen/-strategien, Designstudien	Projektleiter, Laborant
Produktion	Produktideen, Konstruktionsunterlagen, Herstellungsverfahren, Qualitätsprüfungsdaten, Steuerungssysteme	Verfahrenstechniker, Qualitätsprüfer, Monteure, Werkstoffprüfer
Einkauf, Verkauf	Lieferantendaten, Kundendaten, Marketingstudien, Marketingstrategien	Einkaufsleiter, Vertriebsleiter
Finanzwesen	Kalkulationsunterlagen, Budgetplanungen, Investitionsvorhaben	Sachbearbeiter
Datenverarbeitung	zentraler Zugriff auf alle Datenbestände	Operator, Programmierer, Wartungstechniker, Systemadministrator

Tabelle 1: Von Ausspähung gefährdete Unternehmensbereiche[5]

Wirtschaftskriminelle Handlungen sind in der Regel ebenfalls in allen Hierarchiestufen anzutreffen. Zu bedenken ist jedoch, dass die Schadenseinschläge in den oberen Hierarchiestufen bedeutend größer sind (auch Management-Fraud genannt) und die Täter hier bereits eine langjährige Unternehmenszugehörigkeit aufweisen. Es bleibt dabei zunächst unberücksichtigt, ob die Taten anfangs im Glauben geschehen, dass sie zu Gunsten des Unternehmens erfolgen (Bestechung für einen Auftrag) oder zu dessen Schaden (Untreue, Betrug, Unterschlagung, Bestechlichkeit).

5 Wirtschaftsspionage in Baden-Württemberg und Bayern – Daten Fakten Hintergründe, Hrsg.: Landesamt für Verfassungsschutz Baden-Württemberg und Bayerisches Landesamt für Verfassungsschutz, Stand Oktober 2006, http://www.verfassungsschutz.bayern.de/imperia/md/content/lfv_internet/service/wirtschaftsspionage_bay_bw_2006.pdf, 22.01.2010.

2.5 Methoden zur Informationsbeschaffung

Konzepte im Bereich der Unternehmenssicherheit sind überwiegend technisch orientiert und daraus folgend auch für die Abwehr technischer An- und Übergriffe geeignet. Geringeres Augenmerk wird jedoch auf Know-how-Verluste durch menschliche Fehler, durch Manipulationen oder Repression gelegt, was für Unternehmen gravierende Folgen haben kann.

Da schutzwürdiges Know-how auf unterschiedlichen Wegen das Unternehmen verlassen kann, werden nachfolgend die wichtigsten Methoden und Mittel für diese Informationsbeschaffung vorgestellt. Erwartungsgemäß sind die wenigsten dieser Methoden legal.

OSINT

Durch öffentlich zugängliche Quellen, d. h. gedruckte oder digitale Medien wie z. B. Radio, Fernsehen, Zeitungen, Zeitschriften, Internet, kommerzielle Datenbanken, Filme und Zeichnungen, können Informationen auf dem legalen Weg beschafft werden (Open Source INTelligence). Diese Informationen werden von Unternehmen bewusst und unbewusst zur Verfügung gestellt. Hinzu kommt der Besuch von öffentlichen Veranstaltungen, wie z. B. Messen, Kongresse, Symposien etc., um durch reine Beobachtung, aber auch durch das Abschöpfen von Informationen in einem Gespräch, Auskünfte über das Unternehmen und seine Strategien zu erhalten. Ebenso können durch die rege Teilnahme am Wirtschaftsleben Informationen (hinzu)gewonnen werden. Fusionieren Wettbewerber oder gründen sie Gemeinschaftsunternehmen, ist es beiden Partnern möglich, Zugriff auf Unternehmensgeheimnisse zu bekommen.

HUMINT

HUMINT (HUMan INTelligence) ist die Beschaffung von Informationen durch Einsatz oder Abschöpfung menschlicher Quellen und zählt zu den bedeutendsten Methoden. Dieser Bereich kann sowohl konspirativ (d. h. verdeckt und nach außen gerichtet) als auch rezeptiv (d. h. offen) ausgeführt werden.

Bei der rezeptiven Durchführung trifft man im Bereich der Wirtschaftsspionage auf die „klassischen“ Agenten. Meist wird sowohl bei der Industriespionage als auch bei

der Wirtschaftsspionage auf das Konzept der sogenannten „Quellen im Objekt“, z. B. eingeschleuste Mitarbeiter etc., zurückgegriffen. Dabei unterscheidet man zwischen dem entsandten Agenten, der meist in das Unternehmen eingeschleust wird, und der angeworbenen Quelle im Objekt.

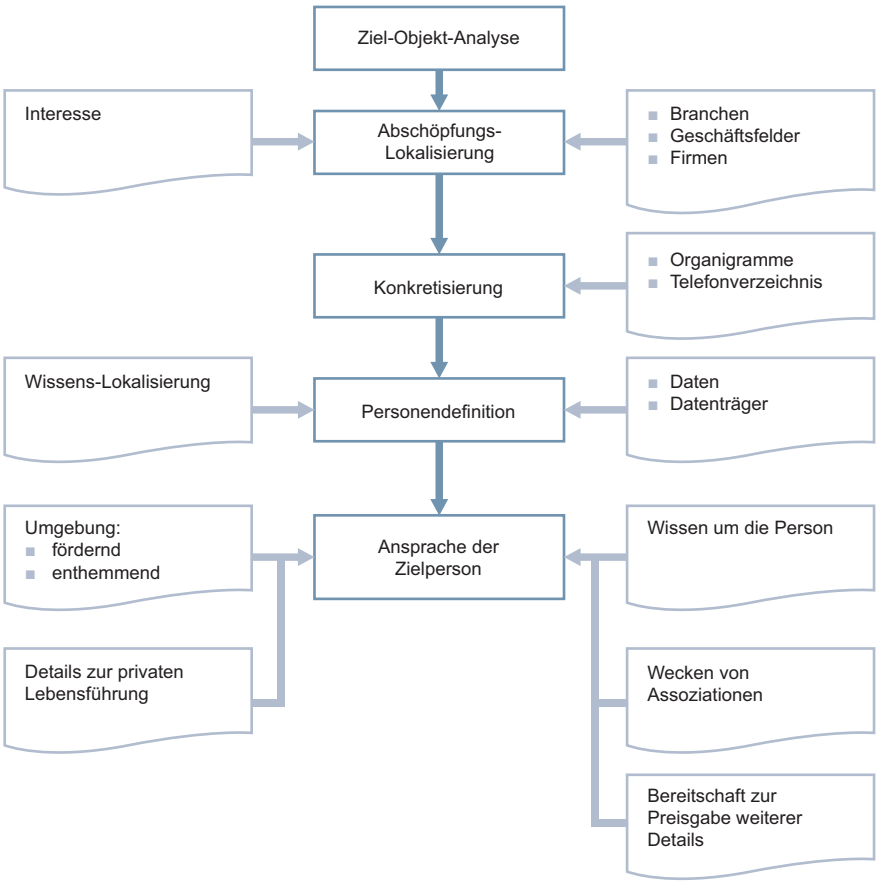


Abbildung 1: Vorbereitung von Abschöpfungsmaßnahmen[6]

6 Dreger, Wolfgang: Counter Intelligence. Betriebliche Spionageabwehr, Expert-Verlag, Renningen, 1998.

Bei der angeworbenen Quelle im Objekt findet eine weitere Differenzierung in fremdmotivierte Täter und sogenannte Eigenanbieter statt. Bei fremdmotivierten Tätern werden durch aggressive Methoden, z. B. Bedrohung oder Erpressung, Mitarbeiter zum Handeln gezwungen. Der Beginn dieser besonderen Form des „Aushorchens“ oder „Abschöpfens“ kann relativ harmlos sein. Das als Social Engineering bezeichnete Vorgehen ist eine Methode, um durch das Ausnutzen menschlicher Eigenschaften unberechtigten Zugang zu Informationen und informationstechnischen Systemen zu erlangen. Diese Eigenschaften können beispielsweise Hilfsbereitschaft, Vertrauen, Angst, Respekt und Autorität sein. Meistens werden Mitarbeiter des auszuspähenden Unternehmens manipuliert, um unzulässige Handlungen durchzuführen, die zu einer Informationsweitergabe an das ausspähende Unternehmen führen. Die systematische Planung von Abschöpfungsmaßnahmen zeigt Abb. 1.

Bei eigen- und fremdmotivierten Tätern können als Grund für die Informationsweitergabe an ein Konkurrenzunternehmen auch materielle Anreize stehen. Jeder Mitarbeiter in einem Unternehmen kann entsprechend seinen Bedürfnissen Unzufriedenheit in Bezug auf seine Bezahlung oder Wertschätzung[7] empfinden und somit potenziell von einem Konkurrenten abgeworben werden bzw. zu einem Insider werden. Neben den finanziellen Aspekten spielen beim Verrat auch der Arbeitsinhalt, das Arbeitsumfeld, die organisationalen Rahmenbedingungen und das soziale Umfeld im Unternehmen eine Rolle[8]. Andere Gründe, z. B. ideologische Überzeugungen und persönliche Bindungen („Verrat aus Zuneigung“), treten seltener auf und werden oft auch als Entlastungsgründe beim Aufdecken einer Tat angebracht.

7 Vergleiche hierzu auch die Bedürfnis-Hierarchie von Maslow, welche die grundlegenden Motive menschlichen Handelns in Form einer Pyramide aufzeigt: physiologische Bedürfnisse, Sicherheitsbedürfnisse, soziale Bedürfnisse, Achtung und Wertschätzung sowie auf der höchsten Stufe Selbstverwirklichung.

8 Meissinger, Jan: Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland, in Schriftenreihe innovative betriebswirtschaftliche Forschung und Praxis, Bd. 175, Verlag Dr. Kovač, Hamburg, 2005.

TECHINT

Werden Informationen mit Hilfe von technischer Ausrüstung bzw. Methoden beschafft, werden sie als TECHINT (TECHnical INTelligence) bezeichnet. Da im TECHINT-Bereich fast immer rezeptive Methoden angewandt werden, bemerkt das Zielobjekt diese – im Gegensatz zur direkten und aktiven Informationsgewinnung durch Personen – nur schwer. In vielen Fällen werden HUMINT und TECHINT kombiniert, da aufgrund von technischen Rahmenbedingungen und organisatorischen Voraussetzungen die technische Ausrüstung mit Hilfe von menschlichen Agenten in eine günstige Position gebracht werden muss, um damit auch erfolgreich zu sein.

Eine der wichtigsten Möglichkeiten der Informationsbeschaffung in diesem Bereich stellt das Abfangen von elektronischen Kommunikationssignalen oder anderen Signalen dar. Durch den immer stärkeren Einsatz von Technik, insbesondere Telekommunikation und Internet in den Unternehmen, ergeben sich immer mehr Angriffsmöglichkeiten für das schädigende Unternehmen oder den Nachrichtendienst. Bei Telekommunikationsanlagen kommt es dabei besonders häufig:

- zum Aufschalten auf bestehende Verbindungen durch Dritte,
- zu Konferenzschaltungen, d. h. der unbemerkte Aufbau einer weiteren Verbindung im Hintergrund,
- zum automatisierten Rückruf,
- zum Abhören von Raumgesprächen durch Freisprecheinrichtungen oder Lauthören.

Auch drahtlose Verbindungen, wie z. B. WLAN-Technologie, Bluetooth-Schnittstellen, DECT-Standard, Funktastaturen und -mäuse und GSM-Technologien, können dazu verwendet werden, unbemerkt an Informationen zu gelangen. Hierbei sind besonders mobile IuK-Endgeräte wie z. B. Laptops, Mobiltelefone, Smartphones, PDAs und USB-Sticks, gefährdet. Die genannten Technologien können sowohl das Zielobjekt von Angriffen sein als auch selbst zum Entwenden von Informationen genutzt werden.

Lauschangriffe klassischer Art auf Büros stellen nach wie vor ein Sicherheitsrisiko dar. Zum Einsatz kommen Abhörgeräte, sogenannte „Wanzen“, akustische (Richt- und Körperschallmikrofone, als Mikrofone manipulierte Lautsprecher) sowie optische (Laser-Abhörsysteme, Infrarotsender und -empfänger) Lauschmittel.

Nach Schätzungen sind bei annähernd 70 % bis 80 % der IT-Angriffe Innentäter, meist illoyale aktive Beschäftigte und ehemalige Mitarbeiter, beteiligt.[9] Die Täter besitzen Kenntnisse über innerbetriebliche Schwachstellen bzw. verfügen oft über ungehinderte und unkontrollierte Zugangs- und Zugriffsmöglichkeiten.

Da die technische Ausrüstung zu großen Teilen frei erhältlich ist, ist auch der TECHINT-Bereich nicht nur den Nachrichtendiensten vorbehalten, sondern steht auch Unternehmen bei der Industriespionage offen.

COMPINT und DATAINT

Die beiden Begriffe COMPINT (COMPuter INTelligence) und DATAINT (DATA INTelligence) werden verwendet, wenn Informationen durch Eindringen in bzw. Nutzung von Computersystemen gesammelt werden.

Dazu wird beispielsweise Schadsoftware (Viren, Trojaner, Würmer) in die Unternehmenstechnik eingeführt, die in der Lage ist, Login-Daten, Netzwerkinformationen, Datenmaterial und Dokumente Unbefugten zugänglich zu machen und diese auch zu verändern. Rechner am Netz können Schadprogramme mittels entsprechend manipulierter E-Mail-Anhänge empfangen oder der Virus wird durch das Surfen auf verseuchten Websites auf dem Rechner installiert. Wird ein infizierter Rechner an ein Netzwerk angeschlossen, überträgt sich die Schadsoftware auf das gesamte Netz. Auch Datenträger (USB-Sticks, Flash-Karten, CDs etc.), z. B. als Werbemittel verteilt, werden zum Einbringen von Schadsoftware genutzt. Oft geschieht das Einbringen der Schadsoftware auch im Anschluss an das Social Engineering in Form empfangener E-Mails.

9 Wirtschaftsspionage in Baden-Württemberg und Bayern – Daten Fakten Hintergründe, Hrsg.: Landesamt für Verfassungsschutz Baden-Württemberg und Bayerisches Landesamt für Verfassungsschutz, Stand Oktober 2006, http://www.verfassungsschutz.bayern.de/imperia/md/content/lfv_internet/service/wirtschaftsspionage_bay_bw_2006.pdf, 22.01.2010.

3 Bedeutung von Know-how-Abfluss für Unternehmen

Know-how-Abfluss und Wirtschaftskriminalität in ihren Begehungsformen sind für Unternehmen bekannte, aber oft noch unterschätzte Risiken. Zu wenige sind sich bewusst, welche Auswirkungen Know-how-Abfluss etwa für ein forschendes Unternehmen haben kann. Umso wichtiger ist es, dass Studien dieses Phänomen aufgreifen, um das Risikobewusstsein zu schärfen und Handlungsempfehlungen zu bieten.

Von der Idee bis zur kommerziellen Nutzung bzw. Anmeldung eines Patentes müssen Unternehmen einen hohen (finanziellen) Forschungsaufwand betreiben, ohne exakt zu wissen, ob und wann daraus der geplante wirtschaftliche Erfolg erwächst. Gelangt ihre Technologie in der Entwicklungs- oder Erprobungsphase an den Wettbewerber, können die getätigten Investitionen ganz oder teilweise vergebens gewesen sein.

Insbesondere für deutsche Unternehmen, die innerhalb der Europäischen Union zu den innovativsten zählen und einen hohen Anteil der weltmarktrelevanten Patentanmeldungen besitzen, stellt der ungewollte Verlust von Know-how ein ernstzunehmendes Sicherheitsrisiko dar. Nach einem Bericht des BMBF lagen die weltmarktrelevanten Patentanmeldungen in Deutschland im Jahr 2007 bei 288 Patentanmeldungen je Million Erwerbstätige. Mit dieser Zahl lag Deutschland im internationalen Vergleich an sechster Stelle und somit noch vor den USA (245 Anmeldungen) und deutlich über dem OECD-Durchschnitt (173 Anmeldungen).[10]

Wirtschafts- und Industriespionage ist keine Erfindung des 21. Jahrhunderts, sondern es gibt sie bereits seit frühester Zeit und sie ist bis heute ein reales Bedrohungsszenarium. Medial spielt sie allerdings eine eher untergeordnete Rolle, da sich Betroffene in der Regel nicht als solche in den Medien wiederfinden. Auch Mechanismen und Kriterien des Medienmarktes (subjektive Attraktivität des Themas, aktuelle politische und wirtschaftliche Lage etc.) sind Gründe dafür.

10 Bericht zur technologischen Leistungsfähigkeit 2007, Hrsg.: Bundesministerium für Bildung und Forschung, http://www.bmbf.de/de/1869.php, 22.01.2010.

Wirtschafts- und Industriespionage hatte immer schon für die verschiedenen Volkswirtschaften und Unternehmen eine sehr große Relevanz. Trotz der hohen Bedeutung dieser Thematik gibt es bislang wenige empirische Erkenntnisse zu Schäden und Folgen aus Know-how-Verlusten.

Darüber hinaus finden schädigende Handlungen aus wirtschaftskriminellen Taten überwiegend erst Beachtung in den Unternehmen, wenn der Schadenseinschlag spürbar und damit erkennbar wird. Die frühzeitige Entdeckung solcher Taten ist für Unternehmen ebenso bedeutsam, wie es deren ungewollte Know-how-Verluste sind.

4 Studiendesign

Die „SiFo-Studie 2009/10“ gibt auf Basis empirisch gewonnener Ergebnisse einen Überblick über die aktuelle Situation überwiegend von kleinen und mittleren Unternehmen unterschiedlicher Branchen Baden-Württembergs in Bezug auf Wirtschaftskriminalität und deren Einschätzung ihrer Sicherheitslage. Von Experten und Fachkräften entwickelt und ausgewertet, liefert sie darüber hinaus wesentliche Erkenntnisse für Unternehmen deutschlandweit.

Von Juni bis August 2009 wurden in Baden-Württemberg über 4.000 Industrie- und Dienstleistungsunternehmen gebeten, einen standardisierten, webbasierten Fragebogen zum Themenbereich Wirtschaftskriminalität zu beantworten. Dabei beschränkte sich die Studie auf eine nach Branchen ausgewählte Stichprobe aus dem Kreis der Mitgliedsunternehmen der IHKs in Baden-Württemberg.

Die Entwicklung des Fragebogens, die Durchführung der Befragung, die Auswertung der Ergebnisse und Veröffentlichung der Studie wurden vom Ferdinand-Steinbeis-Institut in Kooperation mit der School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin u. a. mit dem wissenschaftlichen Leiter des Institute Corporate Integrity Management, Prof. Dr. Kai-D. Bussmann, durchgeführt.

Gegenstand der Untersuchungen waren Informationen zum Unternehmen, zu den Sicherheitsvorkehrungen im Hinblick auf den Schutz von Geschäfts- und Betriebsgeheimnissen, zu (potenziellen) Schädigungen durch Spionagefälle sowie zu Erfahrungen mit erlebten oder beobachteten Spionagefällen.

In die Auswertung eingeflossen sind letztlich die Angaben von 239 Unternehmen (welche im Folgenden, wenn nicht anders erwähnt, als „Unternehmen“ bezeichnet werden). Damit handelt es sich um eine der größten themeneinschlägigen, empirischen Untersuchungen in Deutschland zum Sicherheitsrisiko in Unternehmen. Über die Hälfte der Antworten (59 %) kommt aus der Geschäftsleitung, 12 % aus der Abteilung Unternehmenssicherheit und 15 % aus der Abteilung IT-Sicherheit, weitere 8 % der Antwortenden sind Compliance-Beauftragte.

Bei der großen Mehrheit der Befragten (86 %) handelt es sich um deutsche Unternehmen ohne ausländische Mehrheitsbeteiligung, etwa die Hälfte ist jedoch international aufgestellt (51 %). 16 % sind börsennotiert und 68 % sind eignergeführte bzw. Familienunternehmen.

Über die Hälfte der Unternehmen (55 %) geben an, dass ihr Unternehmen in Baden-Württemberg viel Forschung und Entwicklung betreibt (45 % wenig oder keine). Entsprechend der wirtschaftlichen Struktur in Baden-Württemberg besteht die Stichprobe überwiegend aus kleinen und mittleren, eigentümergeführten Unternehmen, wie sich an der Mitarbeiterzahl und ihrem Umsatz zeigt. Die Mehrheit der befragten Unternehmen gehört dem verarbeitenden Gewerbe an. In den folgenden Kapiteln werden nun die Studienergebnisse dargestellt.

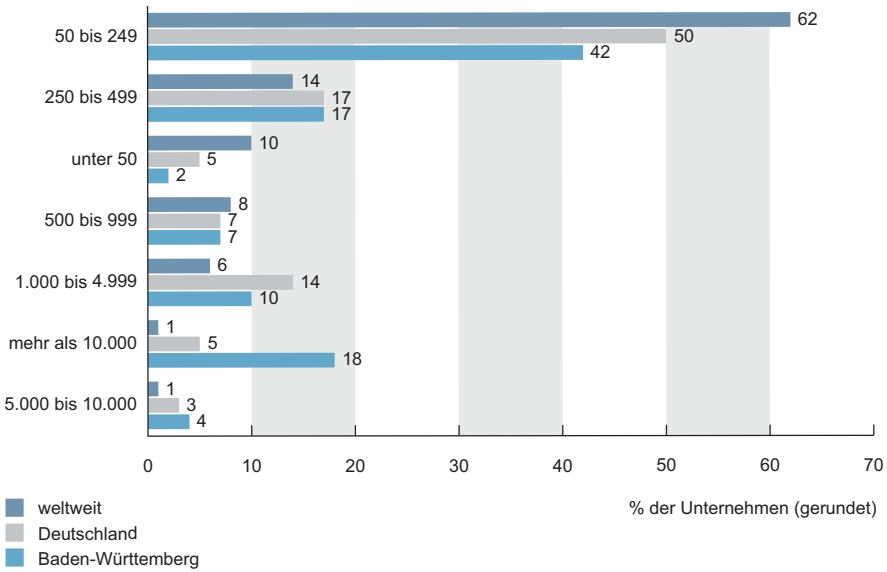


Abbildung 2: Mitarbeiteranzahl in den befragten Unternehmen

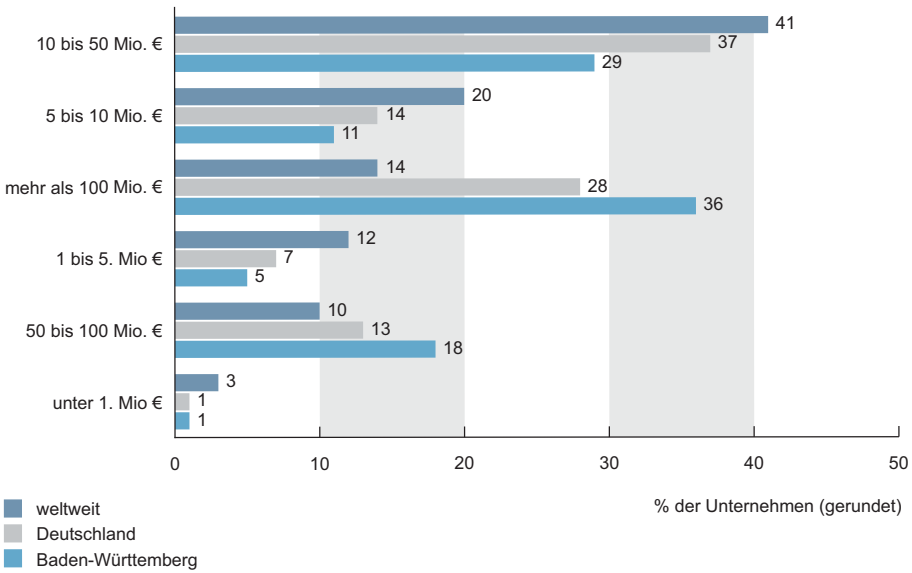


Abbildung 3: Umsatz der befragten Unternehmen

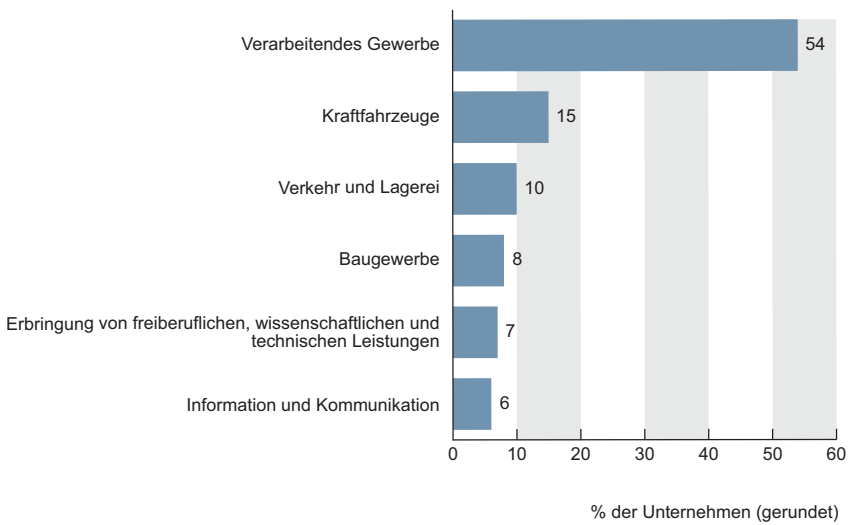


Abbildung 4: Branchen der befragten Unternehmen

5 Urheberrechtsverletzungen

Vom Verlust geistigen Eigentums sind Unternehmen nach wie vor erheblich betroffen. Angesichts dessen könnten sie jedoch ein größeres Repertoire an Schutzmaßnahmen nutzen, um ihren gewerblichen Rechtsschutz zu optimieren.

5.1 Von Urheberrechtsverletzungen betroffene Unternehmen

Geistiges Eigentum ist in der heutigen Zeit von ebenso bedeutendem Wert wie gegenständliches Eigentum. Unternehmenserfolg gründet sich auf erfolgversprechenden Ideen zu Produkten, Technologien und Design. Erfolgreiche Ideen finden allerdings zunehmend Nachahmer, zumal der Bedarf an Falsifikaten durch Markenfetischismus, gepaart mit einer „Geiz ist geil"-Mentalität, genährt wird. Insofern bedarf geistiges Eigentum von Unternehmensseite eines besonderen rechtlichen Schutzes. Dieser erfolgt mit strafrechtlichen und außerstrafrechtlichen Mitteln.

In der Studie werden die Verletzungen der wichtigsten Urheberrechte erhoben. Sie gibt daher ein differenziertes Bild über die Schwerpunkte der Rechtsverletzungen wieder. Des Weiteren berücksichtigt sie nicht nur Fälle, die aus Sicht des Unternehmens aufgeklärt sind, sondern auch konkrete Verdachtsfälle, die ebenfalls Gegenstand von strafrechtlichen Ermittlungen sein können. In der Kriminalstatistik des Bundeskriminalamtes werden nur Straftaten erfasst, die den Strafverfolgungsbehörden bekannt geworden sind und durch sie bearbeitet wurden. Diese sogenannte Hellfeldstatistik spiegelt nur einen kleinen Ausschnitt der vollständigen Risikolage von Urheberrechtsverletzungen wider.

Die Dunkelfeldstudie belegt, wie häufig Unternehmen durch Urheberrechtsverletzungen geschädigt werden. Die Ergebnisse der Befragung zeigen, dass sich knapp 38 % der Unternehmen in den letzten vier Jahren Urheberrechtsverletzungen ausgesetzt sahen (Verstöße gegen Patent- und Markenrechte, Gebrauchsmuster- und Geschmacksmusterrechte). Am stärksten werden vor allem die Unternehmen durch Produkt- und Markenpiraterie getroffen, die intensive Forschung und Entwicklungsarbeit betreiben.

Fast zwei Drittel dieser Unternehmen (65 %) sind hierdurch mindestens einmal geschädigt. Diese forschungsintensiven Unternehmen sind dadurch am häufigsten von Verstößen gegen ihre Patente (46 %) sowie dem Missbrauch einer geschützten Marke (33 %) betroffen.

Des Weiteren gibt jedes vierte forschungsintensive Unternehmen Gebrauchsmusterverletzungen (24 %) an. Auch gegen Geschmacksmusterrechte wird relativ häufig verstoßen; fast jedes fünfte forschungsstarke Unternehmen ist betroffen (17 %); weitere 8 % der befragten Unternehmen geben an, einen konkreten Verdachtsfall in den letzten vier Jahren gehabt zu haben.

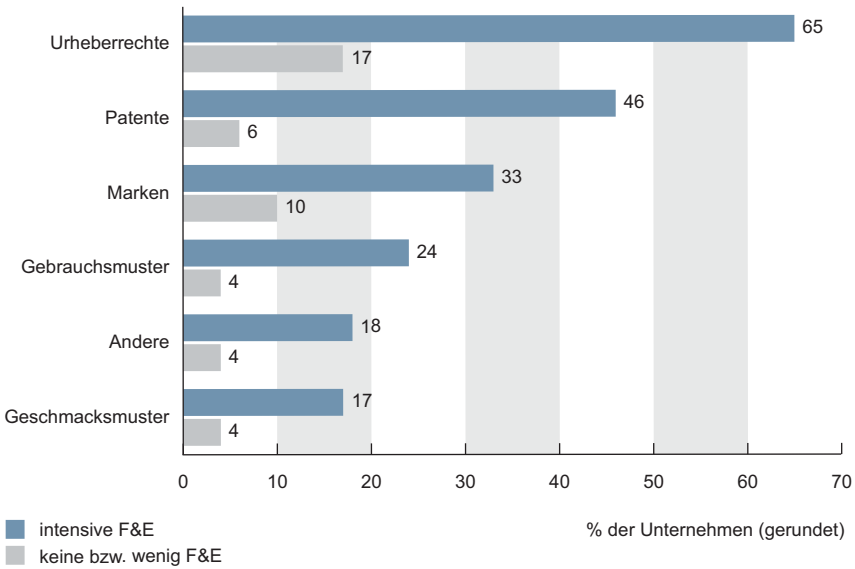


Abbildung 5: Verletzung von Rechten

5.2 Unmittelbare Schäden aus Urheberrechtsverletzungen

Die unmittelbaren Schäden aus Urheberrechtsverletzungen sind materieller Art, wie z. B. Wiederbeschaffungskosten, Wiederherstellungskosten, Sofortausfall der zu erwartenden Erträge aus Forschungsaufwendungen etc. Sie entstehen direkt mit der Begehung der Tat und können erheblich sein, wie die Studie zeigt. So geben die Unternehmen an, Schäden bis über zwei Millionen Euro je Vorfall gehabt zu haben. Im Durchschnitt handelt es sich hierbei um einen finanziellen Verlust für die geschädigten Unternehmen in Höhe von 364.000 Euro.

Die mit Abstand höchsten Schäden sind bei forschungsintensiven Unternehmen zu verzeichnen: im Durchschnitt über eine halbe Million Euro (548.000 Euro). Bei 23 % liegen die Schäden deutlich oberhalb dieses Mittelwertes.

5.3 Mittelbare Schäden aus Urheberrechtsverletzungen

Darüber hinaus sind die indirekten Auswirkungen nicht zu unterschätzen. Diese werden häufig auch als sogenannte Kollateralschäden bezeichnet und sind kaum geringer als bei anderen Wirtschaftsdelikten. Hierzu gehören z. B. langfristige Auswirkungen auf den Wettbewerb durch den Verlust exklusiven Know-hows, Beeinträchtigung der Geschäftsbeziehungen, Imageverlust, Kosten für die Durchsetzung von Schadenersatzansprüchen und Marktanteilsverluste durch Nachahmerprodukte, die in Folge von Urheberrechtsverletzungen entstehen können.

Insbesondere für forschungsintensive Unternehmen sind diese indirekten Folgen von Urheberrechtsverletzungen durch Verletzungen des geistigen Eigentums gravierend. Über die Hälfte (53 %) dieser forschungsintensiven Unternehmen berichten über Beeinträchtigungen der Geschäftsbeziehungen und nahezu jedes zweite Unternehmen (46 %) beklagt Umsatzeinbußen infolge von Urheberrechtsverletzungen. Kaum weniger Unternehmen stellen bedeutende strategische Vorteile für die Wettbewerber (44 %) sowie einen ungewollten Transfer von Forschungswissen (40 %) fest. Auch das Ansehen des Unternehmens und seiner Marke bzw. seines Produktes kann Schaden nehmen, beispielsweise durch Imitate. Mehr als jedes dritte forschungsstarke Unternehmen ist von derartigen negativen Folgen betroffen.

Festgelegte Regeln, Richtlinien oder Gesetze müssen praktikabel sein und von Unternehmen umgesetzt werden. Die Hauptlast der Rechtsdurchsetzung tragen die geschädigten Unternehmen, wie die Studie zeigt. Über zwei Drittel (67 %) der betroffenen forschungsintensiven Unternehmen bewerten ihre Aufwendungen finanzieller und zeitlicher Art für die zivil- und strafrechtliche Rechtsdurchsetzung als besonders hoch.

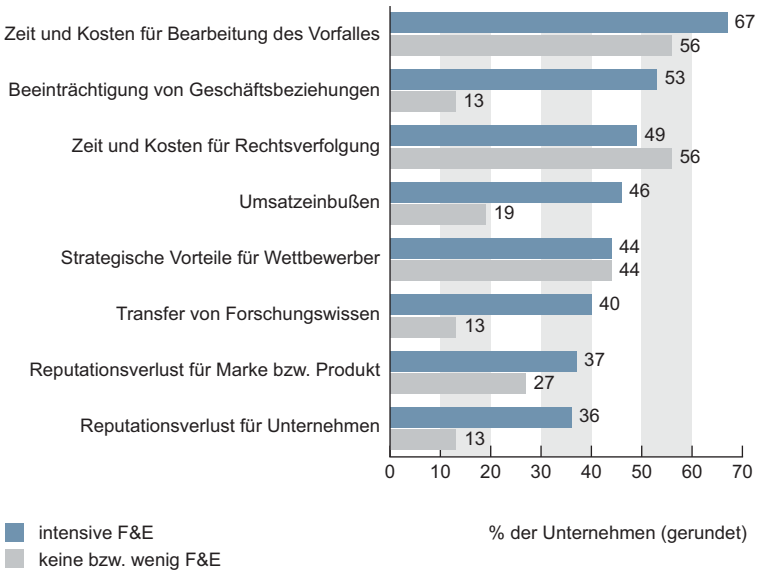


Abbildung 6: Mittelbare Schäden aus Urheberrechtsverletzungen

Die Unternehmen, welche die Hauptlast für Forschung und Entwicklung tragen, werden somit nicht nur deutlich häufiger durch Urheberechtsverletzungen geschädigt, sie tragen auch die höchsten hieraus resultierenden finanziellen Konsequenzen, die sich indirekt auch in Managementkosten und Wettbewerbsnachteilen niederschlagen. Letztere sind nur schwer finanziell zu beziffern, können jedoch durch ihre Fernwirkung durchaus das Niveau der finanziellen Schäden erreichen, wie sich aus der Vielfalt der indirekten Auswirkungen schließen lässt.

5.4 Schutzmaßnahmen

Unternehmen, die keine oder nur wenig Forschung und Entwicklung betreiben, verfügen auch kaum über antragsfähige Erfindungen und andere Formen geistigen Eigentums. Bei der Mehrheit der forschungsintensiven Unternehmen ist dies jedoch anders, wie Abb. 7 zeigt.

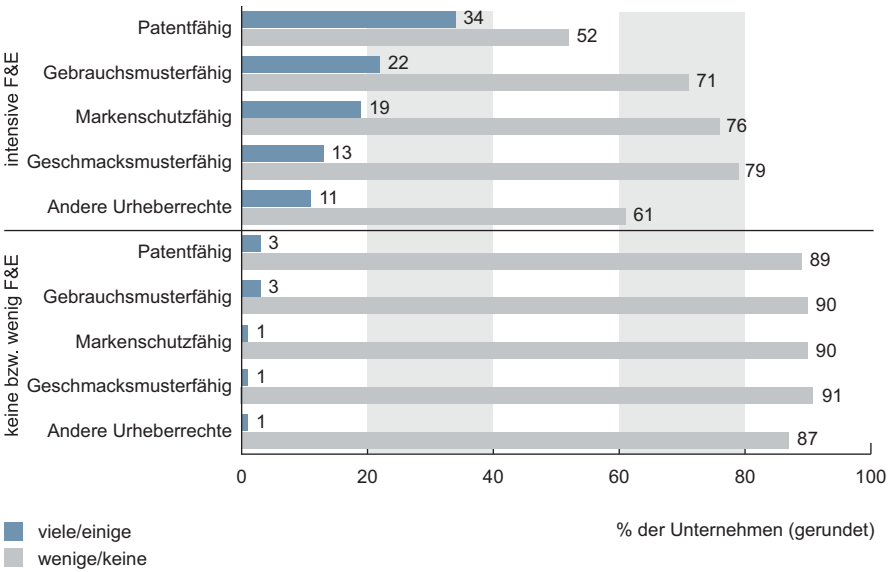


Abbildung 7: Schutzmaßnahmen vor Urheberrechtsverletzungen

Ein Drittel dieser Unternehmen verfügt über eine Reihe antragsfähiger (64 %), aber bislang nicht geschützter Patente. Fast jedes vierte Unternehmen (22 %) aus dieser Gruppe verfügt über ungeschützte Geschmacksmusterrechte (Designschutz). Dieses Bild zeigt sich auch bei den anderen Formen geistigen Eigentums. Ein Teil ihres geistigen Eigentums ist somit rechtlich schutzlos.

Die Gründe für diese Situation sind vielfältig. Eine zentrale Ursache gibt es nicht. Beinah alle im Fragebogen vorgegebenen Begründungen werden gleichermaßen ausgewählt, hier bestehen kaum Unterschiede zwischen forschungsintensiven und

den übrigen Unternehmen. Bei der Hälfte der Unternehmen mit ungeschützten Patenten liegt aus ihrer Sicht die Antragsreife noch nicht vor (54 %), aber fast ebenso viele der kleinen und mittleren Unternehmen scheuen vor allem den hohen zeitlichen (48 %), finanziellen (48 %) und rechtlichen Aufwand (44 %) einer Antragstellung.

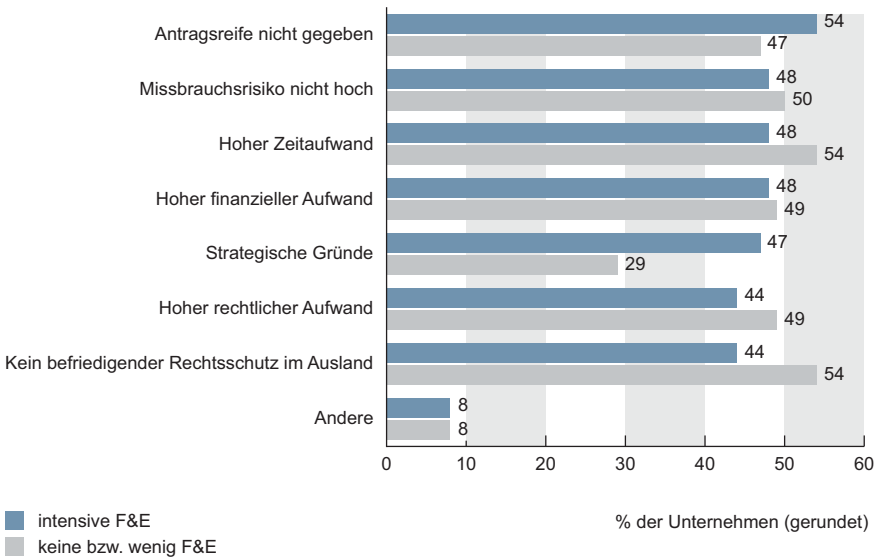


Abbildung 8: Gründe für das Unterlassen von Maßnahmen zum Schutz von Urheberrechten

Etwa die Hälfte beklagt sich zudem über den mangelhaften Schutz im Ausland, so dass bei einigen Produkten auf eine Eintragung eines Patentes verzichtet wurde. Dies ist ein alarmierendes Ergebnis. Hier zeigt sich, wie wichtig Fortschritte im internationalen Urheberrechtsschutz für Forschung und Entwicklung in Deutschland sind.

6 Verrat von Geschäfts- und Betriebsgeheimnissen

Know-how-Abfluss zu entdecken und aufzuklären, bedeutet zunächst, die Risikofaktoren und Gefahrenbereiche innerhalb und außerhalb eines Unternehmens zu erkennen. Die Erhebung macht deutlich, welche Unternehmensbereiche mit Fällen konfrontiert sind und welche Schäden daraus abzuleiten sind.

6.1 Von Verrat von Geschäfts- und Betriebsgeheimnissen betroffene Unternehmen und einzelne Geschäftsbereiche

Die am meisten verbreitete Form der Wirtschafts- und Industriespionage ist der Verrat oder das Ausspähen von Geschäfts- und Betriebsgeheimnissen. In dieser Studie werden die Häufigkeit dieser Deliktsform und der jeweilige Unternehmensbereich, der hiervon betroffen war, erhoben. Der Vergleich zwischen forschungsintensiven und anderen Unternehmen zeigt, dass erwartungsgemäß die forschungsintensiven Unternehmen deutlich häufiger Opfer von Geheimnisverrat und Spionage wurden. Mehr als jedes Vierte dieser Unternehmen gibt mindestens einen derartigen Fall an. Hier liegen die Hauptziele der Täter naturgemäß im Bereich Produktion und Fertigung (19 %) sowie Forschung und Entwicklung (14 %).

Vergleichsweise selten sind die Bereiche Einkauf und Vertrieb sowie Marketing und Werbung ebenso wie die Personalabteilung ein erfolgreiches Ziel der Täter (jeweils 5 %). Aus den Bereichen Finanzabteilungen und Geschäftsleitung wird von forschungsintensiven Unternehmen kein Fall berichtet.

Dies erklärt sich u. a. daraus, dass diese Unternehmen generell einen höheren Sicherheitsstandard aufweisen (siehe Kap. 10.3) und es ihnen trotz ihrer starken Forschungsorientierung offenbar im Allgemeinen besser gelingt, viele Bereiche ihres Unternehmens vor Angriffen zu schützen. Bei den Unternehmen, die keine oder nur wenig Forschung und Entwicklung betreiben, streuen sich dagegen die Vorfälle über alle Bereiche relativ gleichmäßig.

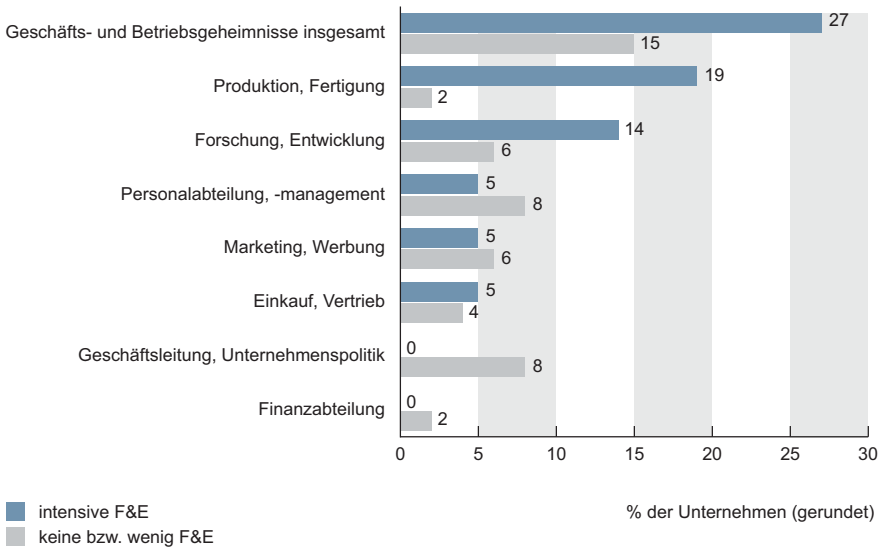


Abbildung 9: Häufigkeit des Verrates von Geschäfts- und Betriebsgeheimnissen

6.2 Dunkelfeld

Fälle von Wirtschaftskriminalität im Unternehmen lassen sich trotz vieler Hinweise häufig nur schwer aufklären. Dieses Problem stellt sich daher im Speziellen auch beim Verrat von Geschäfts- und Betriebsgeheimnissen und Urheberrechtsverletzungen. Daher wird in der Studie nicht nur nach den eindeutigen Fällen, sondern auch nach konkreten Verdachtsfällen gefragt. Im Vergleich zeigt sich, dass forschungsintensive Unternehmen seltener über konkrete Verdachtsfälle berichten als Unternehmen, die weniger intensiv Forschung betreiben. Mehr als jedes dritte Unternehmen (38 %) nennt mindestens einen Verdachtsfall gegenüber jedem vierten (24 %) in der Gruppe der forschungsintensiven Unternehmen.

Dies spricht für die These, dass forschungsintensive Unternehmen besser gegen derartige Angriffe gewappnet sind und diese eher entdecken. Umgekehrt können sich Unternehmen, die kaum Forschung und Entwicklung betreiben, nicht generell sicherer fühlen.

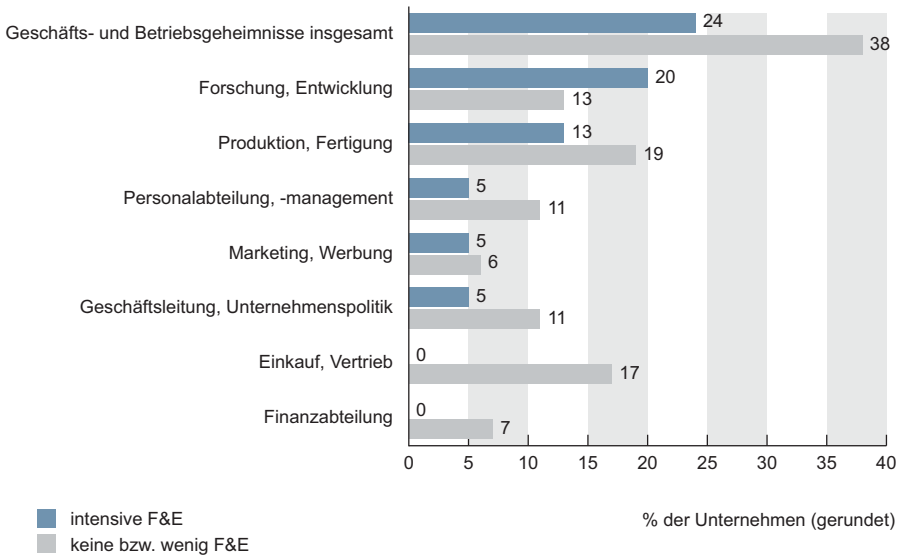


Abbildung 10: Verdacht auf Verrat von Geschäfts- und Betriebsgeheimnissen

Auch sie werden häufig durch Verrat und Spionage von Geschäfts- und Betriebsgeheimnissen geschädigt; ihnen gelingt jedoch die Entdeckung der Angriffe seltener. Viele Vorfälle bleiben Vermutungen oder dunkle Ahnungen. Die Quote von nicht aufgeklärten Verdachtsfällen in beiden Unternehmensgruppen lässt vermuten, dass das Dunkelfeld erheblich sein dürfte, da mit dieser Befragung nur ein kleiner Teil des Dunkelfeldes „erhellt“ wird.

Im Unterschied zur polizeilichen Kriminalstatistik wird bei den Verdachtsfällen keine Strafanzeige vorausgesetzt – nur bei jedem dritten Vorfall erfolgte eine Strafanzeige (siehe Kap. 8.3) –, gleichwohl müssen derartige Delikte überhaupt entdeckt worden sein, bevor hiervon in der Umfrage berichtet werden konnte. Diese Verdachtsfälle bilden nur einen kleinen Ausschnitt aus dem Dunkelfeld, da die Ergebnisse von der Sensibilität, vom Umfang und der Effizienz der Kontrollmaßnahmen in den Unternehmen abhängen. Aus diesem Grund kann derzeit ein beachtliches absolutes Dunkelfeld vermutet werden.

Erst durch ein hohes Problembewusstsein in den Unternehmen verbunden mit effektiven Kontroll- und Präventionsmaßnahmen kann dieses Dunkelfeld verringert werden, ohne jedoch eine sofortige kriminalitätssenkende Wirkung zu erreichen. Aus kriminologischer Sicht handelt es sich um ein Kontrollparadox, denn die Entdeckungswahrscheinlichkeit hängt von der Kontrollintensität ab. Allein aufgrund höherer Sensibilität und verbesserter Kontrolle werden häufiger Straftaten entdeckt, die früher unentdeckt blieben, so dass das Dunkelfeld aufgehellt wird.

Mit einer Zunahme der Entdeckungen vergrößert sich das Hellfeld und das Dunkelfeld verkleinert sich entsprechend. Aus der kriminologischen Forschung weiß man, dass der höchste Abschreckungseffekt weniger durch die Androhung strenger Konsequenzen und Strafen, sondern durch die Erhöhung des subjektiven Entdeckungsrisikos erreicht wird. Kontrollen sind daher am wirksamsten, wenn sie jedem bekannt sind, sie im Unternehmen kommuniziert und wahrgenommen werden.

6.3 Unmittelbare Schäden durch den Verrat von Geschäfts- und Betriebsgeheimnissen

Die wirtschaftlichen Auswirkungen durch Verrat oder Ausspähung von Geschäfts- und Betriebsgeheimnissen lassen sich nur schwer schätzen. Die betroffenen Unternehmen beziffern im Durchschnitt ihre finanziellen Schäden mit 171.000 Euro, wobei der Betrag bei forschungsintensiven Unternehmen mit 259.000 Euro deutlich höher ist.

Derartige Verluste können vor allem mittelständische Unternehmen bereits empfindlich treffen. 19 % der geschädigten Unternehmen stufen die finanziellen Folgen immerhin als beträchtlich ein. Zu berücksichtigen ist überdies, dass es sich nur um Durchschnittswerte handelt. Bei jedem fünften betroffenen Unternehmen liegen die angegebenen Schäden deutlich oberhalb eines Betrages von einer halben Million Euro.

6.4 Mittelbare Schäden durch den Verrat von Geschäfts- und Betriebsgeheimnissen

Darüber hinaus sollten die indirekten Auswirkungen nicht unterschätzt werden. Sie sind kaum geringer als bei anderen Wirtschaftsdelikten; auch hier berichtet die Mehrheit über teilweise erhebliche mittelbare Folgen. In vielen Fällen sind diese mittelbaren Folgen einschneidender als die direkten finanziellen Schäden. Signifikante Unterschiede zwischen den forschungsintensiven Unternehmen und den Unternehmen, die weniger Forschung betreiben, finden sich nicht.

Bemerkenswert ist, dass infolge der Spionagefälle nur 7 % der betroffenen Unternehmen über einen ungewollten Transfer von Forschungswissen berichten, aber jedes zweite als Konsequenz vor allem erhebliche strategische Vorteile für Wettbewerber feststellt. Zurückzuführen ist dies besonders darauf, dass zwar die Bereiche Forschung und Entwicklung sowie Produktion und Fertigung besonders zahlreich betroffen sind, aber hier wichtiges Forschungswissen überwiegend urheberrechtlich – zumeist durch Patente – geschützt wird. Angriffe auf dieses Forschungswissen fallen folglich unter die Deliktsgruppe der Urheberrechtsverletzungen.

Der Schwerpunkt der Fälle von Verrat oder Ausspähen von Geschäfts- und Betriebsgeheimnissen richtet sich auf das Ausforschen von strategisch verwertbaren Informationen wie Forschungsstrategien, Produktions- und Vertriebsplanungen usw. Gelangen diese Informationen an den Wettbewerber, können sich schwerwiegende Beeinträchtigungen der Geschäftsbeziehungen ergeben, da z. B. die Konkurrenz mit gleichen oder ähnlichen Strategien an die Kunden oder Lieferanten herantritt. Jedes vierte Unternehmen konstatiert in dieser Befragung schwerwiegende Beeinträchtigungen von Geschäftsbeziehungen (24 %). Zahlreiche Unternehmen berichten des Weiteren über hohe Aufwendungen für die Bearbeitung der Vorfälle (33 %) sowie die Rechtsverfolgung (27 %).

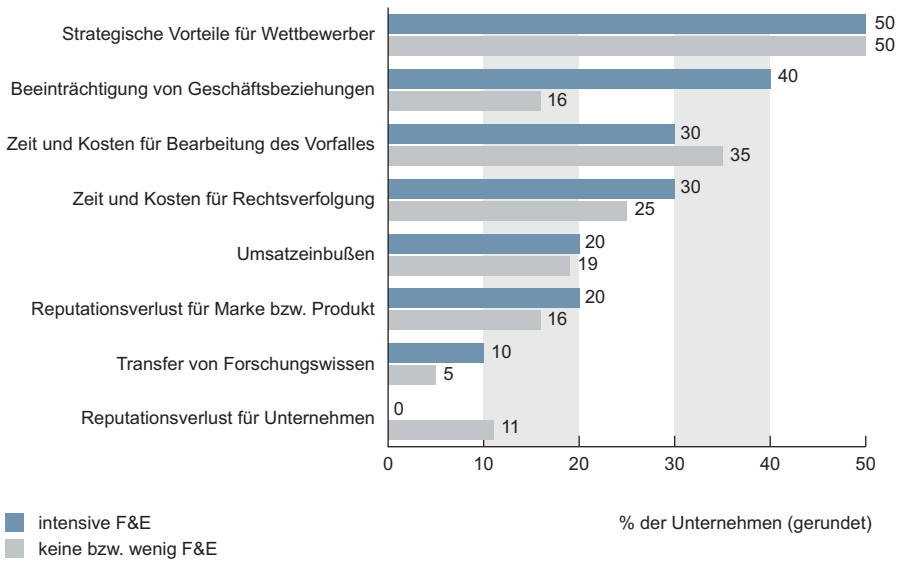


Abbildung 11: Mittelbare Schäden durch den Verrat von Geschäfts- und Betriebsgeheimnissen

7 Wirtschaftskriminalität

Die Bedeutung der Wirtschaftskriminalität ist bei forschungsintensiven und innovativen Unternehmen nicht zu unterschätzen. Ihre Bedrohung wird aber deutschlandweit noch als zu gering bewertet.

Neben Know-how-Abfluss stellen wirtschaftskriminelle Handlungen nach wie vor ein weiteres Risiko für Unternehmen dar. Die Studie untersucht daher auch, inwieweit sich die Unternehmen in der Vergangenheit mit wirtschaftskriminellen Machenschaften in den eigenen Reihen auseinandersetzen mussten.

Ob forschungsintensiv oder nicht, spielt für die Delikte der Wirtschaftskriminalität keine nennenswerte Rolle: Von Unterschlagung, Untreue und Betrug sind sowohl forschungsintensive als auch nicht forschungsintensive Unternehmen spürbar betroffen (24 % bzw. 32 %), während Korruption für die befragten Unternehmen offenbar nur geringe Bedeutung hat und nur bei weniger als 10 % der Unternehmen erkannt wurde, wie Abb.12 zeigt.

Durchschnittlich verzeichnen die betroffenen Unternehmen in den letzten vier Jahren drei bis vier Fälle von Unterschlagung, Untreue und Betrug, jedoch nur ein bis zwei Fälle von Korruption.

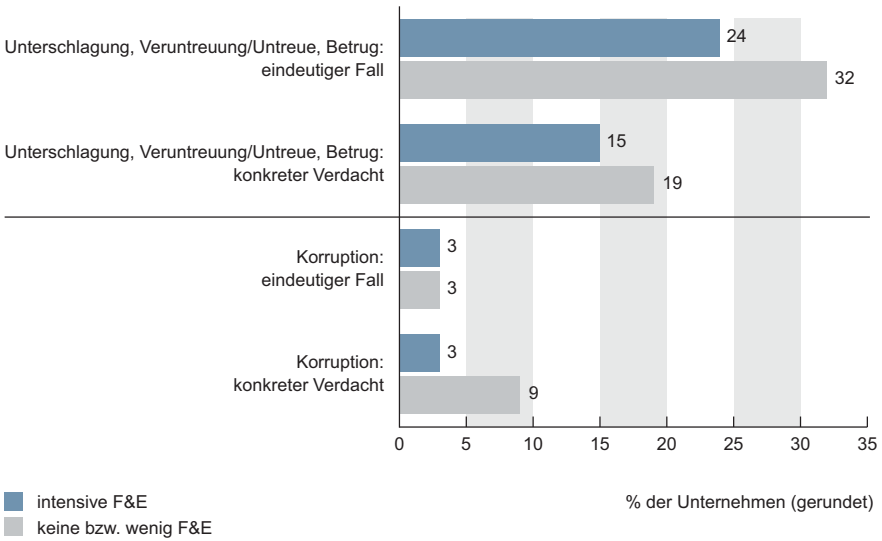


Abbildung 12: Häufigkeit von Wirtschaftskriminalität

Diese Erkenntnisse entsprechen nicht den Ergebnissen aus einschlägigen übergreifenden Studien zur Wirtschaftskriminalität. Zum einen ist dies darauf zurückzuführen, dass sich die „SiFo-Studie 2009/10“ überwiegend an Sicherheitsverantwortliche und forschungsintensive Branchen wendet, die verstärkt mit Know-how-Abflüssen zu kämpfen haben. Zum anderen referenzieren die internationalen Wirtschaftskriminalitätsstudien auch große Unternehmen, deren Fallzahlen und Schadensausmaße nicht unmittelbar vergleichbar mit der Zielgruppe der vorliegenden Erhebung sind. Allerdings lässt sich aus diesem Ergebnis auch folgern, dass die Gefahr der Wirtschaftskriminalität überwiegend erst erkannt wird, wenn das Unternehmen von Schadenseinschlägen betroffen ist. Wirtschaftskriminalität ist ein Kontrolldelikt. Erst professionelle Kontrolle deckt die zum Teil langjährigen kriminellen Machenschaften im Verborgenen auf.

Die Gefahr von Wirtschaftsdelikten darf von einer verantwortungsbewussten Unternehmensleitung daher nicht unterschätzt werden, auch wenn die Risiken aus Know-how-Verlusten auf den ersten Blick wesentlicher erscheinen.

Die Verantwortlichen sollten zum eigenen Unternehmensschutz proaktiv mit dem Thema Wirtschaftskriminalität umgehen und gleichzeitig ein gemeinsames Werteverständnis im Unternehmen schaffen, um schädigendes Verhalten zu minimieren und die öffentliche Wahrnehmung des Unternehmens damit gleichzeitig zu verbessern. Entscheidend ist neben der Einführung von verständlichen und vertrauensfördernden Regeln die unbedingte Kontrolle der Einhaltung und bei Nichtbeachtung die konsequente Sanktionierung.

Ebenfalls nicht zu unterschätzen sind von der Unternehmensführung vorgegebene Leitbilder, die – zumindest moralisch – für die Einhaltung der Werte des Unternehmens verantwortlich sind. Vertrauen in eine wertebasierte Unternehmenskultur lässt sich nur aufbauen und erhalten, wenn das gesamte Top-Management hinter diesem Konzept steht.

Durch regelmäßige Schulungen werden die Mitarbeiter erreicht und nachhaltig in den Prozess eingebunden, um diese Kultur im Unternehmen zu pflegen und weiter auszubauen.

8 Entdeckung der Taten

Wird eine Straftat oder eine unerwünschte und gleichzeitig schädigende Handlung im Unternehmen erkannt und schließlich auch sanktioniert? Herrscht Transparenz und Kommunikationsbereitschaft bis hin zur oberen Führungsebene? Diese Aspekte fördern oder hemmen die Ermittlung von Straftaten oder Fehlverhalten. Kontrolle im Einklang mit positiver und nachhaltig orientierter Unternehmenskultur stärkt die Integrität des Einzelnen und erhöht darüber hinaus das Entdeckungsrisiko eines Täters enorm.

8.1 Entdeckungswege

Für eine wirksame Prävention gegen Täterverhalten ist eine möglichst hohe Entdeckungswahrscheinlichkeit entscheidend. Demgegenüber besitzt das Drohen mit einer möglichen Strafanzeige keine vergleichbare Wirkung. Aus diesem Grund sollten die implementierten Kontrollmaßnahmen nicht nur effektiv, sondern auch allgemein bekannt sein. Nur dann ist die Wahrscheinlichkeit der Entdeckung auch aus der Sicht potenzieller Täter erkennbar hoch. Der subjektiven Entdeckungswahrscheinlichkeit kommt daher die höchste Abschreckungswirkung zu.

Unternehmen sollten sich dabei bewusst sein, dass sie in der Entdeckung von Angriffen und der Gefährdung ihrer Geschäfts- und Betriebsgeheimnisse weitgehend auf sich allein gestellt sind. Lediglich 4 % der Fälle werden laut Angaben der Unternehmen durch Strafverfolgungsbehörden wie Polizei und Staatsanwaltschaft aufgedeckt. Dies bedeutet, dass das Entdeckungsrisiko für potenzielle Täter außerordentlich gering bleibt, wenn Unternehmen vor allem auf die Aufklärungsarbeit staatlicher Stellen vertrauen.

Dieses Ergebnis stimmt mit kriminologischen Erkenntnissen zur klassischen Kriminalität überein. Auch hier werden Straftaten primär nicht von der Polizei bemerkt, sondern von Opfern und Zeugen angezeigt.[11] Würde die Gesellschaft in erster Linie auf die Entdeckung dieser Straftaten durch die Strafverfolgungsbehörden bauen, gäbe es eine extrem hohe Dunkelziffer.

11 Siehe beispielsweise Kunz, Karl-Ludwig: Kriminologie, 4. Aufl., UTB, Stuttgart, 2004, § 27 Rdn. 19.

In der vorliegenden Studie sind es Hinweise von internen (42 %) oder externen (31 %) Tippgebern, die in fast drei Viertel der Fälle (73 %) zur Aufdeckung führten. In anderen Studien zur Wirtschaftskriminalität liegt diese Quote ähnlich hoch.[12] Ohne diese Hinweisgeber wäre das Dunkelfeld noch sehr viel größer.

Demgegenüber spielen unternehmensinterne Abteilungen zur Unternehmens- und IT-Sicherheit, für Compliance, Recht und Revision eine vergleichsweise untergeordnete Rolle (8 %). Dies lässt vermuten, dass die vorhandenen Kontrollmechanismen vielleicht zur Abschreckung, aber wenig zur Aufdeckung beitragen. So beruhen 8 % der Ermittlungen auf Zufallsfunden. Die Tatsache, dass unternehmensinterne Abteilungen in dieser Studie nur sehr selten an der Aufdeckung von Taten beteiligt sind, kann damit zusammenhängen, dass die in dieser Studie sehr stark vertretenen kleinen und mittleren Unternehmen derartige Verantwortungen nicht als gesonderte Abteilungen führen bzw. diese sich noch im Aufbau befinden.

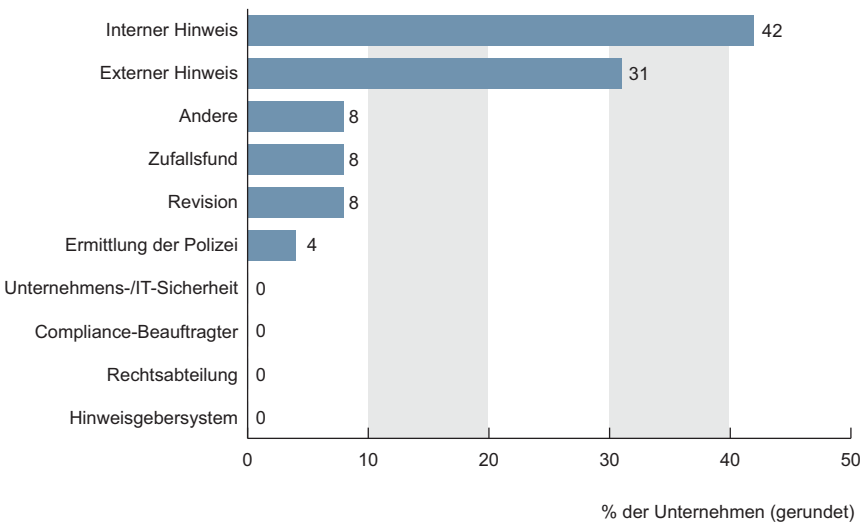


Abbildung 13: Entdeckungswege der Taten im Unternehmen

12 U. a. PricewaterhouseCoopers, Wirtschaftskriminalität 2007 – Sicherheitslage der deutschen Wirtschaft, http://pwc.com.

Die Aufdeckung von Wirtschaftsdelikten ist somit von vielen Zufällen abhängig, insbesondere von der Bereitschaft von internen und externen Personen, dem Unternehmen einen Hinweis auf mögliche Schadensfälle zu geben. Dies bedeutet auch, dass im Dunkelfeld vieler Unternehmen Wirtschaftsstraftäter weiterhin ungestört tätig sein können und kaum befürchten müssen, entdeckt zu werden.

Prävention darf sich daher nicht allein auf potenzielle Täter ausrichten, sondern sie sollte auch ihre soziale Umgebung, vor allem die Unternehmensangehörigen, in Form von Schulungen einbeziehen. Es kommt auf die Sensibilität der Belegschaft an, die auch durch die Unternehmenskultur geprägt wird, und auf die soziale Missbilligung einer Straftat im persönlichen, informellen Umfeld des Täters. Sie kann die informelle Sozialkontrolle, d. h. die Kontrolle und Sanktion von Taten innerhalb des Unternehmens durch Unternehmensangehörige, positiv oder negativ prägen. Strafbare Verhaltensweisen können sich auf diese Weise entweder ungestört ausbreiten oder aber sie werden eingedämmt[13].

Die informelle Sozialkontrolle erfüllt somit eine wichtige Funktion. Je größer die Kommunikationsbereitschaft und Transparenz in einem Unternehmen ist, desto höher sind die Tathemmungen potenzieller Täter. Denn diese Täter müssen befürchten, auf strafrechtlich relevante Verhaltensweisen angesprochen zu werden oder sogar Ächtung zu erfahren. Der Kampf gegen Wirtschaftskriminalität ist somit wie auch bei der klassischen Kriminalität ein gemeinsamer Kampf, der ohne ethisches Klima und positive Unternehmenskultur nicht erfolgreich geführt werden kann.

Ein hoher Anteil externer und interner Tippgeber kann folglich Indikator für eine intakte informelle Sozialkontrolle darstellen. Wichtig wäre es jedoch, dass Hinweisgeber sich an dafür zuständige Stellen im Unternehmen wenden könnten, wie etwa die Interne Revision, oder über ein Hinweisgebersystem an einen dafür verantwortlichen Ansprechpartner. Dies ist jedoch noch zu selten der Fall.

13 Bussmann, Kai-D.: Compliance in der Zeit nach Siemens – Corporate Integrity, das unterschätzte Konzept, in: Zeitschrift für Betriebswirtschaftliche Forschung und Praxis (BFuP), Heft 5/2009, S. 224.

Insbesondere empfehlen sich Hinweisgebersysteme, über die jedoch nur jedes Fünfte der befragten Unternehmen (19 %) verfügt (siehe Kap. 10.5). Im Rahmen eines derartigen Systems wendet sich der Informant – im Gegensatz zum externen Whistleblowing (d. h. der Weitergabe von Verstößen an externe Stellen) – an eine vertrauensvolle Stelle innerhalb der eigenen Organisation, so dass Reputationsschäden in der Öffentlichkeit nicht zu befürchten sind. Dies nutzt zunächst dem Unternehmen: Negative öffentliche Reaktionen sind nicht zu befürchten; das vitale Interesse an Informationen über zum eigenen Nachteil begangene Straftaten wird befriedigt. Ohne solche Hinweise würden die im Verborgenen ablaufenden dolosen Handlungen fortgeführt, das Unternehmen würde weiterhin geschädigt und an Wettbewerbsfähigkeit einbüßen.

Aus Furcht vor negativen Folgen verschweigen Unternehmensangehörige jedoch häufig Kenntnisse über Gesetzesverstöße von Vorgesetzten oder Kollegen. Hier kann ein solches auf Anonymität ausgerichtetes System Abhilfe schaffen. Darüber hinaus tragen Hinweisgebersysteme auch zur Erhöhung des subjektiven Entdeckungsrisikos bei. Jahrzehntelange kriminologische Forschungen zeigen, dass nicht schwere Strafen abschrecken, sondern die Furcht entdeckt zu werden. Hinweisgebersysteme können dieses subjektive Entdeckungsrisiko für potenzielle Wirtschaftsstraftäter erhöhen. Gegenwärtig ist das objektive und eng damit verbunden auch das subjektive Entdeckungsrisiko im Bereich der Wirtschaftsdelikte generell sehr niedrig. Die primäre Zielsetzung eines Hinweisgebersystems liegt mithin weniger in der Aufdeckung, sondern mittel- und langfristig primär in der Prävention durch Drohung mit Entdeckung.

8.2 Beteiligte an der Ermittlung

Die Ermittlung in Fällen von Verrat oder Spionage von Geschäfts- und Betriebsgeheimnissen machen die befragten Unternehmen in der Regel zur „Chefsache“. In acht von zehn Fällen ist die Geschäftsleitung maßgeblich an der Aufklärung des Falles beteiligt (81 %). Sie wird in jedem vierten Fall durch die IT-Abteilung unterstützt (23 %). Die Ermittlungen werden außerdem in einigen Fällen durch Mitarbeiter aus den Bereichen Compliance, Recht und Revision sowie durch weitere nicht im Einzelnen genannte Abteilungen durchgeführt bzw. maßgeblich unterstützt.

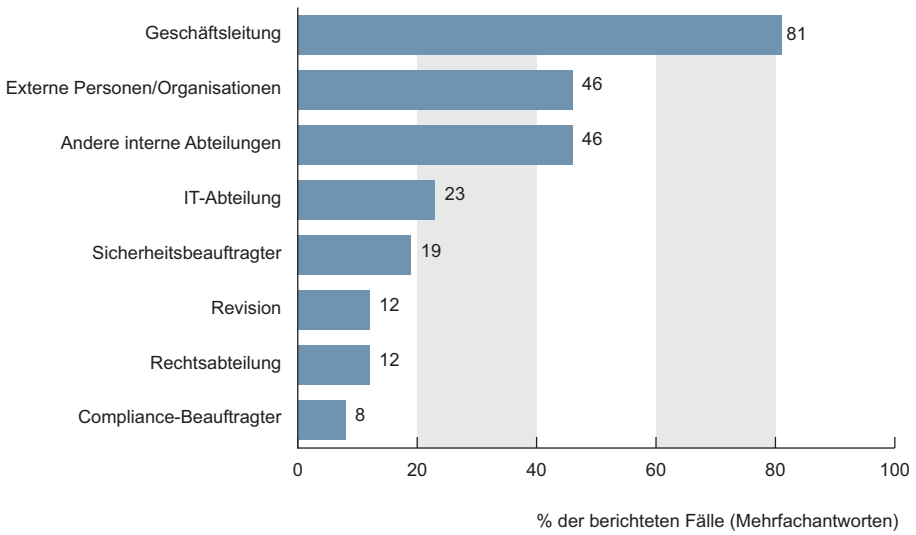


Abbildung 14: Involvierte Personen bei der Bearbeitung von Vorfällen

Bemerkenswert ist, dass viele Unternehmen sich bei ihrer Ermittlung von externen Personen und Organisationen unterstützen lassen. Insbesondere für kleine und mittlere Unternehmen rechnet sich das eigene Vorhalten forensischer Fachkompetenz nicht. Beinahe in jedem zweiten Fall sind daher externe Personen involviert (46 %).

8.3 Reaktionen auf die Taten

Auf Vorfälle von Verrat und Spionage von Geschäfts- und Betriebsgeheimnissen reagieren die betroffenen Unternehmen zumeist mit organisatorischen Maßnahmen im Bereich Personal und Geschäftsabläufe (75 %).

Diese Maßnahmen sind einfacher und schneller umsetzbar als IT-Sicherungs- und Objektschutzmaßnahmen. Daraus erklärt sich der hohe Prozentsatz. Andererseits sind in den Geschäftsabläufen auch häufig Schwachstellen anzutreffen, die oft erst durch Taten Einzelner entdeckt werden. Die logische Reaktion auf die Entdeckung einer Tat ist dann das sofortige Schließen der Lücke, um Wiederholungstaten zu

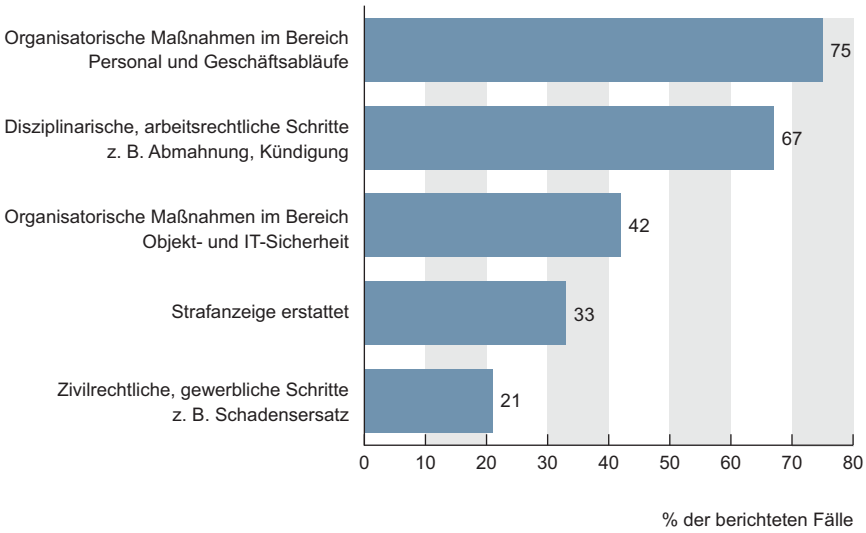


Abbildung 15: Maßnahmen aufgrund des Verrates von Geschäfts- und Betriebsgeheimnissen

vermeiden. Dies sind zum Beispiel Verschluss von Akten, Anweisungen an das Personal, Umorganisation von Informationswegen usw. Hierfür spricht auch, dass sich die befragten Unternehmen sehr viel stärker gegen Angriffe im Objekt- und IT-Bereich und weniger im Bereich Personal und Geschäftsabläufe rüsten (siehe Kap. 10.5). Zudem schätzten sie den Schwerpunkt der Tatbegehungsformen falsch ein. Dieser liegt weniger in der IT- und Telekommunikationstechnik als vielmehr in dem geringer geschützten Bereich Personal und Geschäftsabläufe (siehe Kap. 9.1).

Gegenüber dem Täter reagieren die Unternehmen überwiegend mit betrieblichen Sanktionen (67 %), dagegen wird nur in jedem dritten Fall eine Strafanzeige gestellt.

8.4 Gründe für das Unterlassen der Strafanzeige

Das überwiegende Unterlassen einer strafrechtlichen Anzeige seitens der Unternehmensleitung kann darauf beruhen, dass sich das Unternehmen schwierigen Beweisfragen gegenübergestellt sieht, Angst vor Reputationsschäden hat bzw. weitere Nachteile befürchtet. In der Tat werden sehr häufig als Grund der unsichere Ausgang der Strafverfolgung (77 %) sowie die Dauer des Strafverfahrens (53 %) genannt.

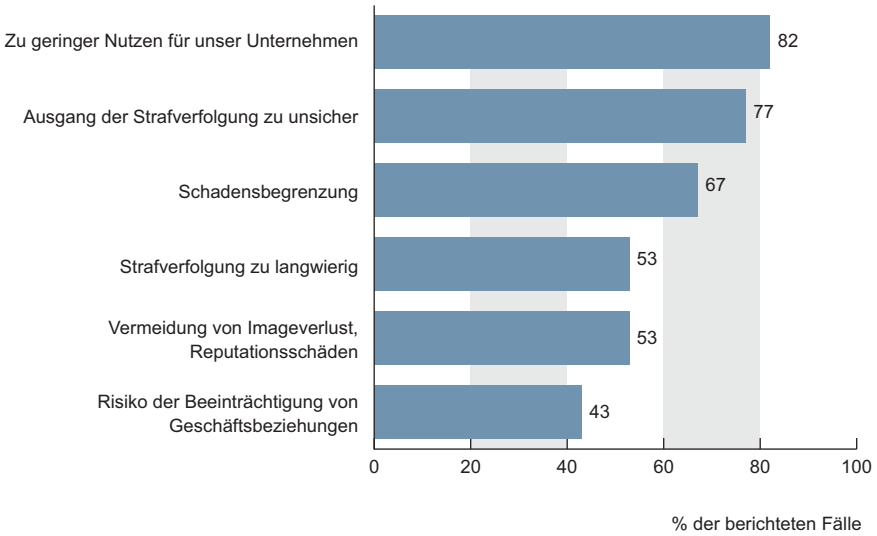


Abbildung 16: Gründe für das Unterlassen von Strafanzeigen

Für 82 % der Unternehmen stellt sich der interne Nutzen einer Strafverfolgung für das Unternehmen als zu gering dar und für zwei Drittel dient das Unterlassen einer Strafanzeige der Schadensbegrenzung (67 %). Jedes zweite Unternehmen nennt konkret drohende Reputationsschäden (53 %) und 43 % befürchten die Beeinträchtigung von Geschäftsbeziehungen.

Unternehmen sollten dabei jedoch Folgendes berücksichtigen: Für ihre Glaubwürdigkeit ist es nach innen wie auch nach außen wichtig, dass auf Regelverletzungen, insbesondere auf strafbare Handlungen, konsequent durch die Geschäftsleitung reagiert wird. Zwar wird auch aus Sicht der kriminologischen Forschung die abschreckende Wirkung einer Strafanzeige eher überschätzt, jedoch eignen sich strafrechtliche Sanktionen langfristig zur Schärfung des Norm- und Unrechtsbewusstseins. Insofern sollten unter dem Gesichtspunkt einer „Zero Tolerance“ zumindest folgenschwere Verstöße mit einer Strafanzeige geahndet werden. Viele Unternehmen berücksichtigen nur selten, dass eine konsequente Strafverfolgung auch zu einem Werte- und Unrechtsbewusstsein beiträgt. Immerhin sehen fast alle Unternehmen im mangelnden Unrechtsbewusstsein der Täter die Hauptursache für ihre Taten (93 %).

9 Täterprofile

Persönlichkeitsstrukturen potenzieller Täter und deren Begehungsformen einer Tat weisen unabhängig von Branche und Größe eines Unternehmens starke Parallelen auf. Durch Tätergruppen wie etwa langjährige Geschäftspartner oder Mitarbeiter entstehen dabei nicht nur erhebliche finanzielle Schäden, deren Taten bringen gleichzeitig erhebliche Zweifel an der Integrität und dem moralischen Anspruch des Unternehmens mit sich. Es zeigt sich wiederholt, dass professionelles Misstrauen einem gesunden Vertrauen gegenüberstehen muss.

9.1 Formen der Tatbegehung

Laut Ergebnissen der Studie ist die häufigste Begehungsform ganz trivialer Art: Die Hälfte der Taten wird nach Angabe der Befragten durch Entwenden und Kopieren von Firmenunterlagen begangen. Daneben gibt es eine Fallgruppe, die auf Unachtsamkeit mancher Unternehmen zurückzuführen ist. Jeder vierte Fall von Verrat und Spionage von Geschäfts- und Betriebsgeheimnissen geschieht unter Verwendung öffentlich zugänglicher Quellen, beispielsweise durch Publikationen von Unternehmensangehörigen, Produktinformationen usw.

Eine weitere Gruppe der Tatbegehungen wird zumeist unterschätzt: Sicherheitslücken im Bereich Personal und Geschäftsabläufe. 25 % der Taten wurden durch ehemalige Mitarbeiter und Manager begangen, die zuvor abgeworben worden waren. Weitere 13 % lassen sich auf das sogenannte Social Engineering – beispielsweise das gezielte Aushorchen von Unternehmensmitarbeitern auf Tagungen und Messen – zurückführen.

Ebenfalls nicht zu unterschätzen sind technische Sicherheitslücken. 13 % der betroffenen Unternehmen berichten über erfolgreiche Angriffe auf ihr IT-System und ebenfalls so viele über Angriffe auf mobile IT-Systeme. In 6 % der Fälle erfolgte die Spionage durch Abhören von Kommunikationsmitteln. Andere Begehungsformen, wie das Abhören von Geschäftsräumen, sind dagegen laut Angaben der Unternehmen relativ selten. Dies bedeutet natürlich nicht, dass derartige Gefahren nicht ernst genommen werden sollten. Sicherheitsmaßnahmen im Objekt- und IT-Bereich

sind wichtig. Darüber hinaus werden die Risiken im Bereich Personal und Geschäftsabläufe zu sehr unterschätzt. Hier ist noch erhebliche Arbeit in der Prävention erforderlich, wie die Ergebnisse der Studie zeigen (siehe Kap. 10).

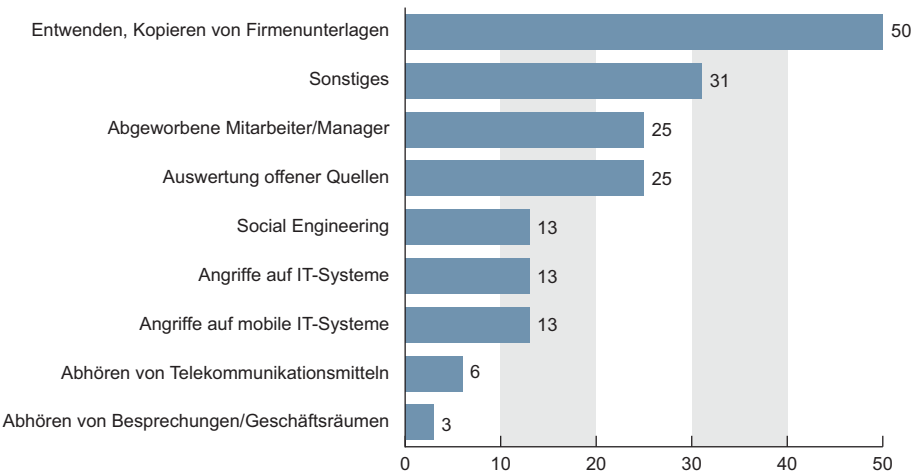


Abbildung 17: Art der Tatbegehung bei Fällen von Spionage

9.2 Herkunftsland der (Haupt-)Täter

Die meisten Täter stammen aus Deutschland, die wenigsten aus dem Ausland. Allerdings gibt es deliktspezifische Besonderheiten. Bei den Verstößen gegen das Urheberrecht kommen die Täter laut Angaben der Befragten am häufigsten aus Asien, gefolgt von deutschen und anderen westeuropäischen Tätern.

Bei den Verstößen gegen Geschäfts- und Betriebsgeheimnisse und bei Fällen von Wirtschaftskriminalität ist das häufigste Herkunftsland der Täter bzw. Organisationen Deutschland. In jeweils über 60 % der Fälle kommen die Täter bzw. Organisationen aus Deutschland, d. h. die Unternehmen wurden im eigenen Land durch eigene Mitarbeiter, Konkurrenzunternehmen etc. geschädigt. Zwar kommen die Täter bzw. Organisationen zum Teil auch aus West- und Osteuropa sowie Asien, jedoch ist dieser Anteil im Vergleich zu den anderen Ländern gering.

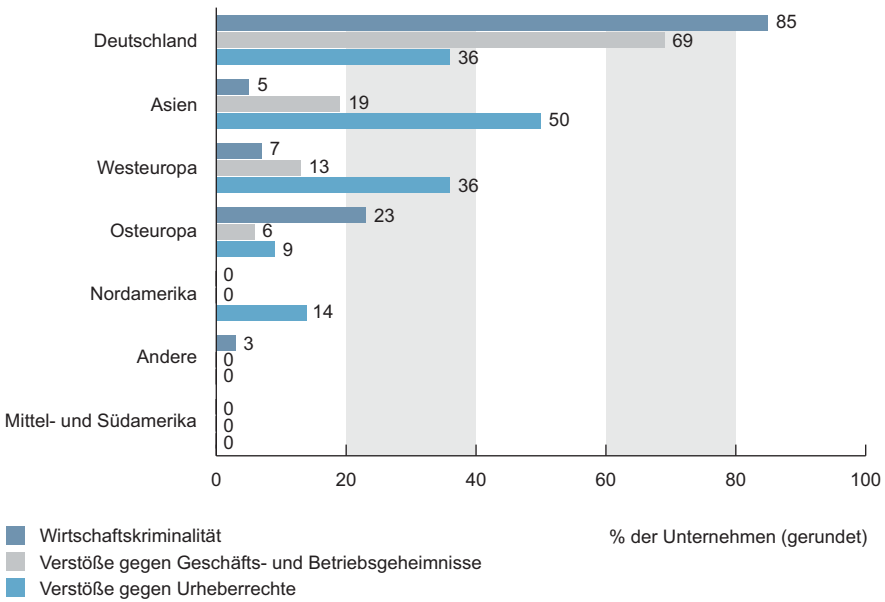


Abbildung 18: Herkunftsland der Täter

9.3 Beziehung der Täter zum Unternehmen

Die meisten Unternehmen machen die gleiche ernüchternde Erfahrung: Die Mehrheit der Täter stammt aus dem Kreis der Mitarbeiter (unabhängig von Tätigkeit und Hierarchiestufe). Einem Großteil der Personen hätte man die Tat nicht zugetraut. Gegen derartige Vertrauensbrüche in den eigenen Reihen vermag man sich zweifellos kaum zu schützen. Viele Studien stellen übereinstimmend fest, dass Wirtschaftsstraftäter eher sozial unauffällig und daher mittels prognostischer Verfahren kaum zu identifizieren sind. Über 70 % der Täter kommen aus den eigenen Reihen des geschädigten Unternehmens. Die Ergebnisse zeigen, dass Unternehmen mit keiner bzw. wenig Forschung und Entwicklung deutlich stärker durch interne Täter betroffen sind. Ein Verlust von Geschäfts- und Betriebsgeheimnissen droht Unternehmen somit eher von innen und weniger von außen. Gemessen an dieser Risikoverteilung werden in vielen Unternehmen Präventionsmaßnahmen im Bereich Personal und Geschäftsabläufe jedoch zu sehr vernachlässigt, wie die Studie ergab (siehe Kap. 10.5).

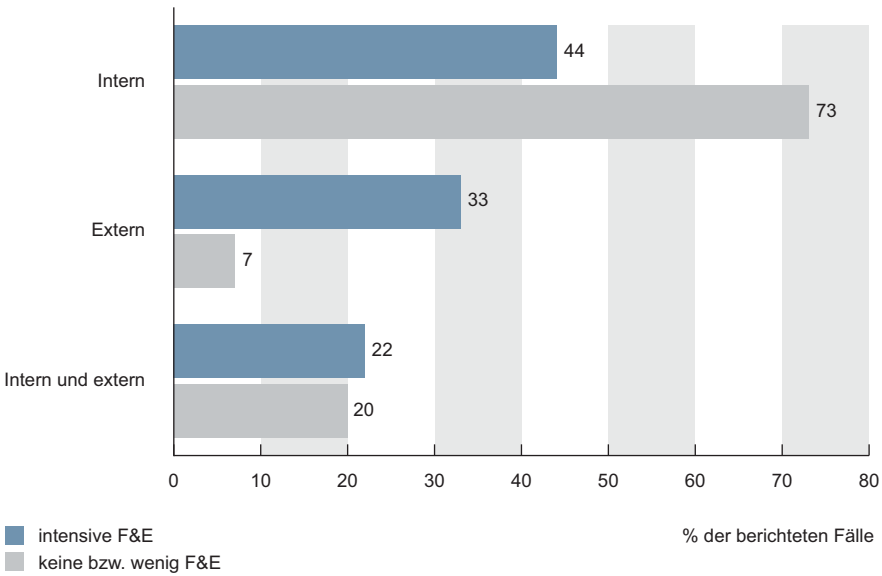


Abbildung 19: Beziehung der Täter zum Unternehmen

Vertrauen baut sich mit zunehmender Betriebszugehörigkeit auf. Neuen Mitarbeitern und Managern begegnet man mit größerer Vorsicht, wenn es um sicherheitsrelevante Informationen geht. Dies ist zwar eine rationale Herangehensweise, jedoch lehrt die wirtschaftskriminologische Forschung, dass dieses Vorgehen falsch ist. Die Gefahren drohen Unternehmen weniger von jungen und neu eingestellten Mitarbeitern und Managern, sondern von Personen, zu denen aufgrund langjähriger Betriebszugehörigkeit ein Vertrauensverhältnis entstanden ist.

Der typische Wirtschaftsstraftäter ist laut Ergebnissen dieser Studie sozial unauffällig. Er ist im Durchschnitt etwa 40 Jahre alt, männlich, überdurchschnittlich gebildet und gehört dem Unternehmen seit zehn Jahren an. Bei den externen Tätern bestand ebenfalls eine mehrjährige Geschäftsverbindung von durchschnittlich sechs Jahren. Dieses Profil gilt ebenso für Fälle mit Verstößen gegen das Urheberrecht als auch mit Verrat oder Ausspähen von Geschäfts- und Betriebsgeheimnissen. Potenzielle Wirtschaftsstraftäter sind somit keine Berufsanfänger, vielmehr sind sie im eigenen Haus „groß geworden“. Viele nutzten offenkundig die Zeit, um die Schwachstellen

in der Unternehmensorganisation zu erkennen und zu ihrem persönlichen Vorteil auszunutzen. Zumindest unter dem Gesichtspunkt der Kriminalprävention sollte daher langjährigen Mitarbeitern mit viel Erfahrung und hohem Ansehen kein besonderer Vertrauensbonus entgegengebracht werden.

Jedoch ist ein generelles Misstrauen gegenüber langjährigen Unternehmensangehörigen ebenso nicht angebracht. Dies könnte sich nach Forschungen zur Arbeits- und Organisationspsychologie sogar als kontraproduktiv erweisen, wenn das Unternehmensklima hierdurch vergiftet wird und infolgedessen die Neigung zu unternehmensschädigendem Verhalten sogar zunimmt. Ein besonderer Vertrauensbonus gegenüber bestimmten Gruppen ist – empirisch gesehen – nicht gerechtfertigt. Kontroll- und Präventionsmaßnahmen sollten sich daher auf alle Gruppen erstrecken. Mithin muss in der Belegschaft ein Problembewusstsein geschaffen und um Akzeptanz der Vorsichts- und Präventionsmaßnahmen seitens der Unternehmensleitung geworben werden.

9.4 Tätergruppen

Die Ergebnisse der Studie zeigen, dass sich die Täter über alle Positionen und Ränge verteilen. Gemessen an ihrer Personalstärke lässt sich ein relativ hoher Anteil von Führungskräften unter den Tätern wiederfinden. In fast jedem fünften Fall (19 %) sind Topmanager zumindest beteiligt, in nahezu jedem dritten ein Manager aus dem mittleren Management (31 %). Weitere Gefahren drohen von abgewanderten Mitarbeitern und Managern (25 %) sowie von Wettbewerbern (22 %) und Subunternehmen (16 %).

Demgegenüber spielen ausländische Nachrichtendienste in der Studie nur eine untergeordnete Rolle (6 %). Allerdings kann dieses Risiko bei forschungsintensiven Großunternehmen deutlich höher sein, als es die Studie zeigt, da sie überwiegend im Bereich der kleinen und mittleren Unternehmen durchgeführt wurde. Auch ist zu berücksichtigen, dass die illegale Informationsbeschaffung durch Nachrichtendienste aufgrund ihrer hohen Professionalität schwerer zu entdecken ist.

Ferner zeigen die Ergebnisse dieser Studie, dass auch in der Gruppe der externen Täter in der Regel eine irgendwie geartete Geschäftsbeziehung bestanden hat. In neun von zehn Fällen ist der Täter dem Unternehmen vor der Tat bekannt. Insgesamt zeigt sich, dass der Verrat von Geschäfts- und Betriebsgeheimnissen typischerweise von unternehmensnahen Tätern begangen wird.

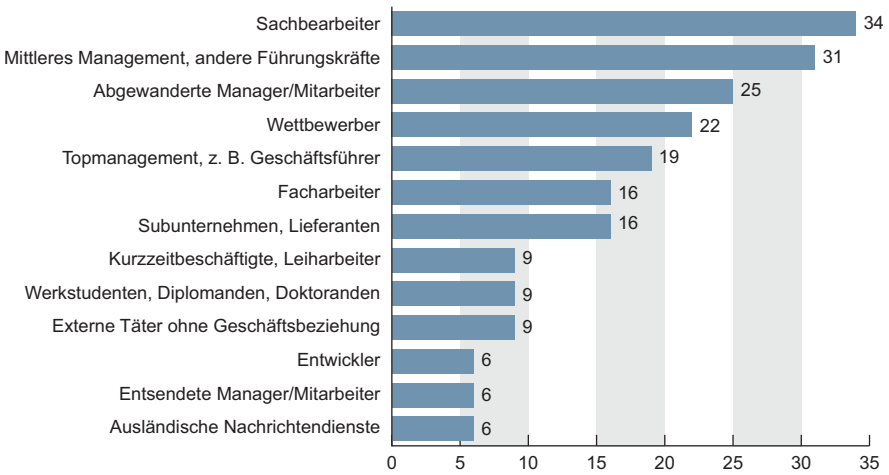


Abbildung 20: Position des Täters

9.5 Tatmotive

Innerhalb der Studie wurde zusätzlich nach den Ursachen und Motiven von Tätern eines Verrates oder einer Spionage von Geschäfts- und Betriebsgeheimnissen gefragt. Die Teilnehmer der Studie wurden gebeten, Angaben zu den internen Tätern zu machen, da Motive und Ursachen von externen Personen oder Organisationen weniger eindeutig zu erklären sind. Die internationale Werteforschung stellt seit langem im Generationenvergleich das Phänomen einer zunehmenden Fragmentierung der Werte fest. Dies heißt, je nach Situation und Kontext werden sie unterschiedlich angewendet und akzeptiert. Was außerhalb eines Unternehmens selbstverständlich als illegal angesehen wird, kann im Arbeitsalltag eines Unternehmens ge-

billigt werden. Werte scheinen von Generation zu Generation allmählich ihre absolute Geltung verloren zu haben. Diese Fragmentierung der Normgeltung ist zudem der Nährboden für subkulturelle Milieus, in denen bestimmte Normen und Werte kaum noch beachtet werden.[14]

Diese Forschung bestätigt den Eindruck der Befragten. In Unternehmen besteht Übereinstimmung darüber, dass auf Seiten der internen Täter mangelndes Werte- und Unrechtsbewusstsein eine der Hauptursachen für die Taten ist (93 %). Des Weiteren spielt Gier eine große Rolle: 82 % der Täter konnten den finanziellen Verlockungen nicht widerstehen und 43 % leugneten die finanziellen Nachteile für das betroffene Unternehmen. Allerdings führen 57 % der geschädigten Unternehmen den Verlust von Geschäfts- und Betriebsgeheimnissen auch auf ihre noch zu unsystematische Prävention und 76 % auf mangelhafte interne Kontrollen zurück. Hier können sich Unternehmen aus eigener Kraft präventiv besser schützen. Ein nicht klar kommunizierter Geheimhaltungswille spielt aus Sicht der Unternehmen kaum eine Rolle (15 %). Des Weiteren geschah jede zweite Tat unter Beteiligung von internen und externen Kollaborateuren und jede dritte aufgrund von Bestechung und Erpressung (31 %). Eine weitere Ursache liegt in der Unternehmenskultur. Mehr als jede zweite Tat wird auf berufliche Enttäuschungen bzw. einen Karriereknick (69 %) zurückgeführt. Zwar schaffen grundsätzlich vermehrte Gelegenheiten und geringere Kontrollen erhöhte Kriminalitätsrisiken, aber das ethische Klima im Unternehmen[15] und die Bindung an das Unternehmen[16] hemmen die Neigung zum Ausnutzen von Tatgelegenheiten. Menschen agieren nicht ausschließlich nach schlichten Kosten-Nutzen-Kalkülen, sondern sie bewegen sich immer auch in einer spezifischen Wertekultur, die auch durch das Unternehmen mitgeprägt wird. Für eine effiziente interne Kriminalprävention ist daher entscheidend, dass eine Unternehmenskultur entwickelt wird, in der in allen Bereichen konsistent die Unternehmenspraxis auf ethischen und integritätsförderlichen Werten und Prinzipien wie Entscheidungstransparenz und Fairness aufbaut.[17]

14 Bussmann, Kai-D.: Kriminalprävention durch Business Ethics – Ursachen von Wirtschaftskriminalität und die besondere Bedeutung von Werten, in: Zeitschrift für Wirtschafts- und Unternehmensethik (zfwu), 2004, S. 35–50.

15 Eigenstetter, Monika / Dobiasch, Stefan / Trimpop, Rüdiger: Committment and Counterproductive Work Behaviour as Correlates of Ethical Climate in Organizations, in: Monatsschrift für Kriminologie und Strafrechtsreform (MschrKrim), Jg. 90(2–3), 2007, S. 224–244.

16 Felfe, Jörg: Mitarbeiterbindung, Hogrefe, Göttingen, 2008.

17 Bussmann, Kai-D.: Steinbeis Compliance und Integrity Monitor, Nachhaltigkeit durch Mitarbeiterbefragung, in: Zeitschrift für Risk, Fraud & Compliance (ZRFC), Heft 5/2009, S. 224.

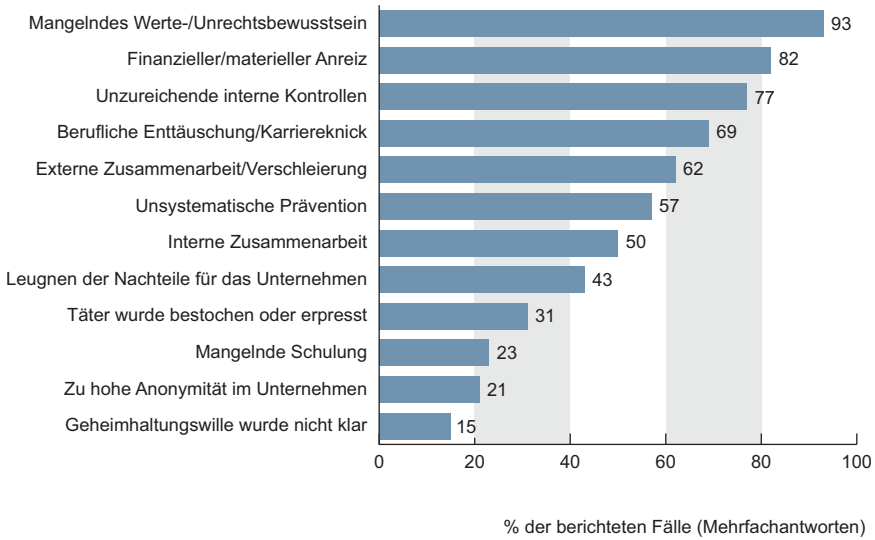


Abbildung 21: Tatgründe der internen Täter

Die Unternehmenskultur ist umso bedeutsamer als aus Sicht der Kriminologie der Sozialisation der Täter eine wesentliche Bedeutung für die Entstehung von Kriminalität zukommt. Unterschieden wird zwischen primärer und sekundärer Sozialisation. Die primäre findet in der Familie statt, die sekundäre Sozialisation im Freundeskreis, in der Schule und im Beruf. Folglich kommt der Sozialisation im Unternehmen eine nicht zu vernachlässigende Bedeutung bei der Verhinderung kriminellen Verhaltens zu. Auch die Ergebnisse dieser Studie zeigen, dass dies in diesem Deliktsbereich umso mehr gilt, da die entdeckten Täter in der Regel keine Berufsanfänger sind, sondern sogar lange dem betroffenen Unternehmen angehört haben, im Durchschnitt zehn Jahre (siehe Kap. 9.3).

Die Ursachen für Wirtschaftsdelikte sind daher nicht ausschließlich in der Täterpersönlichkeit oder in mangelnden Kontrollmaßnahmen zu sehen. Für einen Teil der Straftaten können sich auch unternehmensspezifische Faktoren begünstigend ausgewirkt haben, die in der Studie nur ansatzweise untersucht werden konnten.

10 Mittelfristige Risikoeinschätzung

Die Bereitstellung von Kapazitäten zum Schutz vor Know-how-Abfluss innerhalb eines Unternehmens ist überwiegend auf IT- und Organisationsprozesse ausgerichtet. Neben diesem technischen Schutz wird dem umfassenden Sicherheitsbedürfnis eines Unternehmens jedoch nur dann nachhaltig Rechnung getragen, wenn bei der Entwicklung von Präventionsmaßnahmen auch das Täterverhalten Berücksichtigung findet. Wie die Studie zeigt, muss eben dieser Umgang mit Geschäftspartnern sowie Unternehmensangehörigen besonders beachtet werden.

10.1 Erwartungen der Unternehmen, Opfer zu werden

Die Mehrzahl der Unternehmen schätzt die Risiken hoch ein, durch Produkt- und Markenpiraterie in den nächsten Jahren geschädigt zu werden: 32 % halten dies in den nächsten zwei Jahren für wahrscheinlich, fast genauso viele waren hiervon bereits innerhalb der vergangenen vier Jahre betroffen.

Ein hohes Problembewusstsein besteht ebenfalls gegenüber den Risiken, Opfer eines Verrates oder einer Spionage von Geschäfts- und Betriebsgeheimnissen zu werden. Allerdings werden die Risiken, durch Vermögensdelikte geschädigt zu werden, im Allgemeinen eher unterschätzt[18].

18 Die niedrige Fallzahl berichteter Korruptionsfälle erlaubt aus methodischen Gründen keinen Vergleich mit der Risikoeinschätzung.

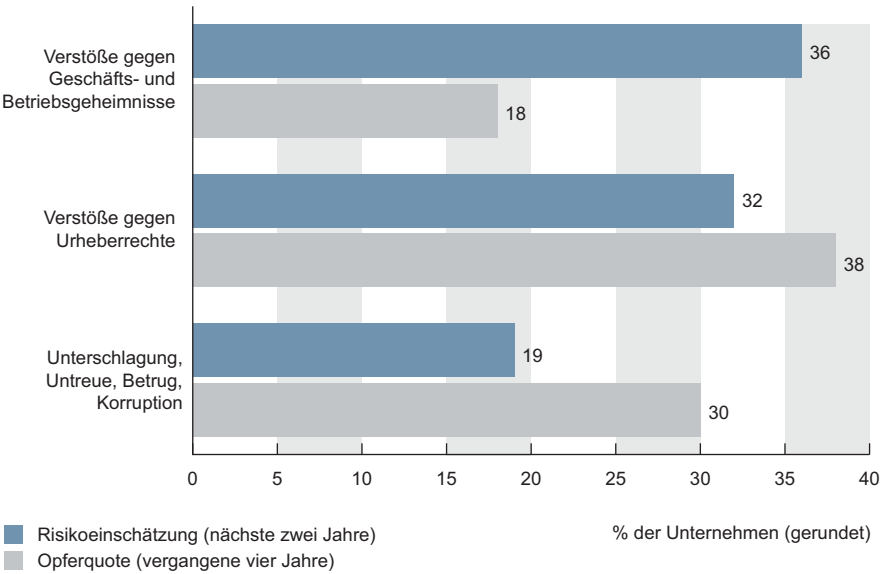


Abbildung 22: Erwartung der Unternehmen, in den nächsten zwei Jahren Opfer zu werden, und Opferquote der vergangenen vier Jahre

10.2 Erwarteter Tathergang

Die Mehrheit der Unternehmen hält vor allem technische Angriffe auf ihre IT oder sonstige technische Geräte für wahrscheinlich und andere Begehungsformen durch Unternehmensangehörige, externe Personen und ausländische Nachrichtendienste für weniger wahrscheinlich. Insbesondere forschungsintensive Unternehmen sehen ihre Schwachstellen in den technischen Sicherheitssystemen.

Fast jedes zweite Unternehmen (46 %) vermutet hier ein hohes Risiko; lediglich 25 % gehen von einem geringen Risiko aus. Dies ist eine Unterschätzung, denn im Vergleich zu den übrigen Unternehmen, die keine oder wenig Forschung und Entwicklung betreiben, werden forschungsintensive Unternehmen deutlich häufiger Opfer von Spionageangriffen als andere. Mehr als die Hälfte der Unternehmen hält es sogar für unwahrscheinlich, dass eigene Mitarbeiter oder Manager betroffen sein könnten. Die Studie belegt, dass dies eine folgenschwere Fehleinschätzung ist. Die größte Tätergruppe stammt aus dem eigenen Unternehmen.

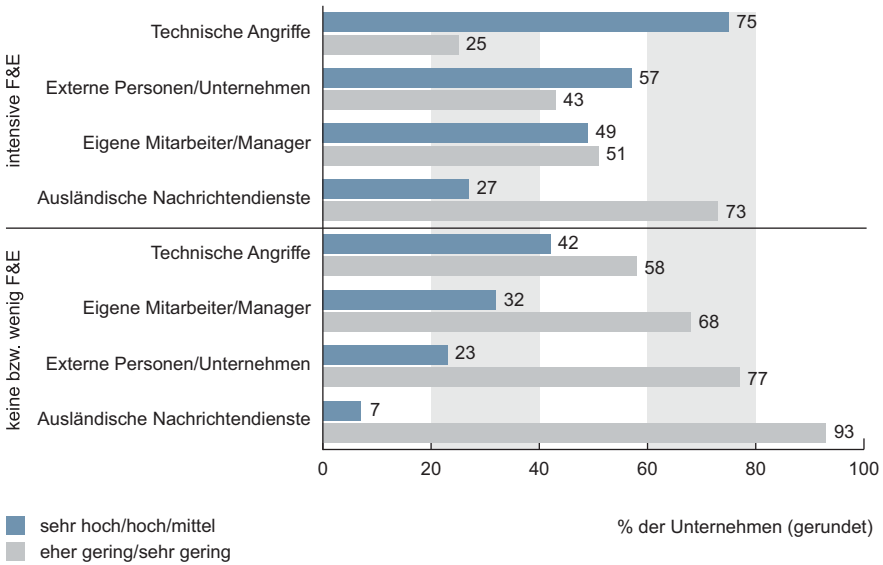


Abbildung 23: Erwartungen an den Tathergang bei erneuten Vorfällen

10.3 Schutz unternehmenssensibler Bereiche

Die Ergebnisse der Studie zeigen, dass die Hauptziele der Täter in den Geschäftsbereichen Forschung und Entwicklung sowie Produktion und Fertigung liegen. Dies gilt vor allem für forschungsintensive Unternehmen. Vergleichsweise selten waren die Bereiche Einkauf und Vertrieb, Marketing und Werbung ebenso wie die Personalabteilung betroffen. Insbesondere bei Unternehmen mit sensiblem Know-how wären daher besonders hohe Sicherheitsstandards im Bereich Forschung und Entwicklung zu erwarten. Dies ist jedoch in der Realität nicht der Fall, wie die Befragten einräumen.

So sind auch bei forschungsintensiven Unternehmen die höchsten Schutzstandards im Bereich Personal und Finanzen sowie in der Geschäftsleitung anzutreffen. Nur 58 % der Befragten berichten, dass sie den für sie besonders wichtigen Bereich Forschung und Entwicklung auch entsprechend intensiv schützen. 7 % bezeichnen ihren Schutz hier nur als schwach. Noch schlechter fällt bei den forschungsaktiven Unternehmen das Ergebnis für Produktion und Fertigung aus. Nur jedes dritte Unternehmen schützt

diesen Bereich intensiv; 20 % bewerten ihren Schutz hier sogar als schwach bzw. fast nicht vorhanden. Im Gegensatz dazu wird dem Schutzbedürfnis in den Bereichen Personalabteilung und -management, Finanzabteilung sowie Geschäftsleitung und Unternehmenspolitik besser Rechnung getragen.

Fazit ist, dass weder im Allgemeinen noch bei Unternehmen, die im besonderen Maße vom Schutz ihres geistigen Eigentums abhängen, diese Bereiche ausreichend geschützt werden. Bereits aufgrund der Selbsteinschätzung der Befragten können nur bei etwa der Hälfte der besonders gefährdeten Unternehmen die Sicherheitsmaßnahmen als gut bewertet werden.

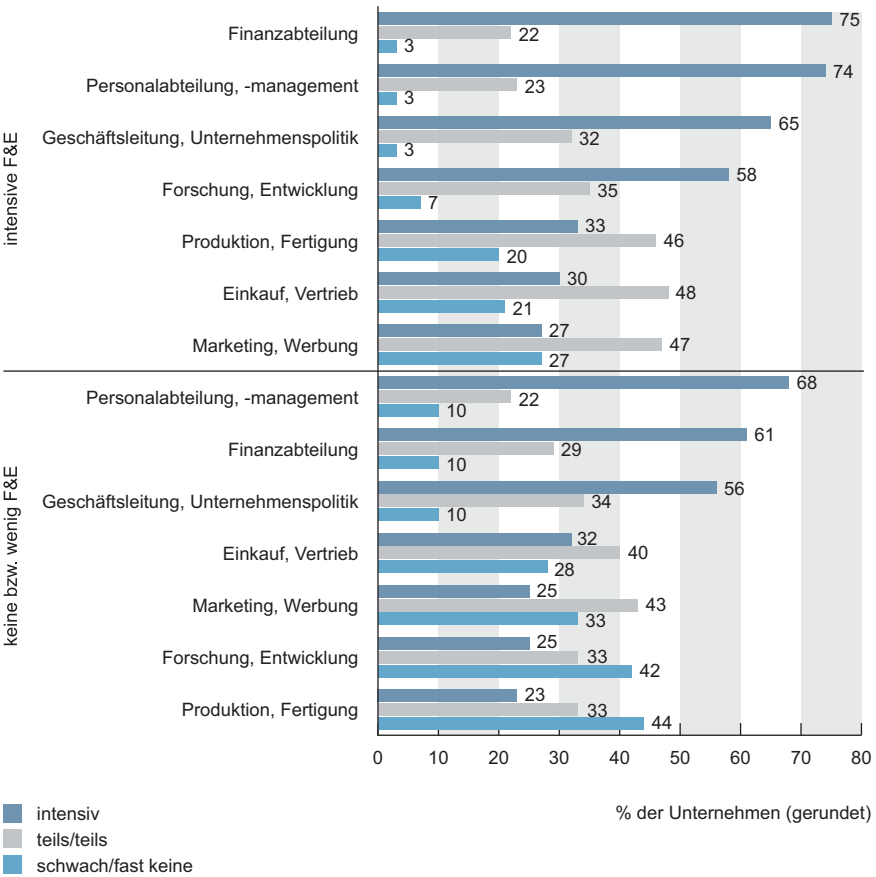


Abbildung 24: Schutzmaßnahmen in sensiblen Unternehmensbereichen

10.4 Vorhandene Maßnahmen im Bereich Objekt- und IT-Sicherheit

Die Studie geht sowohl auf die in den Unternehmen bereits implementierten Präventions- und Sicherheitsmaßnahmen im Bereich Objekt- und IT-Sicherheit als auch auf jene im Bereich Personal und Geschäftsabläufe ein. Entsprechend ihrer erhöhten Risiken, Opfer von Wirtschafts- und Industriespionage zu werden, schützen sich forschungsintensive Unternehmen häufiger und vielfältiger als Unternehmen mit weniger intensiver Forschung.

Der Schwerpunkt der Schutzmaßnahmen liegt bei der Objekt- und IT-Sicherheit. Hier dominieren Zugangskontrollen zum und auf dem Unternehmensgelände sowie Schutzkonzepte für IT- und Telekommunikationssysteme. Jedoch schützt jedes vierte forschungsintensive Unternehmen seine Zugänge nicht. Die meisten Unternehmen verfügen aus ihrer Sicht über einen besonders geschützten Serverbereich sowie über Passwortschutz auf allen Geräten. Hierbei handelt es sich eigentlich um Selbstverständlichkeiten. Allerdings fehlen bei vielen forschungsintensiven Unternehmen zeitgemäße Maßnahmen, die Tätern deutlich höhere Hürden bieten und somit die Risiken von Fehlverhalten minimieren könnten. So besteht nur bei etwa der Hälfte dieser besonders gefährdeten Unternehmen eine Segmentierung von Daten nach Gefährdung (49 %) sowie eine Verschlüsselung von Daten, Netzen und des E-Mail-Verkehrs (55 %). 44 % der nicht forschungsintensiven Unternehmen überwachen besonders sensible Bereiche gar nicht.

Im Bereich der Unternehmenssicherheit ist zudem die stärkste Entwicklung erkennbar. Jedes fünfte der besonders bedrohten Unternehmen beabsichtigt beispielsweise Verschlüsselungstechniken einzuführen (20 %).

Kaum Anwendung finden auch bei dieser Gruppe der gefährdeten Unternehmen regelmäßige Lauschabwehrprüfungen von Räumen (3 %) oder Abhörschutz für Telekommunikationsanlagen (7 %).

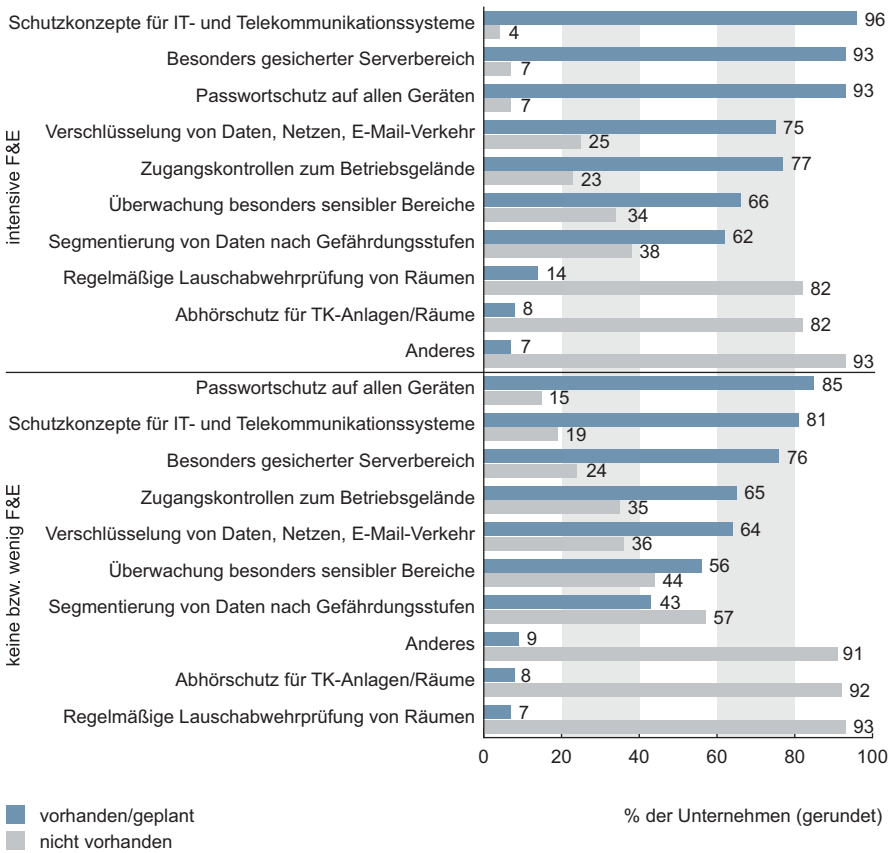


Abbildung 25: Schutzmaßnahmen im Bereich Objekt- und IT-Sicherheit

10.5 Vorhandene Maßnahmen im Bereich Personal und Geschäftsabläufe

Gegenüber dem Schutz im Objekt- und IT-Bereich fallen die Anstrengungen zur Prävention im Bereich Personal und Geschäftsabläufe deutlich geringer aus. Hier zeigt sich, dass die Risiken unterschätzt werden, die von Unternehmensangehörigen ausgehen, denn die größte Tätergruppe stammt aus dem eigenen Unternehmen, wie die Ergebnisse der Studie zeigen (siehe Kap. 9.3).

Die forschungsintensiven Unternehmen als besonders gefährdete Gruppe optimieren ihre aktuellen Sicherheitsstandards im Bereich Personal und Geschäftsabläufe. Jedoch erreichen sie nach wie vor nicht das Niveau der Standards im Bereich Objekt- und IT-Sicherheit. Die Mehrheit der Unternehmen verfügt über Wettbewerbs- und Geheimhaltungsklauseln in Arbeitsverträgen sowie über einen Verhaltenskodex. Da die erforderlichen Schulungsmaßnahmen und fallpraktischen Übungen in den entsprechenden Abteilungen jedoch überwiegend fehlen, drohen die eingeführten formalen Regeln an der Akzeptanz zu scheitern.

Nur jedes zweite Unternehmen stellt sicher, dass sensibles Wissen nur relevanten Mitarbeitern bekannt ist. Bei den forschungsintensiven Unternehmen ist dieser Anteil mit 68 % höher. Nicht alle Unternehmen nutzen zudem ethische Richtlinien oder Verhaltenskodizes, um mangelndem Wertebewusstsein entgegenzuwirken und den Mitarbeitern den Umgang mit sensiblen Informationen zu verdeutlichen. Am häufigsten wird hiervon bei forschungsintensiven Unternehmen Gebrauch gemacht (72 %).

Bedenklich ist außerdem: Schulungen zur Sensibilisierung der Mitarbeiter zum Thema Schutz von Unternehmens-Know-how sind nur bei 52 % der forschungsintensiven Unternehmen vorhanden und nur jedes Dritte dieser Unternehmen besitzt ein Hinweisgebersystem. Immerhin verwenden zwei von drei der besonders gefährdeten Unternehmen das „Need-to-know-Prinzip“ (68 %), d. h. die Unternehmensangehörigen erhalten die für die unmittelbare Erfüllung ihrer Aufgaben notwendigen Informationen, bzw. planen es einzuführen. Allerdings ist dies bei den Unternehmen, die nicht zu den forschungsintensiven zählen, nur bei 46 % der Fall.

Eine weitere wichtige Gruppe, die in das Sicherheitskonzept des Unternehmens eingebunden werden sollte, sind die Geschäftspartner. Immerhin stellen sie die zweitgrößte Gruppe der potenziellen Täter dar. Bei den wenigsten Tätern handelte es sich um Personen, zu denen keine Geschäftsbeziehungen bestanden haben. Bei weniger als der Hälfte der Unternehmen mit besonders schutzbedürftigem Know-how (45 %) erfolgt eine derartige Einbeziehung. Zu wenig verbreitet sind überdies auch in dieser Unternehmensgruppe Risikoanalysen von Geschäftspartnern (44 %) und eine Risiko- und Schwachstellenanalyse (46 %) im eigenen Unternehmen.

Eine derartige rationale Analyse der Risikogruppen bedeutet nicht, grundsätzlich jedem mit Misstrauen zu begegnen – weder gegenüber Unternehmensangehörigen noch Geschäftspartnern –, sondern auf gewisse Schutzvorkehrungen gegen Vertrauensmissbrauch nicht zu verzichten. Dieser Ansatz hat offenbar noch nicht Eingang in die Sicherheitskonzepte vieler Unternehmen gefunden. Selbst bei den besonders gefährdeten Unternehmen planen weniger als 10 % an diesen neuralgischen Punkten einen weiteren Ausbau.

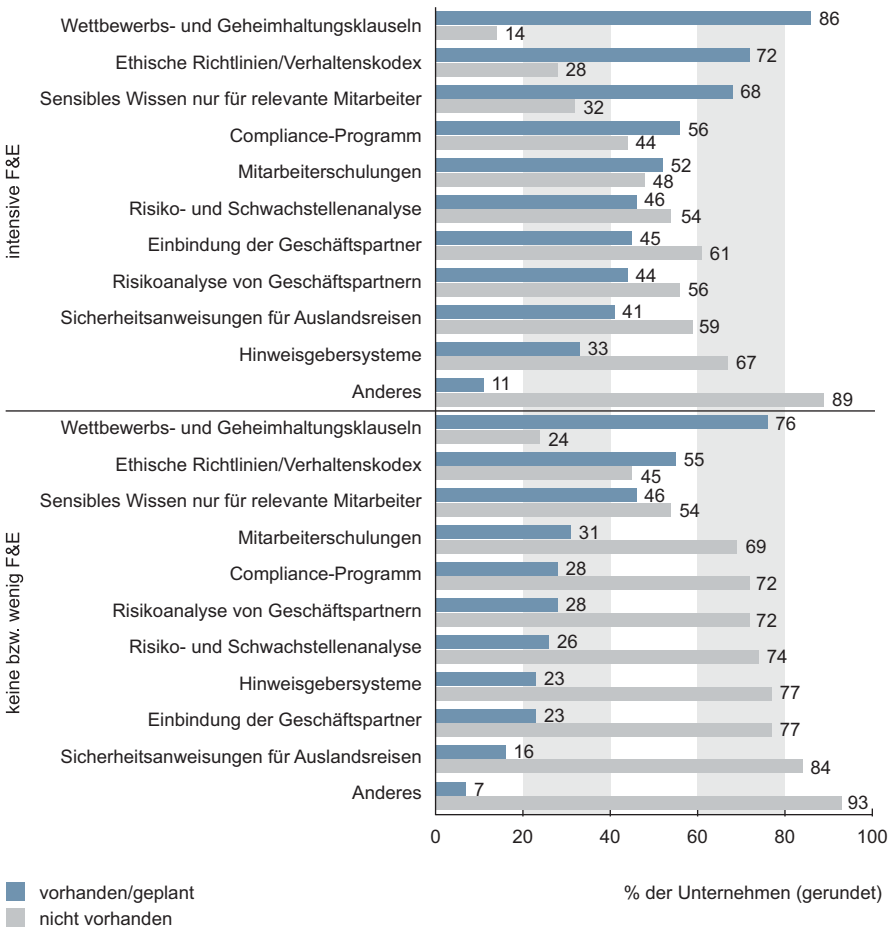


Abbildung 26: Schutzmaßnahmen im Bereich Personal und Geschäftsabläufe

10.6 Chancen der Präventionsmaßnahmen

Die wenigsten Unternehmen planen eine Verstärkung ihres Sicherheitskonzeptes. Diese Zurückhaltung erstaunt vor allem bei den forschungsintensiven Unternehmen, denn sie sind mehrheitlich der Auffassung, dass verbesserte Maßnahmen sowohl im Bereich Objekt- und IT-Sicherheit als auch im Bereich Personal und Geschäftsabläufe Angriffe auf sensibles Know-how und sensible Informationen erschweren könnten. Über zwei Drittel der forschungsintensiven Unternehmen (69 %) meinen, dass durch Verbesserungen im Bereich Objekt- und IT-Sicherheit Angriffe auf ihre Geschäfts- und Betriebsgeheimnisse erschwert oder auch verhindert werden könnten. Ein weiterer Ausbau der Schutzmaßnahmen wäre somit hier erforderlich. Zwar sehen sie eher die Notwendigkeit des verstärkten Schutzes von Gebäuden und ihrer IT- und Telekommunikationssysteme als in der Präventionsarbeit bei Unternehmensangehörigen und Externen, wie Geschäftspartnern und unternehmensbezogenen Dienstleistern. Gleichwohl besteht auch hier bei vielen ein Problembewusstsein. Vom Nutzen verstärkter Prävention im Bereich Personal und Geschäftsabläufe sind immerhin fast zwei Drittel der forschungsintensiven Unternehmen überzeugt (61 %).

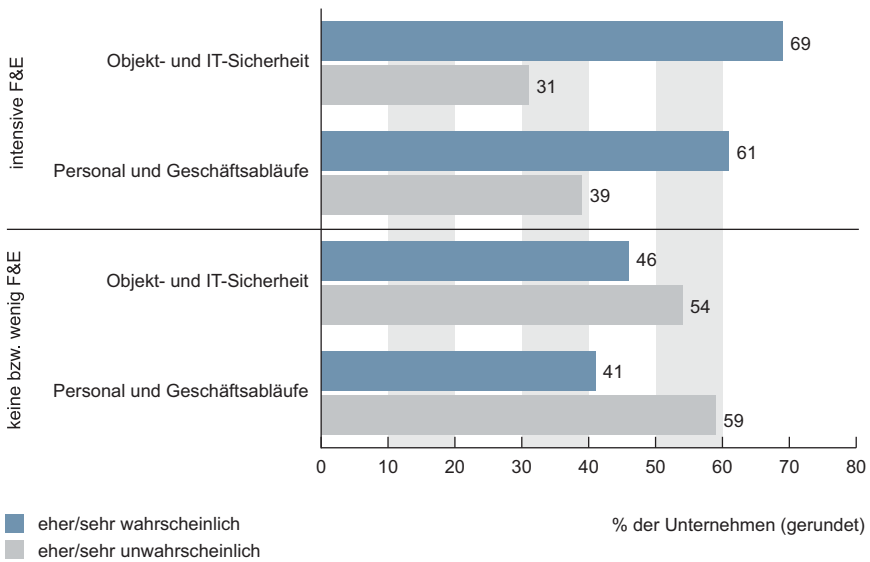


Abbildung 27: Wahrscheinlichkeit der Verstärkung von Sicherheitsmaßnahmen

10.7 Budget für Sicherheitsmaßnahmen

Erstaunlicherweise baut die Mehrheit der Unternehmen trotz des Bewusstseins, dass sie Opfer werden können, und der Auffassung, dass verbesserte Maßnahmen Angriffe auf sensibles Know-how und sensible Informationen erschweren könnten, ihre Schutzsysteme nicht aus. Positiv ist, dass Unternehmensausgaben für die Einführung von Sicherheitsstandards nicht sinken. Allerdings hat über die Hälfte der Unternehmen (65 %) in den letzten fünf Jahren ihr Budget im Bereich Objekt- und IT-Sicherheit nicht aufgestockt. Unverändert blieben in der Regel auch die Ausgaben für Prävention im Bereich Personal und Geschäftsabläufe (77 %).

Es muss an dieser Stelle offen bleiben, ob diese Zurückhaltung auch der gegenwärtigen, generell schwierigen wirtschaftlichen Lage geschuldet ist. Sollte dies der Fall sein, so wäre hierin gleichwohl keine empfehlenswerte Unternehmenspolitik zu sehen. Denn es ist mit einem weltweit sich weiter verschärfenden Wettbewerb zu rechnen. Dieser wird auch eine erhöhte Gefährdung unternehmenssensibler Informationen zur Folge haben. Ferner erhöht die gegenwärtig wachsende Sorge bei Mitarbeitern (unabhängig von Tätigkeit und Hierarchiestufe) um ihren Arbeitsplatz die Wahrscheinlichkeit von Wirtschaftsdelikten[19]. Damit steigt das Risiko von Angriffen auf Geschäfts- und Betriebsgeheimnisse durch interne Tätergruppen.

Es spricht somit viel dafür, dass die Zahl der Wirtschaftsdelikte in den nächsten Jahren eher ansteigt als abnimmt. Daher ist eine Intensivierung des Schutzes unternehmenssensibler Informationen von hoher Bedeutung.

19 Siehe die Ergebnisse der Umfrage zu den Auswirkungen der Wirtschaftskrise unter 500 deutschen Großunternehmen von PwC August 2009, http://www.pwc-wikri2009.de/ und Korruptionswahrnehmungsindex 2009 von Transparency International November 2009, http://www.transparency.de/Corruption-Perceptions-Index-2.1523.0.html, 22.01.2010.

Auch für die besonders gefährdete Gruppe der forschungsintensiven Unternehmen zeigt sich kein wesentlich besseres Bild. Bei kaum mehr als jedem Dritten dieser Unternehmen (39 %) erfolgte eine Erhöhung des Budgets für Sicherheitsmaßnahmen im Bereich Objekt- und IT-Sicherheit. Dies erscheint unabhängig von der gegenwärtigen Wirtschaftskrise nicht sachgerecht, da durch den globalen Wettbewerb die Kriminalitätsrisiken vermutlich steigen werden.

Auch eine Erhöhung des Budgets im Bereich Personal und Geschäftsabläufe ist selten vorgesehen (23 %). Dies erscheint in Anbetracht bestehender Risiken nicht adäquat. Wie bereits ausgeführt, erfolgen die häufigsten erfolgreichen Angriffe nicht im Bereich Objekt- und IT-Sicherheit, sondern im Bereich Personal und Geschäftsabläufe. Außerdem stammt die größte Gruppe der Täter aus dem eigenen Unternehmen (siehe Kap. 9.3).

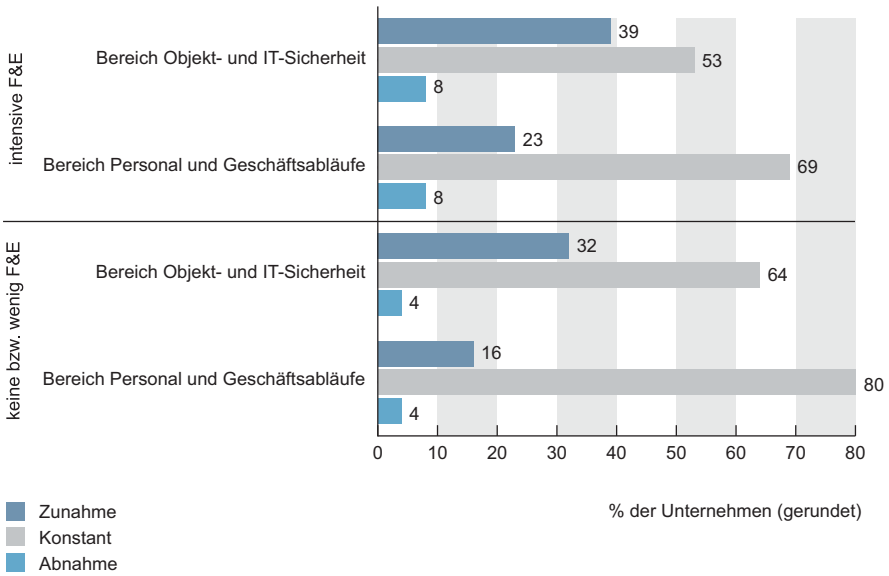


Abbildung 28: Budgetentwicklung im Bereich der Sicherheitsmaßnahmen

11 Beratungsangebote

Privatwirtschaft, Behörden und Verbände bieten eine Vielzahl an Hilfestellungen, von denen Unternehmen im Bedarfsfall Gebrauch machen können. Betroffenen Unternehmen steht damit durchaus eine große Bandbreite an Beratungsmöglichkeiten zur Verfügung, die sie stärker als in der Vergangenheit nutzen sollten. Bisherige Kenntnisse zu Handlungsoptionen würden dadurch verbessert und Netzwerke sinnvoll genutzt.

Diese Situation wirft die Frage auf, durch wen sich Unternehmen beraten und unterstützen lassen und wie zufrieden sie mit dem jeweiligen Beratungs- und Informationsangebot sind. Der Vergleich zeigt, dass private Anbieter besonders häufig in Anspruch genommen werden (64 %). Nur 30 % der Unternehmen geben an, das Beratungs- und Informationsangebot mindestens einer öffentlichen Einrichtung genutzt zu haben.

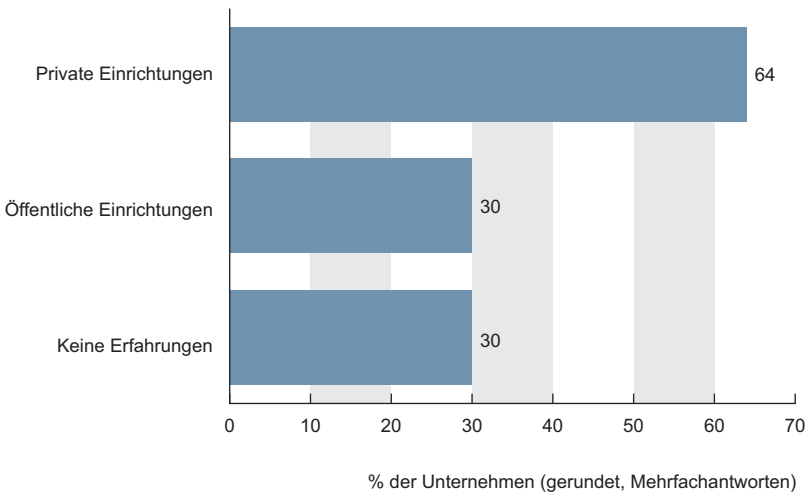


Abbildung 29: Inanspruchnahme von Beratungsangeboten

Der Vergleich zeigt, dass vor allem forschungsintensive Unternehmen das Beratungsangebot der öffentlichen und der privaten Einrichtungen nutzen. Unter den öffentlichen Anbietern wird zumeist das Bundesamt für Sicherheit in der Informationstechnologie in Anspruch genommen (34 %). Auf die Informationsangebote des Sicherheitsforums Baden-Württemberg wird ähnlich häufig wie auf diejenigen des Bundeskriminalamtes und des Landesamtes für Verfassungsschutz zugegriffen.

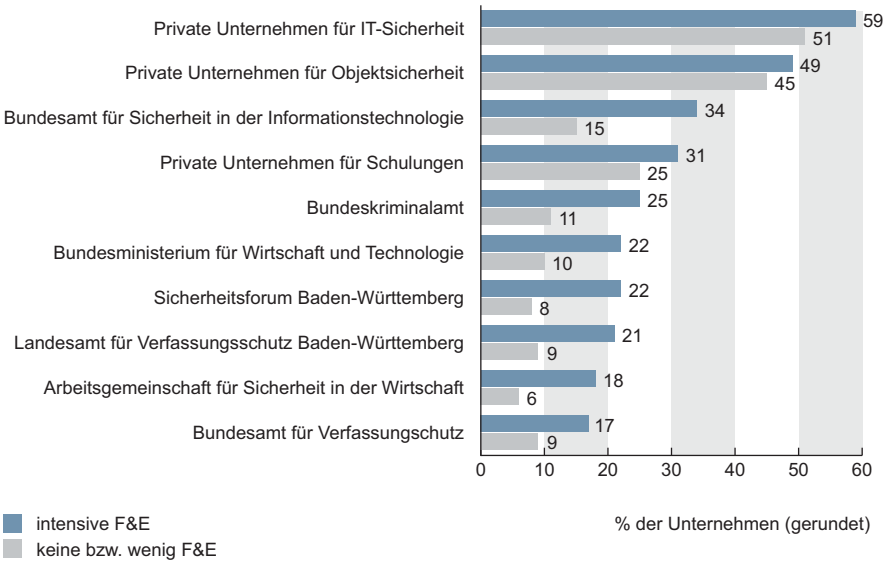


Abbildung 30: Nutzung von Beratungsanbietern

Von den wenigen Unternehmen, welche die Angebote der Behörden bereits in Anspruch genommen haben, empfinden nur ein Drittel dies als hilfreich. Allerdings wird der Nutzen von privaten und öffentlichen Beratungs- und Informationsangeboten ähnlich bewertet. Lediglich eine geringe Anzahl an Unternehmen neigt zu einem kritischen Urteil. Die Mehrheit tendiert zu einem „teils / teils“. Hierbei muss offen bleiben, ob dies auch in zu hohen Erwartungen begründet ist. Zweifellos sind bei der Zusammenarbeit zwischen den beteiligten Institutionen noch erhebliche Synergieeffekte zu erzielen.

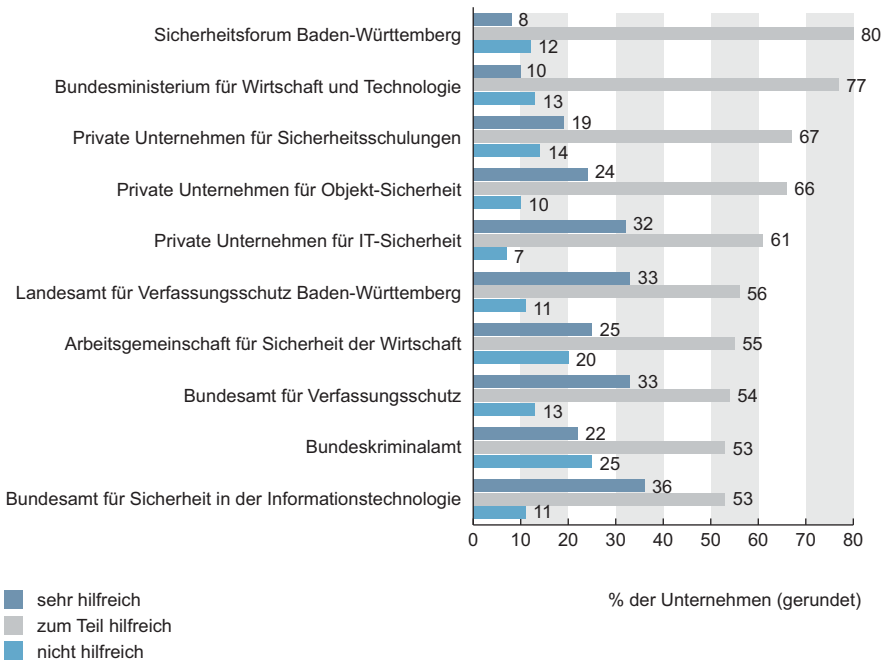


Abbildung 31: Erfahrungen mit Beratungsanbietern

Die Gründe für die Unterschiede in der Wahrnehmung der Betreuungsangebote sind vielfältig und wurden im Rahmen dieser Studie nicht erhoben. Zu vermuten ist, dass sich viele Unternehmen nicht der Möglichkeiten bewusst sind, die ihnen Behörden und Verbände bieten. Einen Überblick über die Angebote und die jeweiligen Ansprechpartner in einschlägigen Behörden und Verbänden bietet u. a. die gesonderte Publikation des Sicherheitsforums zu den Handlungsempfehlungen, die aus der Studie abgeleitet wurden.

Ein weiterer Grund für die Zurückhaltung bei der Inanspruchnahme von externen Beratungsstellen kann in der Sorge eines Reputationsverlustes liegen. Viele Unternehmen befürchten, dass Fälle von Industrie- und Wettbewerbsspionage in der Öffentlichkeit bekannt werden, es damit zu einem Reputationsverlust beim Kunden kommt und das Ansehen des Unternehmens darüber hinaus auch bei den Unternehmensangehörigen schwinden könnte.

12 Zusammenfassung

Die vorliegenden Ergebnisse machen deutlich, dass Urheberrechtsverletzungen und Spionage bzw. Informationsabfluss besonders in den forschungsintensiven Unternehmen realistische, aber noch unterschätzte Bedrohungen darstellen.

Über 60 % der forschungsintensiven Unternehmen hatten in den letzten vier Jahren mindestens einen eindeutigen Fall von Verstößen gegen Patent- und Markenrechte oder Gebrauchs- und Geschmacksmusterrechte und/oder einen konkreten Verdacht und immerhin 27 % einen Fall von Spionage bzw. Informationsabfluss zu verzeichnen.

Folge dieser Fälle waren für die Unternehmen gravierende Umsatzeinbußen, Beeinträchtigungen von Geschäftsbeziehungen und strategische Vorteile für Wettbewerber. Besonders Dauer und Kosten der Bearbeitung des Vorfalles stellten für die Unternehmen einen erheblichen bis sehr hohen Schaden dar. Dabei lagen die finanziellen Schäden zwischen unter 10.000 Euro bis über zwei Millionen Euro je Vorfall. Aus Sicht der Unternehmen ist das Risiko, in den nächsten Jahren Opfer von Verstößen gegen das Urheberrecht bzw. Opfer von Verrat von Geschäfts- und Betriebsgeheimnissen zu werden, weiterhin hoch.

Dem gegenüber stehen die Sicherheitsmaßnahmen zur Abwehr von Industrie- und Wirtschaftsspionage der Unternehmen und staatliche Organisationen und Verbände, die diese dabei unterstützen. Angesichts der auch in dieser Studie empirisch nachweisbaren Risiken wappnen sich viele Unternehmen zu wenig gegen Wirtschafts- und Industriespionage. So werden die Beratungsangebote staatlicher Organisationen und Verbände zu wenig genutzt. Oft wird das Know-how hierfür im eigenen Unternehmen aufgebaut oder es werden private Anbieter hinzugezogen. Im Bereich Objekt- und IT-Schutz haben viele der Unternehmen bereits Präventionsmaßnahmen ergriffen bzw. planen deren Einführung. Zwar werden auch im Bereich Personal und Geschäftsabläufe eine Reihe von Maßnahmen eingesetzt, aber gemessen an den hier bestehenden hohen Risiken wird dieser Bereich im Unterschied zum Objekt- und IT-Schutz immer noch zu sehr vernachlässigt. So fehlen bei den meisten Unternehmen Maßnahmen zur Einbindung der Unternehmensangehörigen in die eigene Philosophie sowie deren Sensibilisierung.

Als Ergebnis der „SiFo-Studie 2009/10“ werden daher neben der Datenerhebung und -auswertung in einer separaten Veröffentlichung Handlungsempfehlungen für die Unternehmen dokumentiert, die ihnen helfen sollen, Netzwerke zum Schutz vor Schäden aus dolosen Handlungen zu bilden und ihre eigenen Präventionsmaßnahmen zu optimieren.

13 Glossar

Betrug
Der Tatbestand des Wirtschaftsstrafrechts Betrug (§ 263 StGB) setzt einen Vermögensschaden voraus. Der Tatbestand Betrug enthält fünf Tatbestandsmerkmale, nämlich:
1. Täuschungshandlung
2. Irrtumserregung
3. Vermögensverfügung des Getäuschten (ungeschriebenes Tatbestandsmerkmal)
4. Vermögensschaden
5. Vorsatz

Dolose Handlungen
Dolose Handlungen beschreiben vermögensschädigende Taten zum Nachteil des Unternehmens. Strafrechtlich werden häufig die Tatbestände Unterschlagung, Betrug und Untreue erfasst.

Dunkelfeld
Der Begriff Dunkelfeld bezeichnet alle Delikte, die den Strafverfolgungsbehörden nicht bekannt geworden sind und somit nicht in den Kriminalstatistiken erfasst werden. Das Dunkelfeld kann durch die sogenannte Dunkelfeldforschung, z. B. durch Befragungen von Tätern und Opfern, teilweise erfasst bzw. erhellt werden. Man bezeichnet diesen Bereich als relatives Dunkelfeld. Die Bereiche, die weder durch die Kriminalstatistiken noch durch die Dunkelfeldforschung aufgehellt werden können, bezeichnet man als absolutes Dunkelfeld.

Forschungsintensive Unternehmen
Im Rahmen der Studie sind forschungsintensive Unternehmen diejenigen, die bei gegebener Auswahlmöglichkeit „viel, wenig, nein“ angegeben haben, dass sie am Betriebsstandort Baden-Württemberg viel Forschung betreiben.

Gesetzlicher Schutz von Know-how
Die zentrale Vorschrift zum Schutz von Know-how in Unternehmen findet sich in § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Unter Strafe gestellt ist die unbefugte Weitergabe von Geschäfts- oder Betriebsgeheimnissen an Dritte zu

Zwecken des Wettbewerbes, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, während der Geltungsdauer des Dienstverhältnisses (Abs. 1) und das Sichverschaffen oder Sichern eines Geschäfts- oder Betriebsgeheimnisses durch die Anwendung technischer Mittel, Herstellung einer verkörperten Wiedergabe des Geheimnisses oder Wegnahme einer Sache, in der das Geheimnis verkörpert ist (Abs. 2)[20].

Durch § 17 Abs. 2 Nr. 1 werden einige typische Begehungsformen der Wirtschaftsspionage erfasst. Bestraft wird, „[...] wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch

a) Anwendung technischer Mittel,
b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,

unbefugt verschafft oder sichert [...]“[21]. Mit der Anwendung von technischen Hilfsmitteln ist der TECHINT-Bereich erfasst, mit Punkt b) wird jede Verkörperung von Geheimnissen, z. B. Texte, Abschriften, Fotografien etc., erfasst und mit Punkt c) der Diebstahl bzw. die Wegnahme von Gegenständen, in denen das Geheimnis verkörpert ist, z. B. Muster oder Prototypen. Die Verletzung dieser Geheimnisse wird mit Freiheitsstrafe bis zu drei Jahren (§ 17 Abs. 1) und in besonders schweren Fällen mit bis zu fünf Jahren (§ 17 Abs. 4) oder Geldstrafe bestraft. Voraussetzung für eine strafrechtliche Würdigung ist, dass der Geheimnisverrat vorsätzlich begangen wurde. Der fahrlässige Verrat von Geschäfts- und Betriebsgeheimnissen, z. B. durch das versehentliche Verlieren von Dokumenten, fällt nicht unter § 17 UWG. Ebenso sind das Aneignen von Geheimnissen mittels Gedächtnisleistung und das Erlangen eines Geheimnisses durch die Befragung von Beschäftigten straffrei.

Der Schutz von Patenten und Gebrauchsmustern ist in den gesetzlichen Bestimmungen der § 50 ff. Patentgesetz (PatG) sowie § 9 Gebrauchsmustergesetz (GebrMG) geregelt.

20 Gesetz gegen den unlauteren Wettbewerb vom 03. Juli 2004 (BGBl. I S. 1414), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. Dezember 2008 (BGBl. I S. 2949).
21 Gesetz gegen den unlauteren Wettbewerb vom 03. Juli 2004 (BGBl. I S. 1414), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. Dezember 2008 (BGBl. I S. 2949).

Hellfeld
Der Begriff Hellfeld bezeichnet die den Straf- und Ermittlungsbehörden bekannt gewordenen bzw. registrierten Straftaten. Auskunft über das Hellfeld geben die polizeilichen Kriminalstatistiken, wie zum Beispiel die Polizeiliche Kriminalstatistik des Bundeskriminalamtes.

Information Technology Experts
Diese Personen sind versierte Computer-Hacker bzw. arbeiten mit solchen zusammen und beschaffen Informationen aus fremden Computersystemen.

Intelligence Trader
Unternehmen, die sich als Informationshändler, Sicherheitsberater oder Detekteien bezeichnen und von Unternehmen beauftragt werden, Informationen auf dem illegalen Weg zu beschaffen. Neben diesen Leistungen bieten diese Unternehmen auch noch legale Sicherheitsberatungen, Implementierungen von Sicherheitskonzepten aber auch die Beschaffung von Informationen mit Hilfe eigener bzw. freier Mitarbeiter an.

Know-how
Know-how bezeichnet die „Kenntnisse und Erfahrungen technischer, kaufmännischer, administrativer, finanzieller oder anderer Natur, die im Betrieb eines Unternehmens oder in der Ausübung eines Berufes praktisch anwendbar sind“[22] und ist somit von der Art des schützenden Guts synonym zu den Begriffen Geschäfts- und Betriebsgeheimnis zu verwenden.

Need-to-know-Prinzip
Nach dem Need-to-know-Prinzip werden jedem Mitarbeiter die Informationen zur Verfügung gestellt, die zur Erfüllung seiner Aufgaben notwendig sind. Es findet besonders bei der Vergabe von Zugangsberechtigungen im IT-Bereich Anwendung.

Social Engineering
Das als Social Engineering bezeichnete Vorgehen ist eine Methode, um durch das Ausnutzen menschlicher Eigenschaften, wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt und Autorität, unberechtigten Zugang zu Informationen

22 Fink, Kerstin: Know-how-Management, Oldenbourg Verlag, München, 2000.

und informationstechnischen Systemen zu erlangen. Meistens werden Mitarbeiter des auszuspähenden Unternehmens manipuliert, um unzulässige Handlungen durchzuführen, die zu einer Informationsweitergabe führen.

Untreue

Wer über fremdes Vermögen verfügt und die ihm auferlegte Pflicht missbraucht oder fremde Vermögensinteressen wahrnimmt und diese verletzt bzw. einen Nachteil zufügt, wird bestraft. Der Tatbestand Untreue (§ 266 StGB) erschöpft sich somit nicht in der Pflichtverletzung, sondern erfordert den Eintritt eines Vermögensschadens, der als „Nachteil“ bezeichnet wird.

Whistleblowing

Whistleblowing bezeichnet die Weitergabe von Verstößen innerhalb eines Unternehmens an interne oder externe Stellen.

14 Daten und Fakten zur Studie

Auftraggeber

- Sicherheitsforum Baden-Württemberg

Unterstützt von

- Steinbeis-Stiftung für Wirtschaftsförderung
- Baden-Württembergischer Industrie- und Handelskammertag

Durchgeführt von

- Ferdinand-Steinbeis-Institut
- School of Governance, Risk & Compliance an der Steinbeis-Hochschule Berlin

Zeitrahmen

Februar 2009 bis Dezember 2009

Methodik

Befragung in Form eines standardisierten Online-Fragebogens

Teilnehmer der Befragung

Baden-Württembergische Unternehmen aus folgenden Branchen

- verarbeitendes Gewerbe
- Baugewerbe
- Handel
- Verkehr und Lagerei
- Information und Kommunikation
- Erbringer von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen

Hintergrund zur Studie

- Zum Teil geringes bis mangelndes Bewusstsein für Wirtschaftsspionage und Konkurrenzausspähung in den Unternehmen
- Deutlichere Definition der realistischen Gefährdungslage
- Praxisbezogene Handlungsempfehlungen für die Unternehmen

Thema der Befragung

- Informationen zum derzeitigen Know-how-Schutz in den Unternehmen
- Konkrete Fragen zum Bewusstsein und zu (potenziellen) eigenen Schädigungen des Unternehmens
- Basisdaten Unternehmen

15 Hintergrundinformation

Im **Sicherheitsforum Baden-Württemberg** haben sich Unternehmen, das Innenministerium und das Wirtschaftsministerium Baden-Württemberg, das Landesamt für Verfassungsschutz Baden-Württemberg, der Baden-Württembergische Handwerkstag (BWHT), der Landesverband der Baden-Württembergischen Industrie e. V. (LVI), der Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V. (VSW), der Baden-Württembergische Industrie- und Handelskammertag, der Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA) Baden-Württemberg sowie das Karlsruher Institut für Technologie (KIT) und die Steinbeis-Stiftung zusammengeschlossen, um die Wirtschaft in Baden-Württemberg vor Wirtschafts- und Industriespionage zu schützen.
www.sicherheitsforum-bw.de

Die **Steinbeis-Stiftung** ist ein weltweit tätiges Dienstleistungsunternehmen im Bereich Technologie- und Wissenstransfer. Zum dezentral organisierten Steinbeis-Verbund gehören derzeit rund 800 rechtlich unselbstständige wie auch selbstständige Steinbeis-Unternehmen sowie Kooperations- und Projektpartner in 50 Ländern, die in den Bereichen Forschung und Entwicklung, Beratung, Analysen und Expertisen sowie Aus- und Weiterbildung tätig sind.
www.stw.de

Das **Ferdinand-Steinbeis-Institut** ist ein Transferzentrum in der Steinbeis-Stiftung und hat die Aufgabe der Koordination und Durchführung von wissenschaftlichen Studien im Steinbeis-Verbund. Der für das Projekt verantwortliche Leiter ist Max Pfeiffer.
www.fsti.info

Die **School of Governance, Risk & Compliance (School GRC)** ist ein Forschungs- und Ausbildungsinstitut der privaten Steinbeis-Hochschule Berlin. Sie bildet Führungskräfte und Spezialisten aus und fort. Die an der School GRC durchgeführten Studien und Forschungen sind bewusst praxisnah ausgerichtet mit dem Ziel, Nutzwert in Branchen, Betrieben und Verbänden zu erzeugen. Die für das Projekt verantwortliche Direktorin der School GRC ist Birgit Galley.
www.school-grc.de

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
Abs.	Absatz
ASW	Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V.
Aufl.	Auflage
Bd.	Band
BFuP	Zeitschrift für Betriebswirtschaftliche Forschung und Praxis
BGBl	Bundesgesetzblatt
BMBF	Bundesministerium für Bildung und Forschung
BVerfG	Bundesverfassungsgericht
BvR	Aktenzeichen einer Verfassungsbeschwerde zum BVerfG
BW	Baden-Württemberg
BWHT	Baden-Württembergischer Handwerkstag
bzw.	beziehungsweise
CD	Compact Disc

COMPINT	COMPuter INTelligence
d. h.	das heißt
DATAINT	DATA INTelligence
DECT	Digital Enhanced Cordless Telecommunications
etc.	et cetera
F&E	Forschung und Entwicklung
ff.	fortfolgende
GebrMG	Gebrauchsmustergesetz
GeschmMG	Geschmacksmustergesetz
GRC	Governance, Risk & Compliance
GSM	Global System for Mobile Communications
Hrsg.	Herausgeber
HUMINT	HUMan INTelligence
IT	Informationstechnik
Kap.	Kapitel
KIT	Karlsruher Institut für Technologie
LVI	Landesverband der Baden-Württembergischen Industrie e. V.
MAD	Militärischer Abschirmdienst

MarkenG	Markengesetz
MschrKrim	Monatsschrift für Kriminologie und Strafrechtsreform
Nr.	Nummer
OECD	Organisation for Economic Co-operation and Development
OSINT	Open Source INTelligence
PatG	Patentgesetz
PDA	Personal Digital Assistant
PwC	PricewaterhouseCoopers
Rdn.	Randnotiz
S.	Seite
SiFo	Sicherheitsforum
StGB	Strafgesetzbuch
Tab.	Tabelle
TECHINT	TECHnical INTelligence
u. a.	unter anderem
USA	United States of America
USB	Universal Serial Bus
usw.	und so weiter

UWG	Gesetz gegen den unlauteren Wettbewerb
VDMA	Verband Deutscher Maschinen- und Anlagenbau e. V.
VoIP	Voice over Internet Protocol
VSW	Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V.
WLAN	Wireless Local Area Network
z. B.	zum Beispiel
zfwu	Zeitschrift für Wirtschafts- und Unternehmensethik
ZRFC	Zeitschrift für Risk, Fraud & Compliance

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

www.sicherheitsforum-bw.de

Baden-Württemberg
INNENMINISTERIUM

Baden-Württemberg
WIRTSCHAFTSMINISTERIUM

Baden-Württemberg

IHK Die Industrie- und Handelskammern in Baden-Württemberg

VSW

LVI
Landesverband der Baden-Württembergischen Industrie e. V.

VDMA

KIT
Karlsruher Institut für Technologie

DAIMLER

EnBW

SAP

BWHT

Steinbeis

ISBN 978-3-941417-20-5

Steinbeis-Edition