Esther Bollhöfer, Angela Jäger

Wirtschaftsspionage und Konkurrenzausspähung

Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung

Esther Bollhöfer
Angela Jäger

Wirtschaftsspionage und Konkurrenzausspähung

Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung im Zuge der Bekanntmachung "Zivile Sicherheit – Schutz vor Wirtschaftskriminalität" des BMBF im Rahmen des Programms "Forschung für die zivile Sicherheit" der Bundesregierung unter dem Förderkennzeichen 13N13410 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autorinnen.

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Freiburg i.Br.

Reihe A: Arbeitsberichte

Herausgegeben von Hans-Jörg Albrecht und Ulrich Sieber

Band A 8 09/2018

Mit der Reihe „Arbeitsberichte" aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht sollen wichtige Forschungsergebnisse, auch aus noch laufenden Projekten, zeitnah einem breiten Fachpublikum zugänglich gemacht werden. Sie dient als ergänzendes Publikationsforum zu den Buchreihen „Kriminologische Forschungsberichte", „Strafrechtliche Forschungsberichte" und „Interdisziplinäre Forschungsberichte".

The series "Working Papers" is designed to make significant findings of the Max Planck Institute for Foreign and International Criminal Law – including results of ongoing research projects – immediately accessible to a broad range of experts in the field. The series supplements the book series "Reports on Research in Criminology", "Reports on Research in Criminal Law" and "Interdisciplinary Research".

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.deabrufbar.

Foto: Pixabay

Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim

ISBN 978-3-86113-270-7

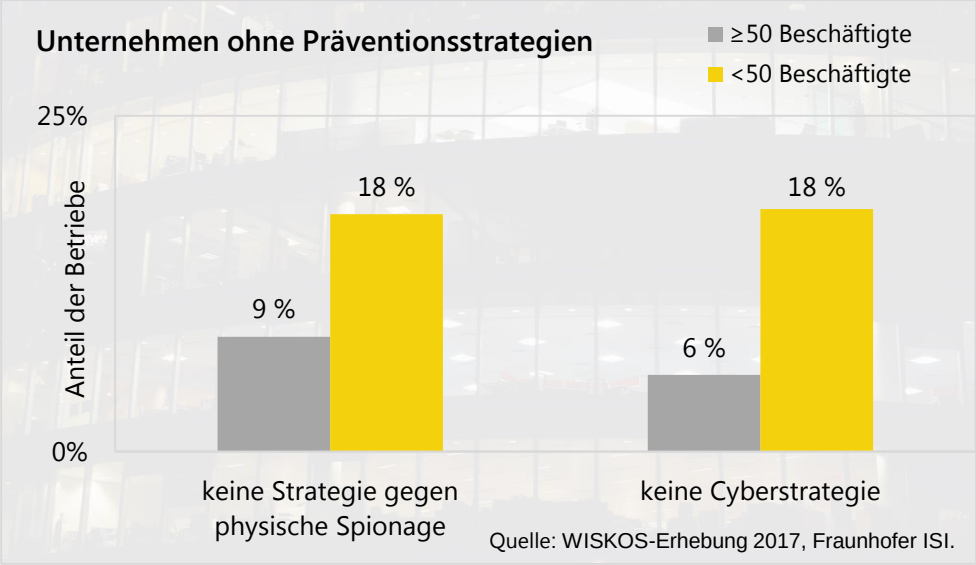
https://doi.org/10.30709/978-3-86113-270-7

Inhalt

Executive Summary

Viele mittelständische Unternehmen verzeichneten in den vergangenen Jahren Schäden durch Fälle von Wirtschaftsspionage und Konkurrenzausspähung. Noch wesentlich mehr Fälle blieben unentdeckt oder wurden von den Unternehmen nicht angezeigt oder veröffentlicht. Schäden, die über die Tages- und Fachpresse veröffentlicht wurden, und Warnungen der Behörden haben den Mittelstand sensibilisiert, so dass er die Prävention durch Einzelmaßnahmen verbessert hat. Doch weiterhin fehlt es gerade bei den kleinen Unternehmen an Präventionsstrategien: Jedes fünfte Unternehmen mit weniger als 50 Beschäftigten hat keine Strategie gegen physische Spionage, nur wenige mehr verfügen über eine Präventionsstrategie gegen Cyberspionage (s. Abbildung 1).

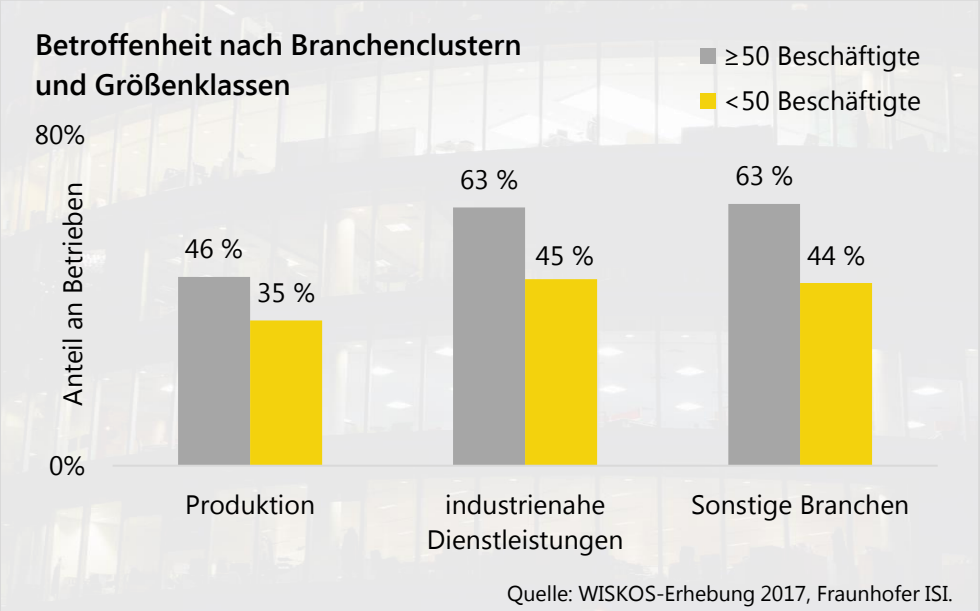
Abbildung 1: Fehlende Präventionsstrategien bei Industrieunternehmen



Über alle Branchencluster hinweg gibt ungefähr jedes zweite Unternehmen an, bereits von einem Vorfall betroffen gewesen zu sein oder zumindest einen Verdacht zu haben, dass bereits ein Angriffsversuch stattgefunden hat (s. Abbildung 2). Darüber hinaus ist von einer hohen

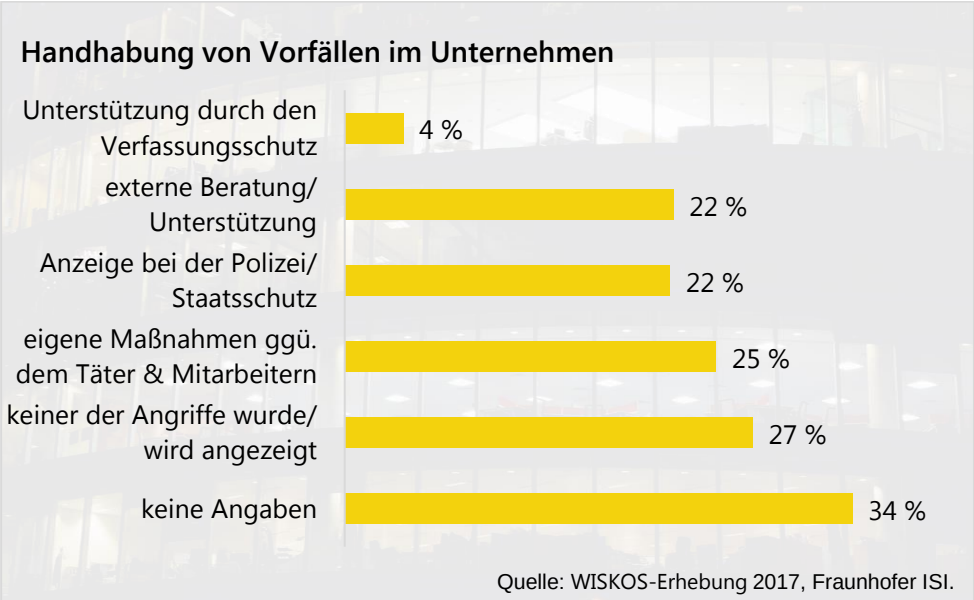
Dunkelziffer auszugehen, die sich aus mehreren Komponenten zusammensetzt: (a) Unternehmen bemerken Vorfälle gar nicht oder sehr verspätet. Dies liegt u.a. an fehlenden Präventionsmaßnahmen und fehlender Beobachtung von typischen Indikatoren. (b) Vorfälle werden einem anderen Kontext zugeschrieben (z.B. Einbruch, Diebstahl); (c) Vorfälle werden im Unternehmen mangels direktem Schaden nicht kommuniziert (vor allem im Cyber-Bereich); (d) Vorfälle werden bewusst nicht nach außen kommuniziert.

Abbildung 2: Betroffenheit durch Wirtschaftsspionage oder Konkurrenzausspähung



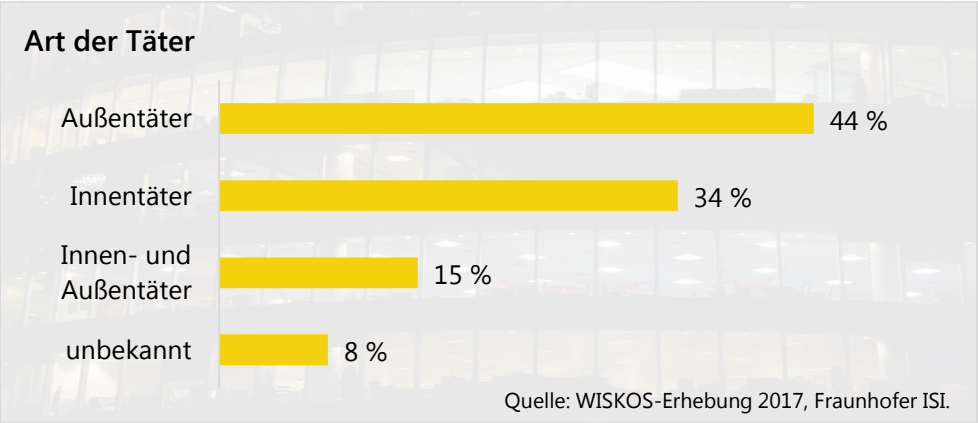
Die Größe des Dunkelfelds lässt sich nur schwer beziffern. Die Erhebung hat aber gezeigt, dass die Unternehmen, die überhaupt über ihre Betroffenheit Auskunft geben, nur in jedem fünften Fall Anzeige bei den Behörden erstatten (s. Abbildung 3). In der Mehrheit der Fälle ziehen die Unternehmen es vor, eigene Maßnahmen gegenüber dem Täter zu treffen (25 Prozent) und/oder externe Dienstleister zu beauftragen (22 Prozent).

Abbildung 3: Handhabung von Vorfällen im Unternehmen



Der Mittelstand hat dabei gleich an mehreren Fronten zu kämpfen: Die Bedrohung durch Spionage besteht gleichermaßen von innen wie von außen. Unzufriedene und ehemalige Beschäftigte hatten bzw. haben Zugang zu Informationen, der nur in einem eingeschränkten Rahmen zu kontrollieren ist. Neue Beschäftigte werden nur selten unter Sicherheitsgesichtspunkten überprüft, Praktikanten und Beschäftigte von Drittunternehmen erhalten oftmals sorglos Zugang zu schützenswertem Know-how. So ist dann auch der hohe Anteil an Innentätern zu erklären (s. Abbildung 4). Trotzdem werden weiterhin Angriffe von außen als deutlich gefährlicher eingeschätzt. Begründet sein mag dies durch die zunehmende Digitalisierung und den damit einhergehenden Möglichkeiten der Cyberspionage. Zudem bleiben sowohl der Ursprung wie auch die Ziele der Angreifer bei Vorfällen oftmals unklar. Ein Angriff eines Freizeit-Hackers (mit dem "kleinen" Ziel zu stören) ist anhand seiner äußeren Merkmale kaum von einem gezielten Angriff auf bestimmte Daten (mit dem Ziel zu manipulieren oder zu übermitteln) zu unterscheiden.

Abbildung 4: Bedrohung aus mehreren Richtungen



Einfache Maßnahmen könnten die Situation jedoch schnell verbessern. Dazu gehören bisher nur wenig genutzte Präventionsmaßnahmen wie z.B. spezielle Maßnahmen und Regeln für Fremd-, Leasing- und sonstiges Personal, regelmäßige Überprüfung der Sicherheitsmaßnahmen durch Tests, Verschlüsselung von E-Mails und Vereinbaren von Regeln zur Nutzung privater Geräte (BYOD) und zum Umgang mit sonstigen Datenträgern.

Interessanterweise gibt jedes vierte betroffene Unternehmen an, dass der Vorfall im Zusammenhang mit dem Einsatz privater Geräte steht – trotzdem werden auf diesem Gebiet nur selten Maßnahmen getroffen: Bei den Mittelständlern mit 50 und mehr Beschäftigten sind es immerhin 30 Prozent, bei den Unternehmen mit weniger als 50 Beschäftigten sind es nur bedenklich niedrige 14 Prozent.

Insbesondere in kleinen Unternehmen mangelt es zudem an einer physikalischen Trennung der Netze, so dass hier die Tore für Cyberkriminalität offenstehen. Auch entsprechen die IT-Sicherheitsmaßnahmen nur in wenigen Fällen den aktuellen Standards. Hier sind Investitionen in die Prävention dringend erforderlich.

Einleitung

1 Einleitung

Viele mittelständische Unternehmen verzeichneten in den vergangenen Jahren Schäden durch Fälle von Wirtschaftsspionage und Konkurrenzausspähung. Vermutlich blieben noch wesentlich mehr Fälle unentdeckt oder wurden von den Unternehmen nicht angezeigt oder veröffentlicht. Schäden, die über die Tages- und Fachpresse veröffentlicht wurden, und Warnungen der Behörden haben den Mittelstand sensibilisiert, so dass er die Prävention durch Einzelmaßnahmen verbessert hat. Dennoch bleibt das Feld weit offen: Die Digitalisierung bringt nicht nur große Potenziale mit sich, sondern auch neue Risiken, gerade auf dem Gebiet des Informationsschutzes.

Für die kleinen und mittelständischen Unternehmen bedeutet dies, in die Prävention zu investieren und Strategien zu entwickeln. Dazu bedarf es zum einen einer systematischen Beobachtung der Bedrohungslage, einer fortlaufenden Information über die Präventionsmöglichkeiten und idealerweise des Anschlusses an ein Experten-Netzwerk, um voneinander zu lernen und im Schadensfall richtig und schnell zu reagieren.

Die vorliegende Studie ist ein Ausschnitt aus dem Projekt WISKOS und liefert, basierend auf zwei quantitativen Erhebungen, ein Bild über den aktuellen Status Quo bei kleinen und mittelständischen Unternehmen sowie Handlungsansätze für Präventionsstrategien.

Den Befragungen voraus gingen Länderanalysen[1] innerhalb der EU und in der Schweiz in Bezug auf Strafverfolgung und regionale Besonderheiten. Im Anschluss an die Selektion von Vergleichsländern (England, Dänemark, Bulgarien, Österreich, Schweiz) erfolgte die Analyse exemplarischer Fälle mit dem Ziel, Handlungsansätze zu identifizieren, gefundenen Ansätze und der Status Quo von Präventionsmaßnahmen und Bedrohungswahrnehmung wurden im Anschluss mit Experten aus der Industrie, den Wissenschaftsorganisationen und den Behörden in

Deutschland diskutiert.[2] Parallel dazu wurde der aktuelle Stand im Rahmen einer repräsentativen quantitativen Befragung im Verarbeitenden Gewerbe 2015 (Befragung *Modernisierung der Produktion* 2015, Fraunhofer ISI, N=1.282) erhoben (s.u. Kapitel 2). Als letzter Baustein folgte eine projektspezifische Unternehmensbefragung bei produzierenden kleinen und mittelständischen Unternehmen sowie bei industrienahen Dienstleistern, an der 583 Unternehmen teilnahmen (s.u. Kapitel 3).

Die Ergebnisse bieten nicht nur Handlungsansätze für Unternehmen, sie ermöglichen es auch den Behörden, die Bedarfe der Unternehmen besser kennenzulernen und darauf Kooperationen aufzubauen, um dem staatlichen Auftrag der Gefahrenprävention besser nachkommen zu können.

1 | *Carl, S. & Kilchling, M.* (Hrsg.): Economic and Industrial Espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin 2018 (Duncker & Humblot).

2 | *Wallwaey, E., Bollhöfer, E. & Knickmeier, S.* (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin 2018 (Duncker & Humblot).

Vorfälle und Verdachtsfälle im Verarbeitenden Gewerbe: Repräsentative Ergebnisse und deren Limitationen

2 Vorfälle und Verdachtsfälle im Verarbeitenden Gewerbe: Repräsentative Ergebnisse und deren Limitationen

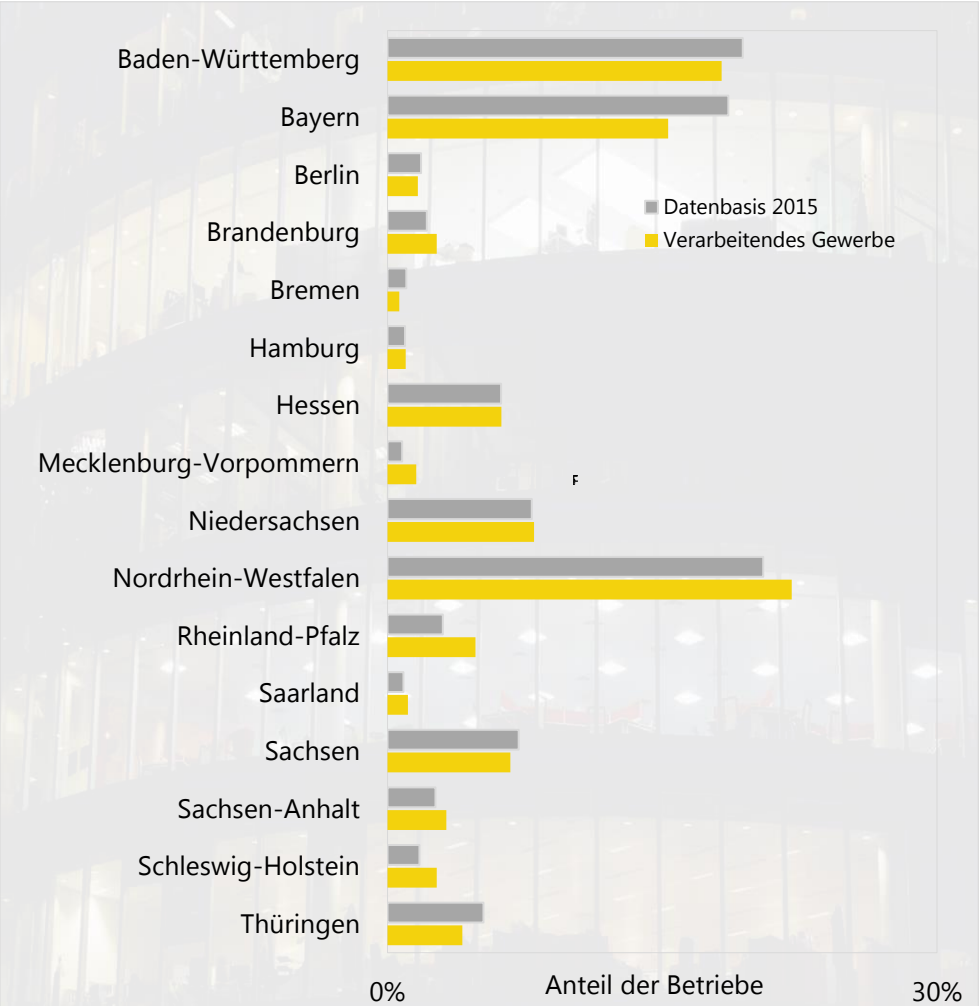
2.1 Methodik

Für eine belastbare Einschätzung der Virulenz von Industriespionage einerseits und der Verbreitung grundlegender Schutzmaßnahmen im Verarbeitenden Gewerbe andererseits kann die Erhebung *Modernisierung der Produktion 2015* des Fraunhofer-Instituts für System- und Innovationsforschung ISI herangezogen werden (*Jäger/Maloca* 2015). Diese seit 1993 regelmäßig durchgeführte Industrieerhebung zielt darauf ab, die Produktionsstrukturen des Verarbeitenden Gewerbes in Deutschland hinsichtlich ihrer Modernität und Leistungsfähigkeit systematisch zu beobachten. Zielgruppe dieser Betriebsbefragung sind die ca. 44.300 Betriebe des Verarbeitenden Gewerbes in der Bundesrepublik Deutschland (Statistisches Bundesamt 2014). Mehr Informationen zur Erhebung stehen auch online zur Verfügung unter **www.isi.fraunhofer.de/de/themen/industrielle-wettbewerbsfaehigkeit/erhebung-modernisierung-produktion.html**.

In der schriftlichen Befragung werden anhand detaillierter Indikatoren Produktionsstrategien, die technische Modernisierung der Wertschöpfungsprozesse, der Einsatz innovativer organisatorischer Konzepte und Prozesse in der Produktion, Fragen des Personaleinsatzes und der Qualifikation sowie das Angebot neuer Geschäftsmodelle zur Ergänzung des Produktangebots um innovative Dienstleistungen erfasst. In Verbindung mit den betrieblichen Rahmendaten und Leistungskennziffern, wie Produktivität, Flexibilität und Qualität, ermöglichen diese Daten detaillierte Analysen zur Modernität und Leistungskraft der Betriebe des Verarbeitenden Gewerbes.

Für die Erhebung *Modernisierung der Produktion* 2015 wurden aus der Grundgesamtheit ca. 15.720 Betriebe zufällig ausgewählt und um Teilnahme gebeten. Von den angeschriebenen Betrieben haben 1.282

Abbildung 5: Vergleich der Verteilung nach Bundesländern in der Grundgesamtheit und in der Erhebung *Modernisierung der Produktion* 2015

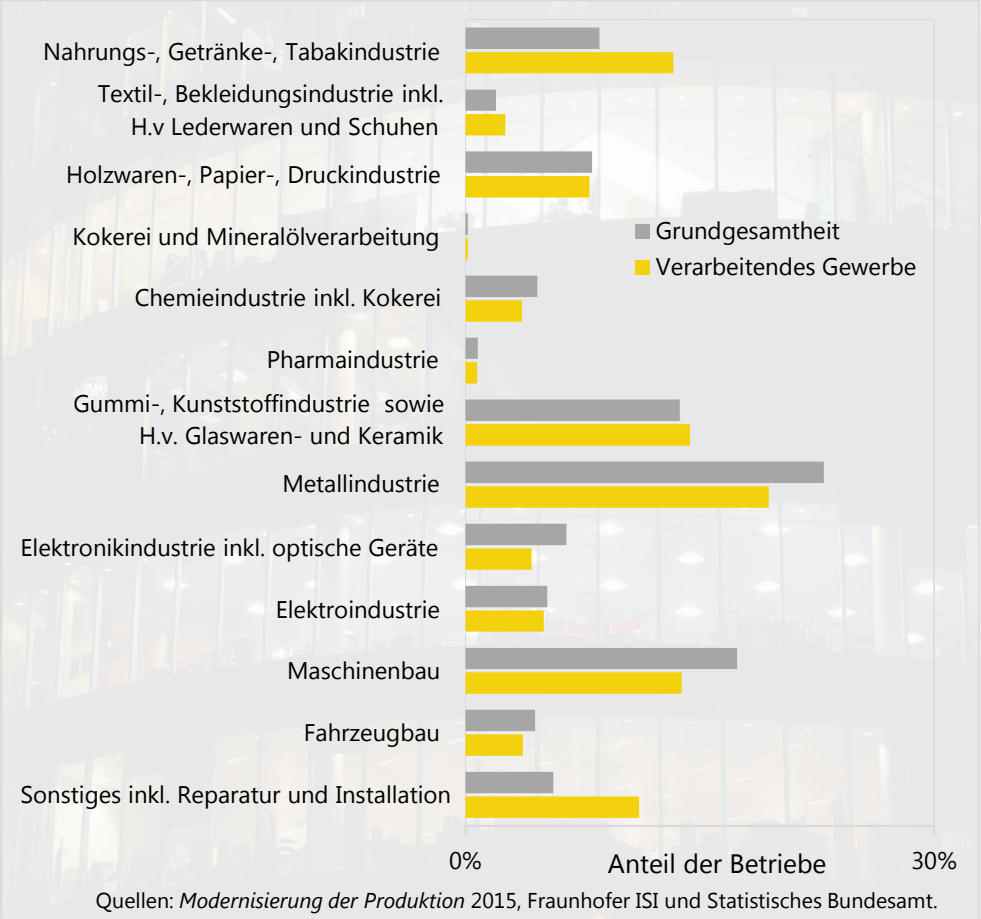


Quellen: *Modernisierung der Produktion* 2015, Fraunhofer ISI und Statistisches Bundesamt (2014).

einen verwertbaren Fragebogen zurückgesandt (Rücklaufquote: 8 Prozent). Die antwortenden Betriebe decken das gesamte Verarbeitende Gewerbe umfassend ab. Der resultierende Datensatz repräsentiert sehr gut die regionale Verteilung über die Bundesländer (s. Abbildung 5) sowie die Verteilung der Branchen im Verarbeitenden Gewerbe Deutschlands (s. Abbildung 6). Unter anderem sind Unternehmen des Maschinenbaus und der metallverarbeitenden Industrie zu 17 bzw. 20 Prozent vertreten, die Elektroindustrie zu zwölf Prozent, die Gummi- und Kunststoff verarbeitende Industrie zu acht Prozent, das

Ernährungsgewerbe zu acht Prozent und das Papier-, Verlags- und Druckgewerbe zu fünf Prozent.

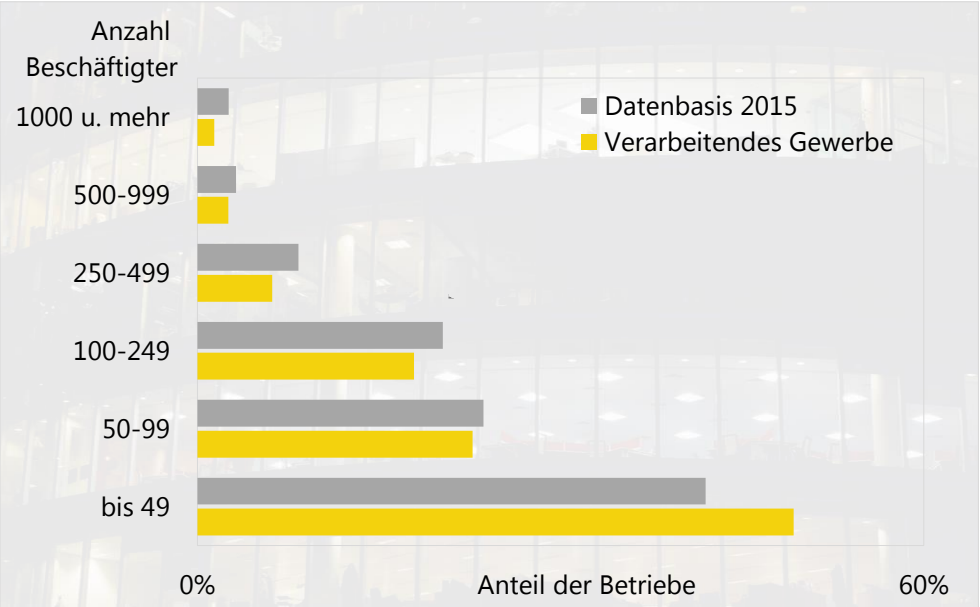
Abbildung 6: Vergleich der Branchenverteilung in der Grundgesamtheit und in der Erhebung *Modernisierung der Produktion* 2015



Quellen: *Modernisierung der Produktion* 2015, Fraunhofer ISI und Statistisches Bundesamt.

Zudem zeigt der Vergleich zwischen den Daten des Statistischen Bundesamtes und der realisierten Stichprobe, dass neben den großen Betrieben auch die kleinen Betriebe gut repräsentiert sind. Mit rund 66 Prozent machen die Betriebe mit weniger als 100 Beschäftigten fast zwei Drittel der realisierten Stichprobe aus, mittelgroße Betriebe 31 Prozent und große Betriebe (mit mehr als 1.000 Beschäftigten) drei Prozent der antwortenden Firmen (s. Abbildung 7). Die Verteilung der Erhebungsdaten über die Betriebsgrößenklassen hinweg ist auch hier mit der Grundgesamtheit vergleichbar (*Jäger/Maloca* 2015).

Abbildung 7: Vergleich der Betriebsgrößenverteilung in der Grundgesamtheit und in der Erhebung *Modernisierung der Produktion* 2015



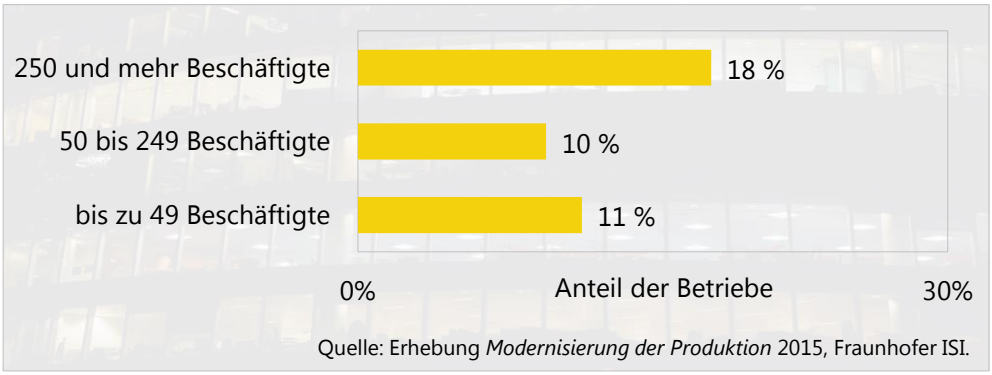
Quellen: *Modernisierung der Produktion* 2015, Fraunhofer ISI /Statistisches Bundesamt (2014).

2.2 Ergebnisse

Mit dieser repräsentativen Befragung konnten erstmals konkrete Zahlen zu Spionagefällen bzw. Verdachtsfällen in Unternehmen des Verarbeitenden Gewerbes in Deutschland vorgelegt werden. Zu beachten ist, dass es sich hierbei um die tatsächlich bekannten Vorfälle und Verdachtsfälle zur Wirtschaftsspionage und Konkurrenzausspähung in den Unternehmen handelt – das sog. doppelte Dunkelfeld, nämlich die Unternehmen, die einen Vorfall nicht nur verschweigen bzw. nicht nennen, sondern die ihn erst gar nicht bemerken oder nicht diesem Kontext zuordnen, bleibt hier noch außen vor. Ein solcher Vorfall oder Verdachtsfall wurde von elf Prozent der Unternehmen im Verarbeitenden Gewerbe bejaht (s. Abbildung 8). Besonders betroffen scheinen zunächst die größeren Unternehmen mit mehr als 250 Beschäftigten zu sein. Dieses resultiert zum Teil daraus, dass die größeren

Unternehmen auch im Außenraum sichtbarer sind und dadurch eher Aufmerksamkeit auf sich lenken. Weiterhin steuern aber auch organisatorische Maßnahmen wie z.B. Frühwarnsysteme ihren Anteil zum Bemerken von Angriffen bei. Diese werden – wie sich in den vorangegangenen Experteninterviews gezeigt hat – bei kleineren Unternehmen wesentlich seltener eingesetzt. Daher ist zu vermuten, dass bei kleineren Unternehmen der Anteil der unentdeckt gebliebenen Angriffe höher einzuschätzen ist als bei größeren Unternehmen mit entsprechenden organisatorischen Maßnahmen. Einen weiteren Erklärungsansatz der großen Differenz liefert der Sprachgebrauch von "Spionage und Ausspähung": Dieser führte zumindest in den qualitativen Interviews oftmals zur spontanen Verneinung. Befragt nach einem ungewollten Informationsabfluss an Dritte, wird die Frage in einigen Fällen plötzlich bejaht. Vor dem Hintergrund des Wordings bzw. der unterschiedlichen Assoziationen sind auch die stark schwankenden Zahlen zur Betroffenheit der deutschen Wirtschaft durch Wirtschaftsspionage und Konkurrenzausspähung in diversen Studien der letzten Jahre zu erklären, bei denen die Betroffenheit der Unternehmen zwischen acht und über fünfzig Prozent schwankt.

Abbildung 8: Vorfälle bzw. Verdachtsfälle bei Unternehmen im Verarbeitenden Gewerbe nach Betriebsgröße



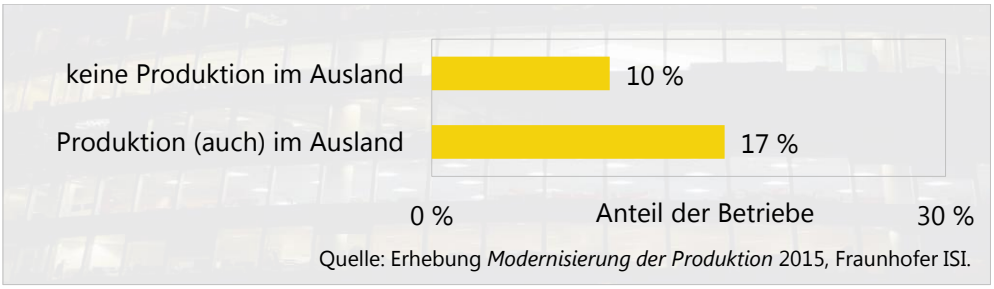
Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI.

Erwartungsgemäß sind Unternehmen mit mittlerer Forschungs- und Entwicklungsintensität (2,5-7 Prozent FuE-Aufwendungen) und hoher

Forschungs- und Entwicklungs-Intensität (> 7 Prozent FuE-Aufwendungen) mit 18% bzw. 19% der Unternehmen stärker betroffen. Ein Grund dafür liegt darin, dass diese Unternehmen durch ihre Forschungsaktivitäten (und folgend durch die Präsentation innovativer Produkte und/oder durch Patentaktivitäten) ins Visier von Angreifern gelangen und eben durch diese Tätigkeiten interessant werden.

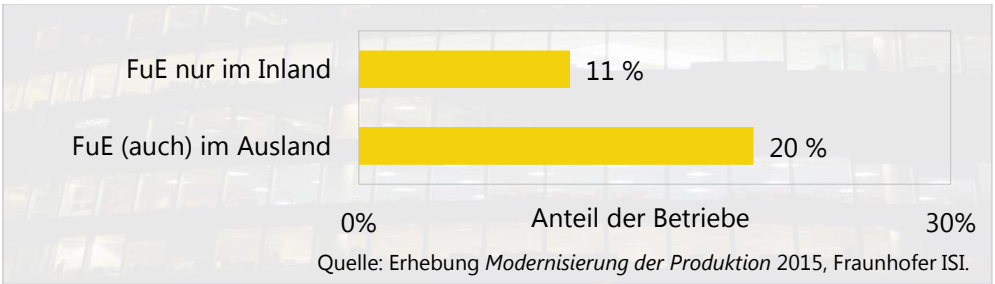
Ein weiterer Sachverhalt, der die Unternehmen ins Ziel der Angreifer rückt, ist der Auslandsbezug: Unternehmen mit (auch) einer Produktionsstätte im Ausland sind mit 17 Prozent deutlich stärker betroffen, als solche ohne (10 Prozent) (s. Abbildung 9). Ebenso meldet jedes fünfte Unternehmen (20 Prozent), das (auch) eine Forschungs- und Entwicklungsabteilung im Ausland unterhält, bereits mindestens einen Vorfall oder Verdachtsfall. Bei den Unternehmen mit FuE-Aktivitäten ausschließlich im Inland sind es nur elf Prozent (s. Abbildung 10).

Abbildung 9: Vorfälle bzw. Verdachtsfälle bei Unternehmen mit Produktionsstandorten im Ausland



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI.

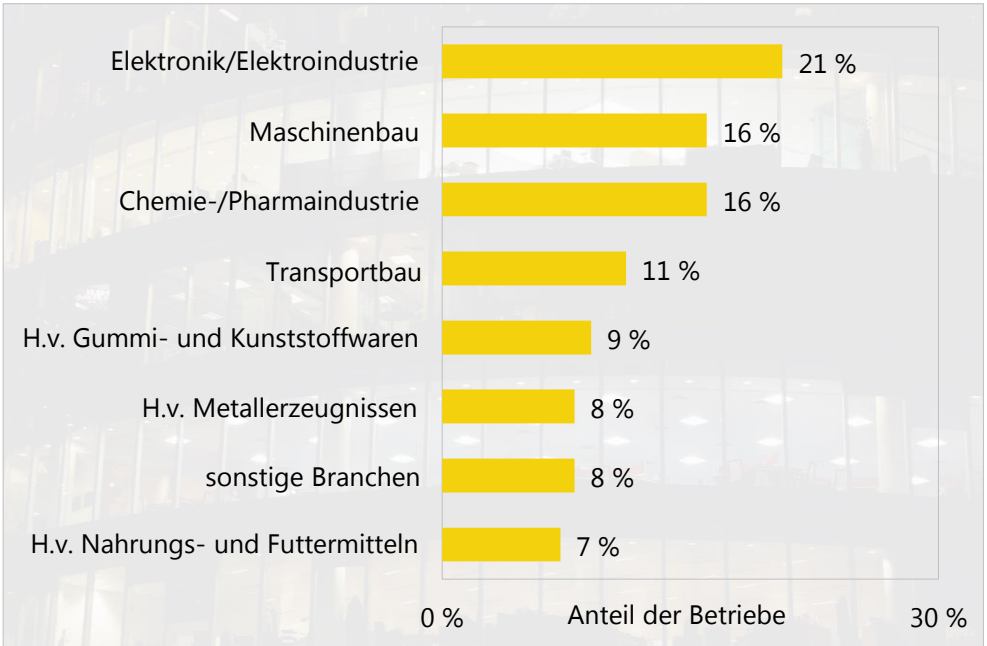
Abbildung 10: Vorfälle bzw. Verdachtsfälle bei Unternehmen mit FuE-Standorten im Ausland



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI.

Erwartungsgemäß stellt sich die heterogene Verteilung der Vorfälle und Verdachtsfälle über die verschiedenen Branchen dar (s. Abbildung 11): Besonders betroffen sind die Elektronik- bzw. Elektroindustrie mit 21 Prozent, gefolgt vom Maschinenbau (16 Prozent) und der Chemie- bzw. Pharmaindustrie (ebenfalls 16 Prozent). Begründen lässt sich die Verteilung durch die langen Forschungs- bzw. Vorlaufzeiten bis zur Produktreife sowie die große Bedeutung von Produkt- und Prozessinnovationen in den betroffenen Branchen.

Abbildung 11: Verteilung der Vorfälle und Verdachtsfälle nach Branchen

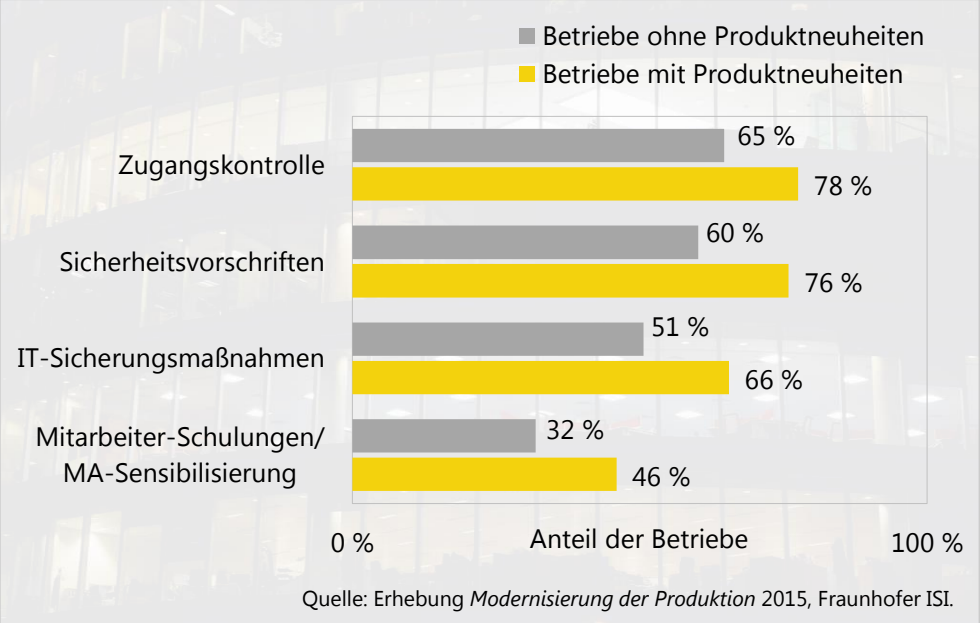


Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI.

Zusätzlich zur tatsächlichen Betroffenheit wurden auch die eingesetzten Schutzmaßnahmen in vier Kategorien erhoben und analysiert: der Schutz vor physischem Zugang zu Produktionsstätten, die Existenz von Sicherheitsvorschriften zum Schutz gegen den unerlaubten Abfluss von Informationen (z.B. Regelungen zum Umgang mit sensiblen

Daten gegenüber Dritten), die Existenz von speziellen IT-Sicherheitsmaßnahmen (wie z.B. Verschlüsselung von Dokumenten, Nutzungsverbot von Clouddiensten und von fremden portablen Datenträgern) und die Schulung bzw. Sensibilisierung von Beschäftigten zu den Gefahren durch Wirtschaftsspionage und Konkurrenzausspähung (s. Abbildung 12).

Abbildung 12: Realisierte Schutzmaßnahmen zur Abwehr von Spionage bzw. Ausspähung im Verarbeitenden Gewerbe



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI.

Insgesamt lässt sich ein verstärktes Bewusstsein für die Gefahrenlage und daraus resultierend ein größerer Umfang an realisierten Schutzmaßnahmen bei Unternehmen feststellen, die in den letzten Jahren Produktneuheiten auf den Markt gebracht haben.

Mit zum Teil weit unter 50 Prozent auffallend niedrig ist der Anteil der KMU, die ihre Beschäftigten überhaupt für die Gefahren *sensibilisieren*. Dieser Umstand wurde daher in den zeitlich später folgenden Experteninterviews mit Unternehmensvertretern thematisiert: Ohne an

dieser Stelle die Ergebnisse umfassend darzustellen, kann jedoch festgestellt werden, dass einige Unternehmen die Schulung/Sensibilisierung ihrer Beschäftigten nicht für nötig halten, da sie das bei den Beschäftigten vorhandene Wissen als nicht relevant für Wirtschaftsspionage bzw. Konkurrenzausspähung erachten. Beispielsweise wurde angeführt, dass nur sehr wenige Beschäftigte aus dem engsten Führungskreis überhaupt wüssten, welche Produkte in Planung sind bzw. über welche technischen Details diese verfügen (sollen). Ein anderes Beispiel ist, dass sich die Kundenkommunikation und die Kundendatenbank ausschließlich auf dem PC der vertrauenswürdigen Assistentin befinden und diese nicht explizit auf die Sensitivität hingewiesen werden müsse.

Von Informationsabfluss durch eigene Beschäftigte betroffene Unternehmen reagieren jedoch nach einem Vorfall schnell und führen zumindest grundlegende Präventionsmaßnahmen ein – die bis zu diesem Zeitpunkt mit den o.g. Argumenten nicht für nötig gehalten wurden. Das Verhalten vor dem ersten Vorfall ist unverständlich, gerade angesichts der Tatsache, dass beispielsweise der Punkt Mitarbeiterschulung bzw. -sensibilisierung mit geringem Aufwand angegangen werden kann.

Weitere Handlungsnotwendigkeiten werden deutlich, wenn man sich die Ergebnisse zur *Existenz von IT-Sicherheitsmaßnahmen* ansieht: 34 Prozent der Unternehmen mit Produktneuheiten und sogar jedes zweite Unternehmen ohne Produktneuheiten treffen überhaupt keine Schutzmaßnahmen gegen ungewollten Informationsabfluss. Angesichts der großen Bedrohung, die Cyberangriffe darstellen – sei es durch das Ausnutzen von Sicherheitslücken im Informations- und Kommunikationstechnologie-Bereich (IKT), den direkten Angriff auf Maschinen und Anlagen mit Netzwerkeinbindung, die Schadsoftware-Infiltration per Internetnutzung (Drive-by-Exploits) oder gezielte Angriffe auf Sicherheits-Hardware (Router) und Firewalls – ist dies nicht

nachzuvollziehen. Für den fehlenden IT-Schutz gibt es unterschiedliche Gründe. Überwiegend besteht zwar durchaus die Bereitschaft, sich des Themas anzunehmen, doch scheitern diesbezügliche Bemühungen oft an Zeit und Ressourcen. Auch fühlen sich die Unternehmen bei der Auswahl der geeigneten Maßnahmen häufig überfordert angesichts der Komplexität und des fehlenden Überblicks über wirkungsvolle und aktuelle Technologien. Hinzu kommt die Schnelllebigkeit mancher Lösung: Kaum ist ein wirksamer Schutz verfügbar, wird er schon wieder umgangen.

Abbildung 13: Dynamische Entwicklung der Nutzung von IT-Sicherheitsmaßnahmen

Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI.

Aufschlussreich ist auch ein Blick in die Historie: Die Unternehmen, die angegeben haben, IT-Sicherheitsmaßnahmen implementiert zu haben, wurden nach dem Jahr der Ersteinführung befragt (s. Abbildung 13). Bis zum Jahr 2000 war das Thema nahezu unbekannt. Mit den zur Jahrtausendwende angekündigten Fehlern und der Reaktion darauf wurden erste Firmen in diesem Bereich aktiv. Bedeutend ist, dass viele der befragten Unternehmen erst in den letzten Jahren überhaupt IT-

Sicherheitsmaßnahmen getroffen haben. Im Jahr 2015 schließlich hatten immerhin fast 60 Prozent der Unternehmen IT-Sicherheitsmaßnahmen installiert. Dies bedeutet allerdings auch, dass zwei von fünf Unternehmen zu diesem Zeitpunkt noch keine Maßnahmen ergriffen hatten.

Die abgefragte dritte Kategorie von Maßnahmen betrifft die Zugangskontrolle (s. Abbildung 12). Diese umfasst zum einen Maßnahmen zum Schutz vor physischem Zugang zu den Betriebs- und Produktionsstätten bzw. bestimmten Bereichen dieser (z.B. Serverraum, Büros der Geschäftsleitung) durch Unbefugte (Zutrittskontrolle) und zum anderen Maßnahmen, die die Nutzung von Maschinen, Anlagen und vor allem Datenverarbeitungseinrichtungen durch Unbefugte verhindern sollen (Zugangskontrolle i.S.d. Nr. 2 der Aufzählung in der Anlage zu § 9 Satz 1 BDSG). Letzteres erfolgt klassisch über eine Kombination von Benutzernamen und Passwort. Gerade bei Maschinen und Anlagen ist oft festzustellen, dass die Standard-Zugangsdaten des Herstellers nicht geändert werden und dem Angreifer somit sein Vorhaben erleichtert wird, da die Zugangsdaten bekannt sind. Ist die Maschine dann sogar noch an das Internet angebunden, steigt das Risiko exponentiell. Es existieren spezielle, frei zugängliche Suchmaschinen im Internet, mit denen selbst der Laie gezielt nach ungeschützten Geräten suchen kann und die Ergebnisse kategorisiert nach Typ und Standort ausgegeben bekommt. An dieser Stelle können bereits kleine Nachlässigkeiten bei der Inbetriebnahme von Gerätschaften große Sicherheitslücken hervorrufen.

Ein ähnlich großes Potenzial für wirksame Präventionsmaßnahmen besteht im Bereich der Sicherheitsvorschriften für Beschäftigte, die lediglich bei 60 Prozent der Unternehmen ohne Produktneuheiten und immerhin bei 76 Prozent der Unternehmen mit Produktneuheiten etabliert sind. Auch hier ist eine Umsetzung einfach und kostengünstig möglich.

Zusammenfassend lässt sich feststellen, dass selbst innovative Unternehmen das Thema Gefahrenabwehr nicht umfassend adressiert haben und damit ein großer Nachholbedarf im Bereich des Schutzes von Unternehmensdaten vor allem bei KMU besteht.

Literaturnachweis:
Jäger, A. & Maloca, S.: Dokumentation der Umfrage *Modernisierung der Produktion* 2015, Fraunhofer ISI, Karlsruhe 2016.

Dunkelfeldbefragung bei KMU

3 Dunkelfeldbefragung bei KMU

3.1 Methodik

Die Dunkelfeldbefragung stellt die Zusammenführung aller vorherigen Projektergebnisse dar. Ihr voraus gingen Länderanalysen[1] innerhalb der EU und in der Schweiz in Bezug auf den soziokulturellen, normativen und verfahrensrechtlichen Rahmen. Der rechtstatsächliche Rahmen wurde über die Erfassung und den Vergleich verfügbarer statistischer Daten erfasst. Zudem lieferte eine Dokumentenanalyse Erkenntnisse über die Endnutzerperspektive, insbesondere der betroffenen Unternehmen. Anschließend erfolgte eine vertiefte Analyse ausgewählter Länder (England, Dänemark, Bulgarien, Österreich, Schweiz) mit dem Ziel der detaillierteren Untersuchung, um neue, auf Deutschland übertragbare Handlungsansätze zu identifizieren. Hierzu wurden 30 Experteninterviews mit Akteuren innerhalb der ausgewählten Länder geführt. Die unterschiedlichen Blickwinkel auf die relevanten Phänomene wurden durch die Auswahl von Vertretern aus der Industrie, von industrienahen Dienstleistern, Verbänden, Behörden und aus Wissenschaftsorganisationen – aus jedem jeweiligen Land – repräsentiert.

Die im Ausland vorgefundenen Ansätze und der Status Quo von Präventionsmaßnahmen und Bedrohungswahrnehmung wurden im Anschluss in Deutschland mit Experten aus Industrie, Wissenschaftsorganisationen und Behörden im Umfang von weiteren 30 Expertengesprächen diskutiert.[2] Parallel dazu wurde der aktuelle Stand im Rahmen einer repräsentativen quantitativen Befragung im Verarbeitenden

1 | *Carl, S. & Kilchling, M.* (Hrsg.): Economic and Industrial Espionage in Germany and Europe: History, developments and present legislative frameworks in a comparative perspective. Berlin 2018 (Duncker & Humblot).

2 | *Wallwaey, E., Bollhöfer, E. & Knickmeier, S.* (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin 2018 (Duncker & Humblot).

Gewerbe 2015 (Befragung *Modernisierung der Produktion* 2015, Fraunhofer ISI, N=1.282) erhoben (s.o. Kapitel 2). Im Rahmen mehrerer Arbeitstreffen des gesamten Konsortiums wurden die Teilergebnisse vorgestellt, diskutiert und die anschließenden Schritte ausgearbeitet. Die assoziierten Partner aus den Bereichen Polizei und Wissenschaft ergänzten die Arbeiten um praktische Erfahrungen und aktuelle Fragestellungen aus dem polizeilichen Bereich. So konnte das breite Spektrum an Vorergebnissen und Erfahrungen in das Design der Dunkelfeldbefragung einfließen. Spezielle Fragestellungen, die sich aus den Vorergebnissen entwickelt haben, jedoch bislang noch nicht empirisch untersucht wurden, konnten so in den Fragebogen aufgenommen werden.

Die *Dunkelfeldbefragung* stellte eine separate quantitative Befragung im Projekt WISKOS dar. Sie schließt sich, wie oben beschrieben, inhaltlich an die Erkenntnisse der vorhergehenden Arbeitspakete an. Im Rahmen der Befragung wurden die Geschäftsführer oder CIOs von 6.284 mittelständischen Unternehmen angeschrieben. Die Auswahl erfolgte in Form einer systematischen Zufallsauswahl auf der Basis der Hoppenstedt Firmenkundendatenbank unter Hinzunahme weiterer Auswahlkriterien. Diese waren neben der Unternehmensgröße (maximal 250 Beschäftigte) die produzierenden Branchen in Deutschland sowie industrienahe Dienstleister. Damit umfasste die Auswahlgrundlage für die Zufallsziehung 23.462 Unternehmen, aus denen die Stichprobe gezogen wurde. Zusätzlich zu den postalisch verschickten Fragebögen konnte die Teilnahme auch online, z.B. über eine Einladung regionaler Industrie- und Handelskammern, erfolgen. Insgesamt 583 Unternehmen beantworteten im Zeitraum von Mitte Juni bis September 2017 den Fragebogen in verwertbarer Form.

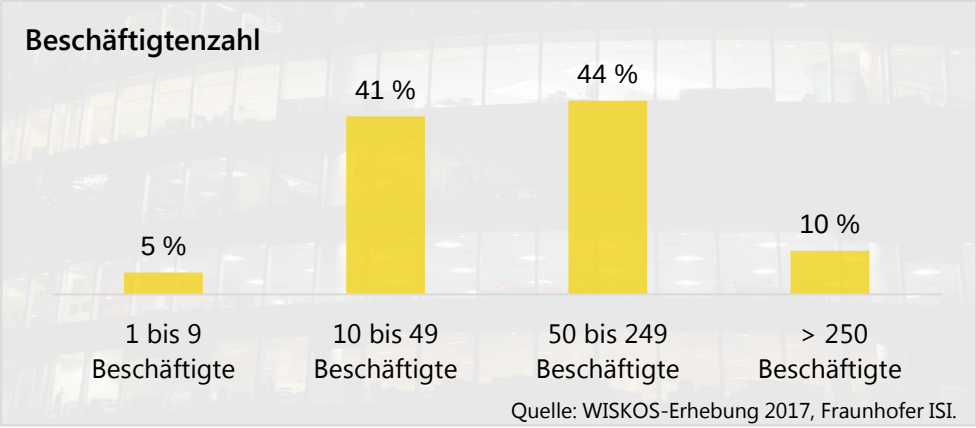
Im Folgenden wird dargestellt, nach welchen Kriterien die Befragungsdaten bislang ausgewertet wurden und an welchen Stellen

Kreuzanalysen zwischen einzelnen Fragen vertiefte Erkenntnisse zulassen.

3.2 Allgemeine Unternehmensdaten

Um die Unternehmen im Rahmen der Auswertungen nach spezifischen Merkmalen kategorisieren zu können, wurden die Unternehmensgröße, der Umsatz und die Branche abgefragt.

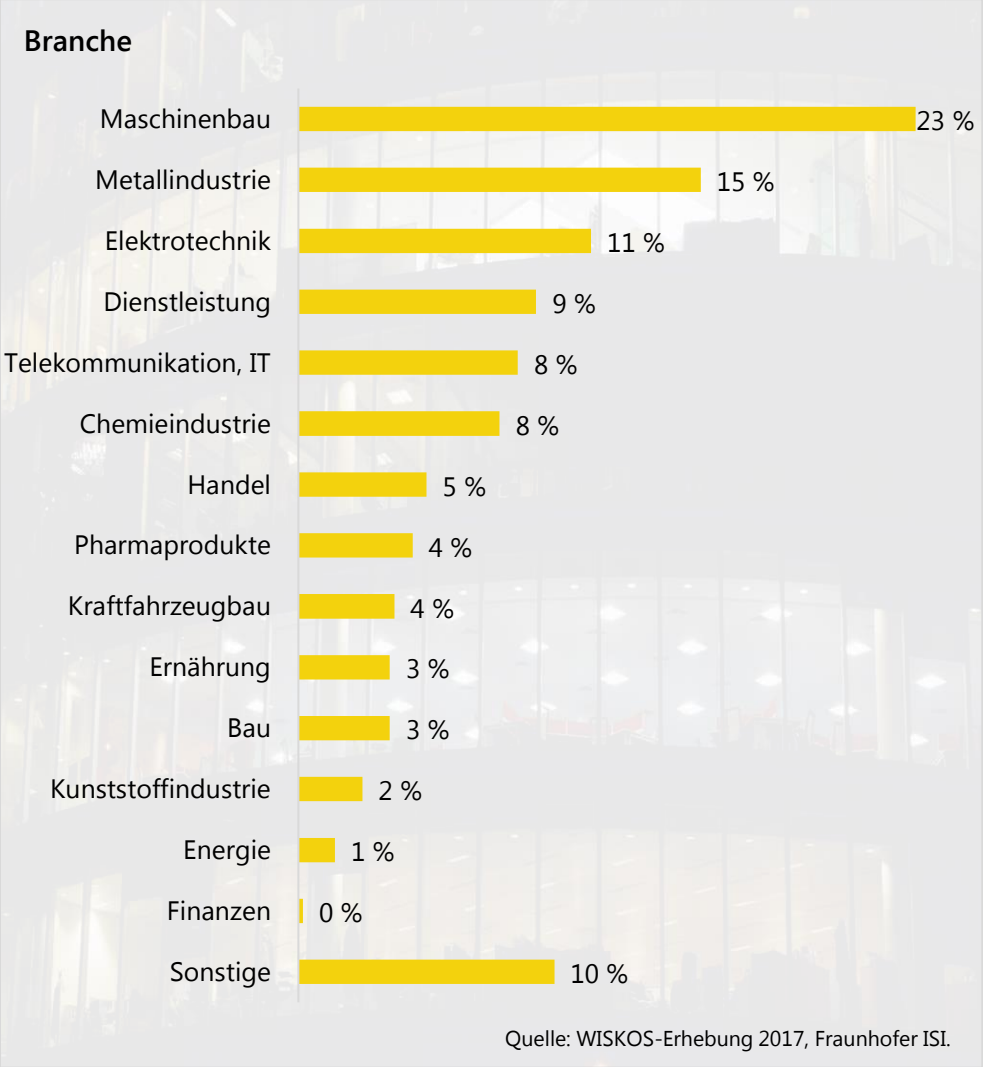
Abbildung 14: Betriebsgröße der befragten Unternehmen

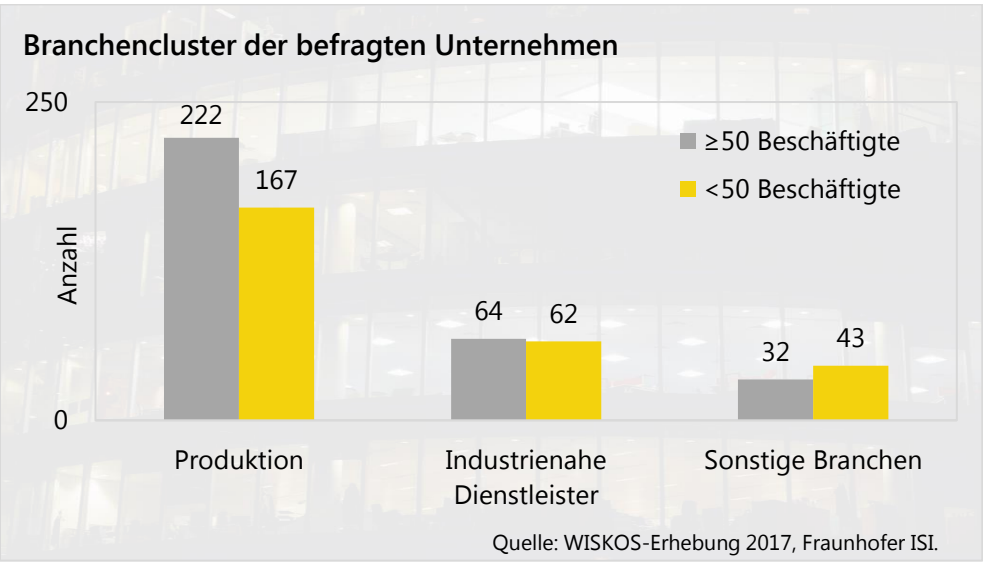


Demnach lag die Teilnehmerzahl bei kleinen Unternehmen mit unter 50 Beschäftigten bei 46 Prozent und bei größeren KMU mit 50 oder mehr Beschäftigten bei 54 Prozent (s. Abbildung 14).

Die Befragung war zugeschnitten auf die speziellen Bedrohungen und deren Handhabung für kleine und mittelständische produzierende Unternehmen; gleichzeitig sollten auch zu einem kleineren Anteil industrienahe Dienstleister Berücksichtigung finden (s. Abbildung 15). Die antwortenden Unternehmen bilden dies gut ab und bieten ausreichend Fälle für getrennte Analysen (vgl. Abbildung 16):

Abbildung 15/16: Branchenzugehörigkeit der befragten Unternehmen im Detail und nach Branchenclustern

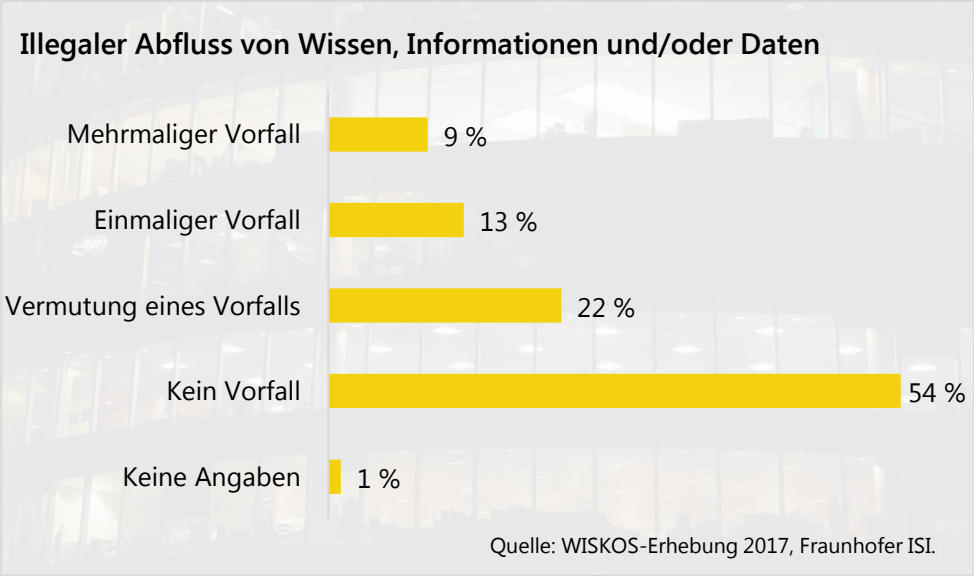




3.3 Vorfälle, Verdachtsfälle und Reaktionen der Unternehmen

Die kleinen und mittelständischen Unternehmen sind gut beraten, das Thema Wirtschaftsspionage und Konkurrenzausspähung nicht auf die leichte Schulter zu nehmen. Gerade der Mittelstand stellt in Deutschland die meisten Arbeitsplätze und ist seit vielen Jahren ein Garant für Wirtschaftswachstum. Die Digitalisierung hat zudem dazu geführt, dass auch kleinere Unternehmen international präsent sein können. Dadurch wurden neue Begehrlichkeiten aber auch neue Ziele für Angreifer geschaffen.

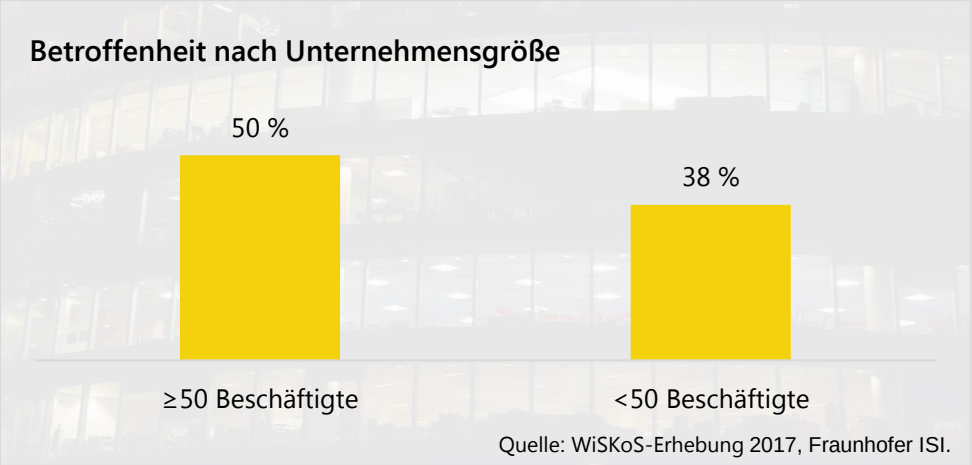
Abbildung 17: Betroffenheit der befragten Unternehmen



Die Ergebnisse dieser, wie auch anderer Befragungen zeigen, dass sich kein Unternehmen sicher fühlen kann. Es gibt weder kaum betroffene Branchen noch kaum betroffene Unternehmensgrößenklassen (s. Abbildung 18 und Abbildung 19). Etwas mehr als jedes zweite Unternehmen berichtet von sich, noch nicht betroffen gewesen zu sein,

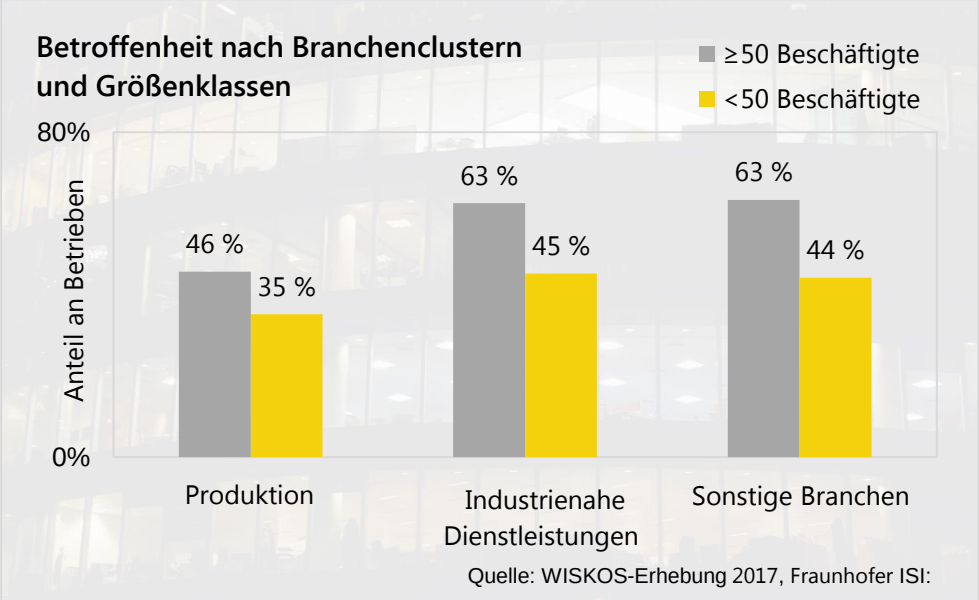
was jedoch auch bedeutet, dass 44 Prozent der Unternehmen bereits einen Vorfall oder zumindest einen konkreten Verdachtsfall hatten (s. Abbildung 17). Fast ein Viertel aller Unternehmen, nämlich 22 Prozent, hatten immerhin bereits mindestens einen Vorfall innerhalb der letzten fünf Jahre.

Abbildung 18: Betroffene Unternehmen nach Größe



Die hohe Zahl der Verdachtsfälle ist auch ein Indiz dafür, dass Wirtschaftsspionage und Konkurrenzausspähung oftmals schwer festzustellen sind. Nicht nur die oben bereits angesprochene Trennung zwischen verschiedenen IT-Vorfällen und Spionage gelingt nur selten, auch die Vermengung mit anderen Delikten, wie z.B. mit Einbruchsdiebstahl, ist häufig anzutreffen. Oftmals liegt dabei der Verdacht der Spionage gar nicht auf der Hand; ein eventueller Abfluss von Informationen wird nicht oder erst viel später in einem anderen Kontext bemerkt.

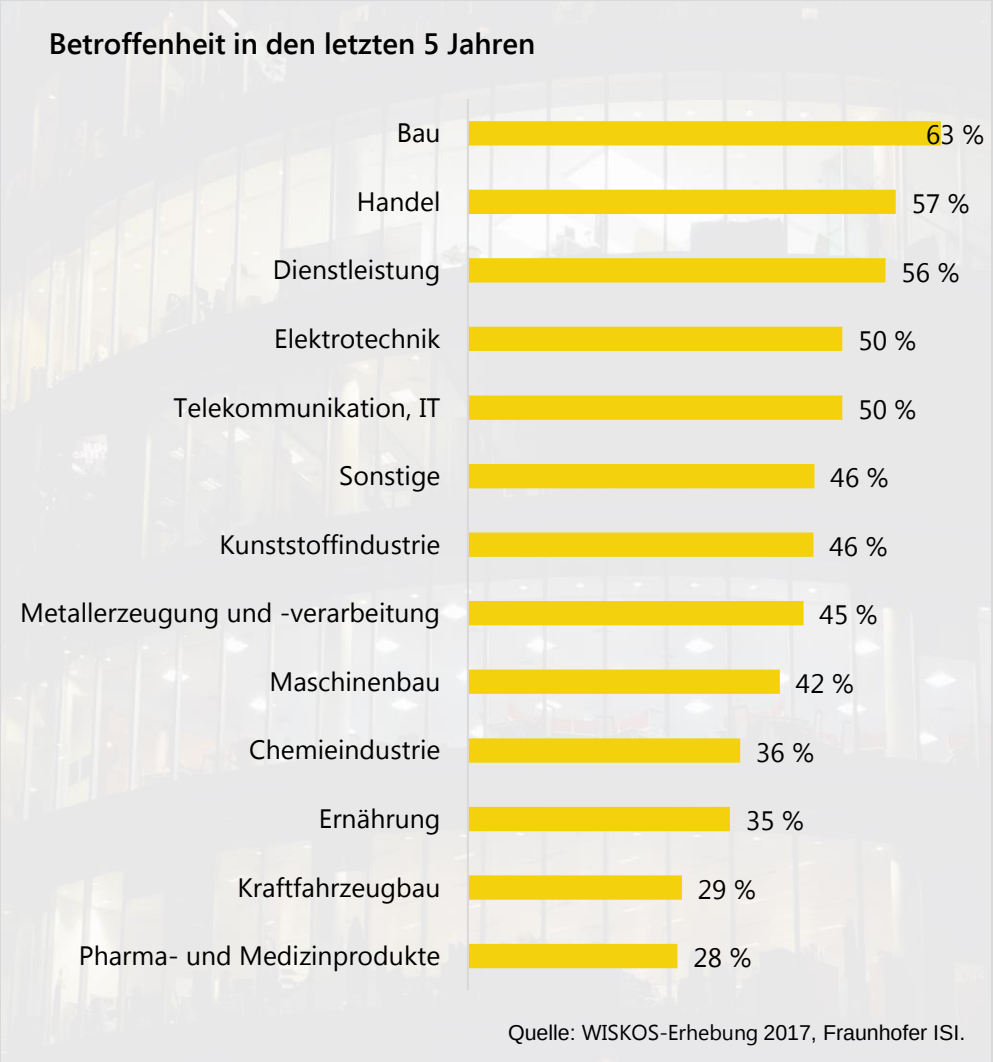
Abbildung 19: Betroffenheit der Unternehmen nach Branchenclustern



In Deutschland sind Baubranche und Handel am stärksten von Vorfällen betroffen (s. Abbildung 20). Die Rangposition 3 für den Bereich der industrienahen Dienstleistungen ist nicht unerwartet: In einer wissensintensiven Branche sind strukturierte Informationen besonders wertvoll. Etwas überraschend ist die geringe Anzahl an Vorfällen im Kfz-Bau, würde man doch gerade hier den Einsatz innovativer Technologien und einen hohen Innovationsgrad – und damit viele Angriffe – vermuten. Die Häufigkeiten können jedoch durch eine unterschiedlich starke Sensibilisierung und die jeweils in Präventionsarbeit investierten Summen in verschiedenen Branchen beeinflusst sein. Nicht zuletzt unterliegen die Kfz-Zulieferer bereits sehr hohen Anforderungen hinsichtlich Dokumentation und Sicherheit durch ihre Auftraggeber, sodass davon auszugehen ist, dass hier derzeit schon entsprechende Präventionsmaßnahmen zum Standard gehören und damit weniger erfolgreiche Angriffe stattfinden. Allgemein können Unternehmen, die

ein systematisches Monitoring von bestimmten Merkmalen betreiben, Vorfälle und Verdachtsfälle eher identifizieren als andere.

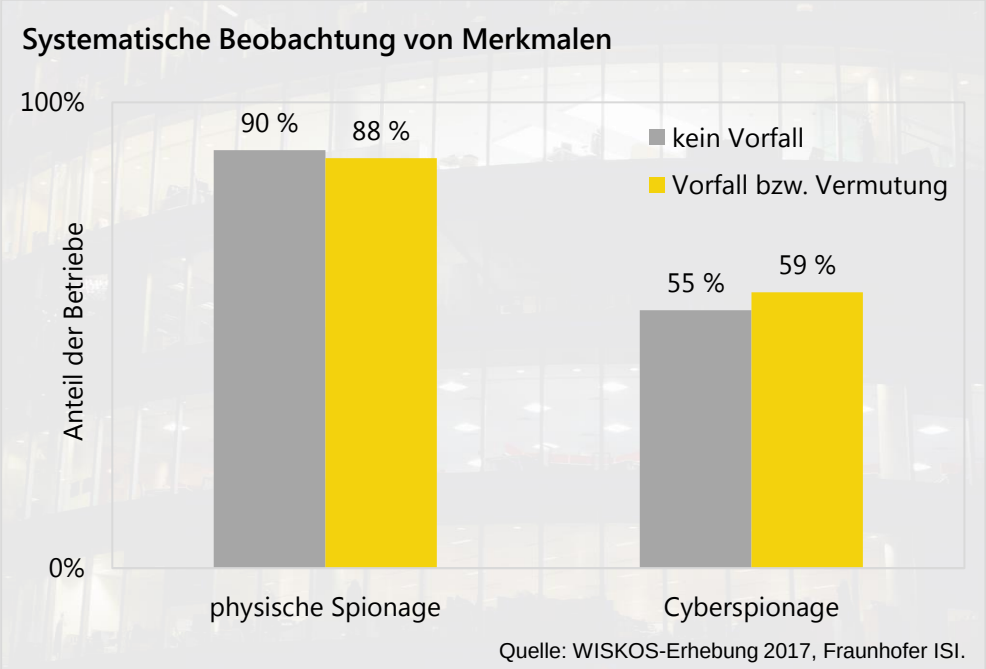
Abbildung 20: Betroffenheit der Unternehmen nach Branchen



Überraschend ist, dass sich durch erlebte Vorfälle oder konkrete Verdachtsfälle keinerlei Lerneffekte bei der systematischen Beobachtung von Verdachtsmerkmalen einstellen: So zeigen bereits betroffene Unternehmen kein anderes Verhalten in Sachen systematischer Merkmalsbeobachtung als nicht betroffene Unternehmen (s. Abbildung 21). Daher gilt es zu hinterfragen, warum betroffene Unternehmen durch

Vorfälle nicht achtsamer werden. Liegt es daran, dass in vielen Fällen der Schaden nicht sofort feststellbar oder nicht bezifferbar ist? Oder liegt es daran, dass eine wirksame Präventionsarbeit ein ganzes Bündel an Maßnahmen erfordert und nicht mit der einmaligen Aktualisierung einer Software zu erledigen ist? Vermutlich ist es eine Kombination aus beidem. In den vorangegangenen Experteninterviews wurde immer wieder deutlich, dass die Unternehmen zwar Handlungsbedarfe sehen, diese aber aus Kapazitätsgründen nicht oder nur nachrangig angehen.

Abbildung 21: Monitoring von Merkmalen vor und nach einem Vorfall bzw. Verdachtsfall



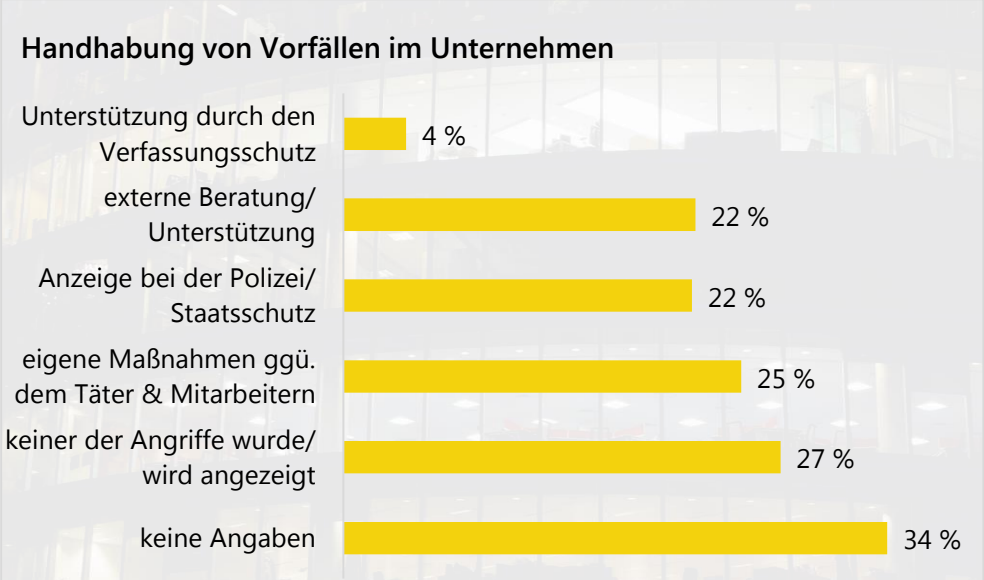
Befragt zu dem Vorgehen bei Vorfällen oder Verdachtsfällen im Unternehmen ergibt sich ein sehr heterogenes Bild: Es gibt keine Standard-Vorgehensweise, das Vorgehen ist von den Umständen des Einzelfalls geprägt, kombiniert mit Einflüssen strategischer Führungsentscheidungen. Auffällig sind vor allem zwei Punkte (s. Abbildung 22): 34 Prozent der Unternehmen wollten hierzu bewusst nicht Stellung

nehmen – und dies nicht etwa durch Auslassen oder Überspringen der Frage, sondern durch explizites Ankreuzen von "keine Angaben". Auch dies kann ein Zeichen für eine große bestehende Unsicherheit der Unternehmen im Kontext der Bedrohung durch Spionage sein. Es ist nicht anzunehmen, dass die Unternehmen bei genau dieser Frage ihre Unternehmensinterna schützen bzw. nicht offenlegen wollten, da sie bei den anderen, z.T. weitaus intimeren Fragestellungen, durchaus auskunftsfreudig agiert haben.

Ein zweiter Wert von starker Aussagekraft ist das Bestreben von 27 Prozent der Unternehmen, dem Täter mit eigenen Maßnahmen zu begegnen und keine externe Unterstützung (durch Behörden oder durch private Dritte) in Anspruch zu nehmen. Diese Tendenz stimmt mit vorhergehenden Beobachtungen überein, dass Unternehmen negative Reaktionen der Kunden bzw. der Öffentlichkeit befürchten, sollte der Vorfall publik werden.

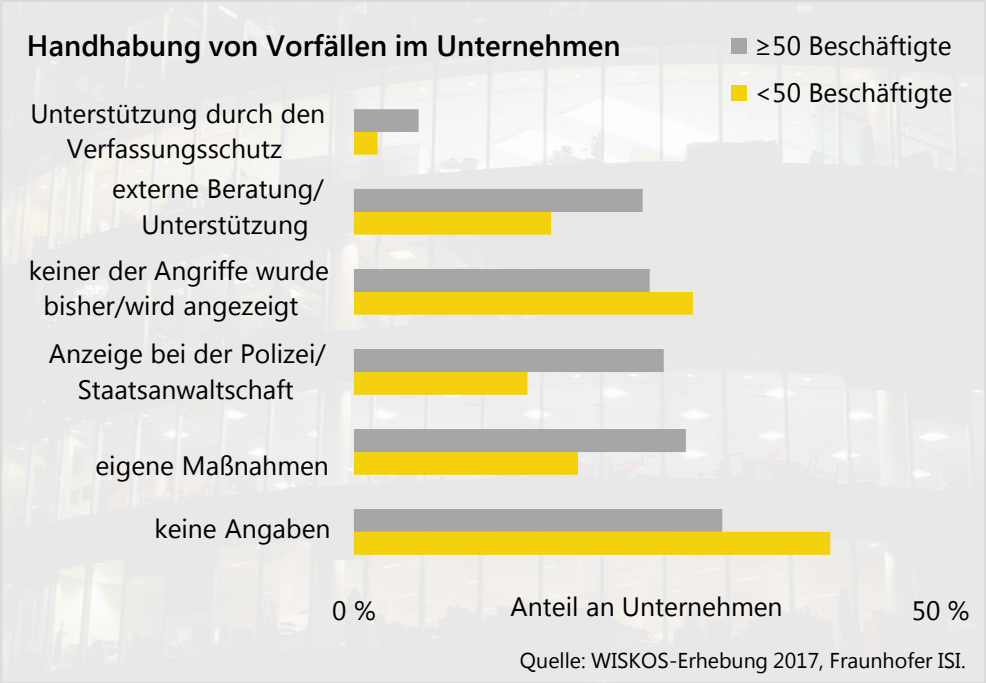
Die geringe Zahl der Betroffenen, die sich bei einem Vorfall an staatliche Stellen wenden, ist mittel- bis langfristig ein Problem, denn die Behörden können nur dann erfolgreich arbeiten, wenn sie auch Kenntnis von den Delikten haben. Auch die finanzielle und personelle Ausstattung der Ermittlungsbehörden ist abhängig von den tatsächlichen Fallzahlen. Aus eigener Kraft bzw. mit Hilfe von privaten Experten können zwar Lösungen erarbeitet und Gefahren eingedämmt werden, jedoch ist keine strafrechtliche Verfolgung der Täter möglich. Auch ein systematisches Vorgehen gegenüber Bedrohungen durch gezieltes Handeln anderer Staaten ist so ausgeschlossen. Die Behörden sind daher gefragt, über das eigene Aufgabengebiet und die bestehenden Kooperationsmöglichkeiten aufzuklären und untereinander ein einheitliches Vorgehen und eine einheitliche Kommunikation abzustimmen.

Abbildung 22: Art der Handhabung von Vorfällen in den Unternehmen



Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

Abbildung 23: Art der Handhabung von Vorfällen nach Unternehmensgröße

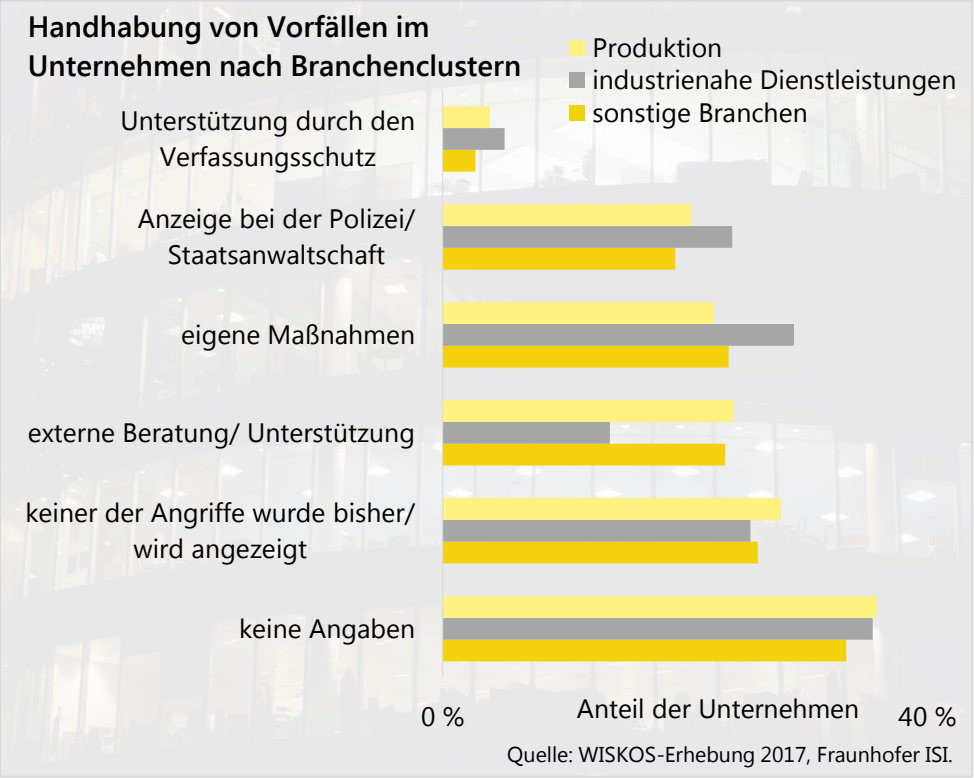


Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

Bei der Differenzierung nach Unternehmensgröße zeigen sich geringfügige Unterschiede zwischen sehr kleinen und mittelständischen Unternehmen (s. Abbildung 23). Vor allem die kleinen Unternehmen agieren sehr zögerlich bis abneigend gegenüber einer Anzeige bei der Polizei oder Staatsanwaltschaft, auch die Angebote des Verfassungsschutzes werden kaum in Anspruch genommen.

Untersucht nach Branchenclustern zeigt sich ebenfalls eine leichte Differenzierung: Die industrienahen Dienstleister nehmen weniger externe Beratung durch Dritte als die anderen Cluster in Anspruch und regeln die Vorfälle dafür häufiger mit eigenen Maßnahmen (s. Abbildung 24). Ebenfalls weist genau dieses Cluster eine stärkere Kooperationsbereitschaft mit Behörden auf.

Abbildung 24: Art der Handhabung von Vorfällen nach Branchenclustern

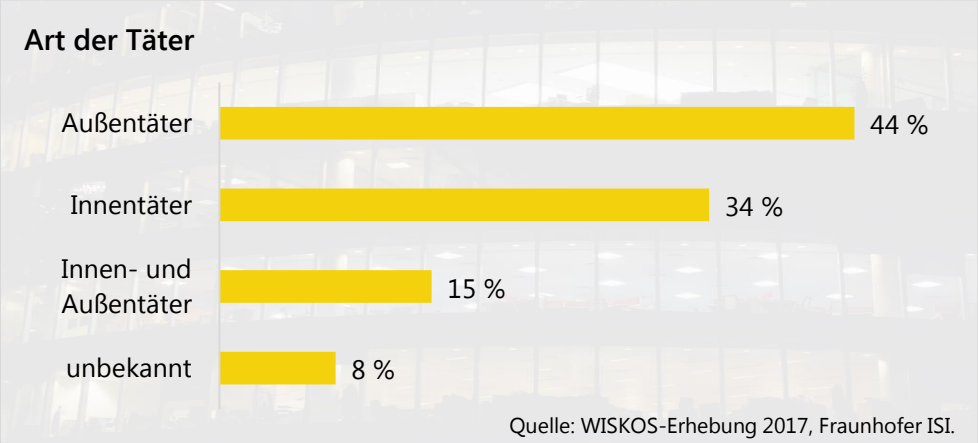


Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

Der Angreifer bei Wirtschaftsspionage und Konkurrenzausspähung ist bei weitem nicht immer der große Unbekannte. In vielen Fällen stammt der Täter sogar aus dem unternehmerischen Umfeld: seien es eigene (auch ehemalige) Beschäftigte, Beschäftigte von Drittfirmen, Wettbewerber oder gar Kunden. Diese Täter sind besonders gefährlich, können sie doch die Lage des Unternehmens und den Wert der einzelnen zu erlangenden Informationen besonders gut einschätzen. Eine Differenzierung auf dieser Ebene ist jedoch nicht valide, da sie zu sehr von Spekulationen geprägt ist. Daher wurde bei der Befragung auf die strafrechtlich etablierte Einstufung über Außen- und Innentäter zurückgegriffen. Ein Innentäter ist in diesem Kontext eine Person, die eine (noch) bestehende Rolle innerhalb des Unternehmens missbraucht, um sich selbst oder Dritten Informationen oder einen Zugang zu diesen zu verschaffen. Korrespondierend dazu kennzeichnet den Außentäter, dass er über keine spezielle Vertrauensstellung innerhalb des Unternehmens verfügt und daher versucht, auf anderem Weg Zugang zu vertraulichen Informationen zu erhalten. Eine Kombination liegt vor, wenn z.B. Beschäftigte durch einen Außentäter in ein Unternehmen eingeschleust werden, welche fortan als Innentäter weiter agieren oder auch beim bewussten oder unbewussten Zusammenwirken von beiden (z.B. durch social engineering).

Abbildung 25 auf der nachfolgenden Seite zeigt die immense Rolle, die Innentäter bei Fällen der Wirtschaftsspionage und Konkurrenzausspähung spielen: In fast jedem zweiten Vorfall ist ein Innentäter beteiligt (Innentäter und Kombinationen von Außen- und Innentäter).

Abbildung 25: Vermutung zur Art der Täter



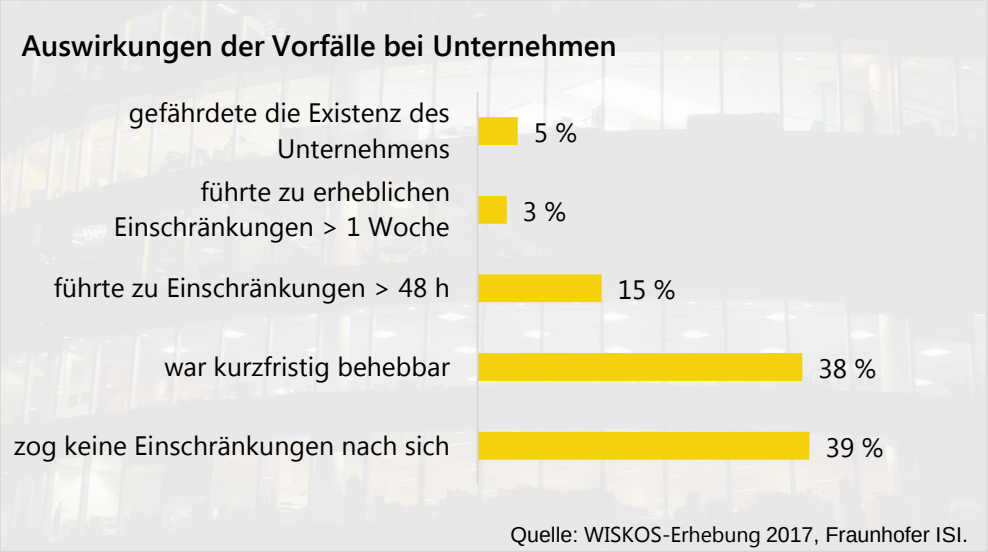
Vorfälle mit Beteiligung von Innentätern erfolgen längst nicht immer mit böser Absicht. Eine Beteiligung kann auch durch Unvorsichtigkeit, Fahrlässigkeit und Unwissen entstehen. Daran anknüpfend können Unternehmen ihre Präventionsmaßnahmen ausbauen und justieren, mit dem Ziel, die Sicherheit im Unternehmen zu erhöhen.

Ein weiterer Anhaltspunkt für die Entwicklung von Präventionsmaßnahmen im Unternehmen ist der inhaltliche Zusammenhang mit anderen Aktivitäten, wie er von den befragten Unternehmen festgestellt wurde (s. Abbildung 26). Es konnte kein signifikanter Unterschied zwischen kleinen und größeren KMU festgestellt werden. Messen, Auslandsreisen und die Teilnahme an Wirtschaftsdelegationen werden nicht als kritisch angesehen, wohl aber der Einsatz privater Geräte wie Smartphones oder Tablets. Bei letzterem konnte ein Viertel der Unternehmen einen Zusammenhang mit Angriffen feststellen.

Abbildung 26: Zusammenhang von Vorfällen mit anderen Aktivitäten

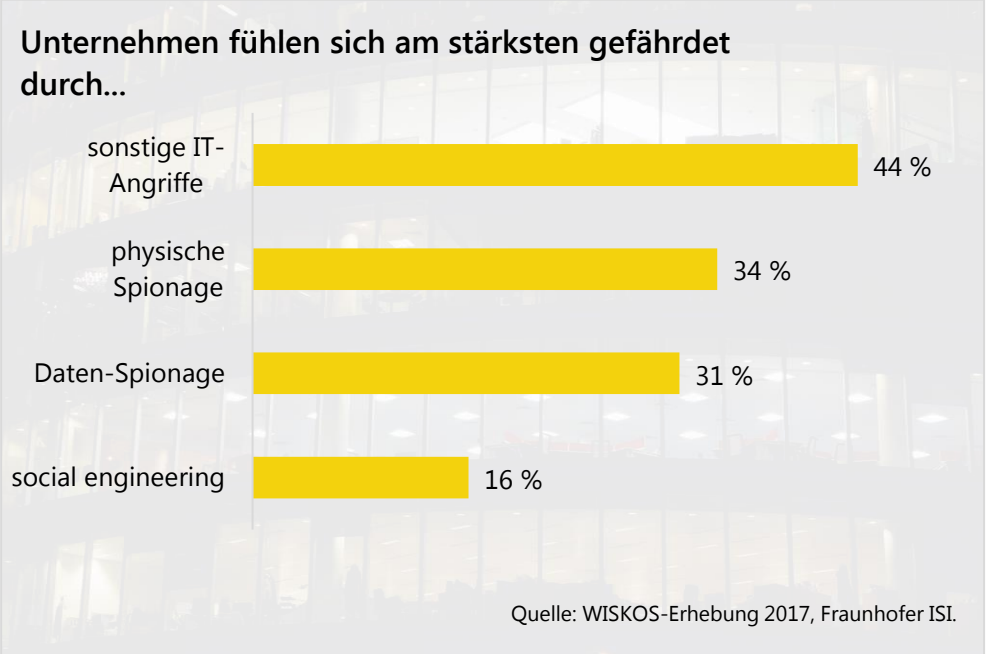
KMU fällt es schwer, die Schäden durch Wirtschaftsspionage und Konkurrenzausspähung zu beziffern oder der Thematik überhaupt eindeutig zuzuordnen. Die existierenden Hochrechnungen dazu beruhen auf Schätzungen und den Erfahrungen von Großunternehmen. Daher wurde im Rahmen der Befragung bewusst nicht auf die Schadenshöhe abgestellt, sondern auf die wahrgenommenen Einschränkungen im Geschäftsbetrieb, die der Angriff bzw. der versuchte Angriff mit sich brachte. Fünf Prozent der Unternehmen, die bereits einen Angriff oder Versuch wahrgenommen haben, haben diesen in einer Form erlebt, die existenzbedrohliche Auswirkungen hatte. Insgesamt erlitten knapp ein Viertel der bereits angegriffenen Unternehmen einen Schaden in Form von Einschränkungen im Geschäftsbetrieb von mehr als 48 Stunden (s. Abbildung 27).

Abbildung 27: Auswirkungen der Vorfälle für die Unternehmen



In der Wahrnehmung der KMU verlagert sich die Gefahr immer weiter in die Richtung von IT-Angriffen: 44 Prozent der Unternehmen geben an, in diffusen IT-Angriffen die größte Gefährdung für ihr Unternehmen zu sehen (s. Abbildung 28). Dies ist bemerkenswert, zumal die Gefahr der gezielten Daten-Spionage mit 31 Prozent geringer eingeschätzt wird. Die Gefahr der physischen Spionage liegt mit 34 Prozent an zweiter Stelle. Die Antworten zu den elektronischen Spionageformen (sonstige IT-Angriffe und Daten-Spionage) zeigen mit 75 Prozent deutlich, wie hochaktuell die Gefahr eines elektronischen Angriffs eingeschätzt wird.

Abbildung 28: Wahrgenommene Gefährdung



Zusammenfassend bleibt festzuhalten, dass sich kein Unternehmen sicher fühlen kann, da Informationsabfluss auf sehr vielen Wegen stattfinden kann und stattfindet. Selbst wenn bei einem Vorfall oder Verdachtsfall ein Schaden nicht unmittelbar feststellbar ist, sollten trotzdem die Strafverfolgungsbehörden sofort informiert werden. Hier laufen die Informationen über Gefährdungen, Vorgehensweisen und mögliche potenzielle Ziele zusammen.

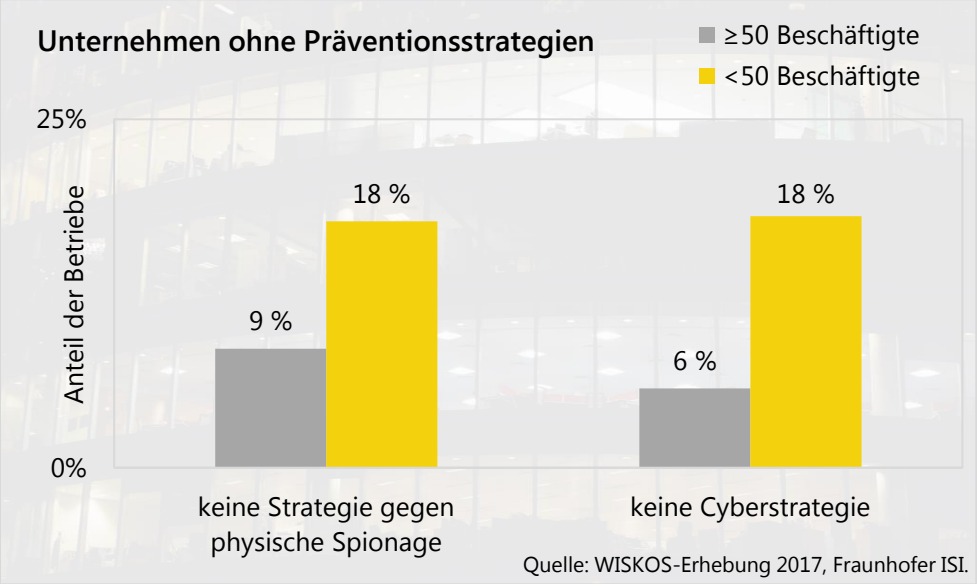
3.4 Präventionsstrategien bei KMU

Es liegt auf der Hand, dass nicht jedes Unternehmen gleich gut gegen Spionage geschützt ist und dass auch nicht alle Präventionsmaßnahmen für jedes Unternehmen sinnvoll sind. Dennoch benötigt jedes Unternehmen eine Präventionsstrategie, die Maßnahmen verschiedenster Disziplinen umfasst. Nur so kann sichergestellt werden, dass sowohl der Informationsabfluss auf digitalem Weg, als auch durch physische

Spionage eingegrenzt werden kann. Die Koordination aller Maßnahmen sollte aus einer Hand erfolgen, idealerweise durch die Geschäftsführung.

Erstaunlich ist vor allem, dass gerade bei den kleinen Unternehmen unter 50 Beschäftigten annähernd jedes fünfte Unternehmen weder eine Strategie zur Prävention vor physischer Spionage noch eine Strategie zur Prävention vor Cyberspionage hat (s. Abbildung 29). Bei den größeren Mittelständlern mit 50 oder mehr Beschäftigten scheint das Thema Prävention schon präsenter zu sein, hier fehlt es nur noch einem kleinen Teil an Strategien. Diese Feststellung allein lässt allerdings noch keinerlei Aussage über die Wirksamkeit bzw. Aktualität der Maßnahmen zu und kann daher nur als Indiz für den Grad der Sensibilisierung der Unternehmen gewertet werden.

Abbildung 29: Anteil Unternehmen ohne Präventionsstrategien

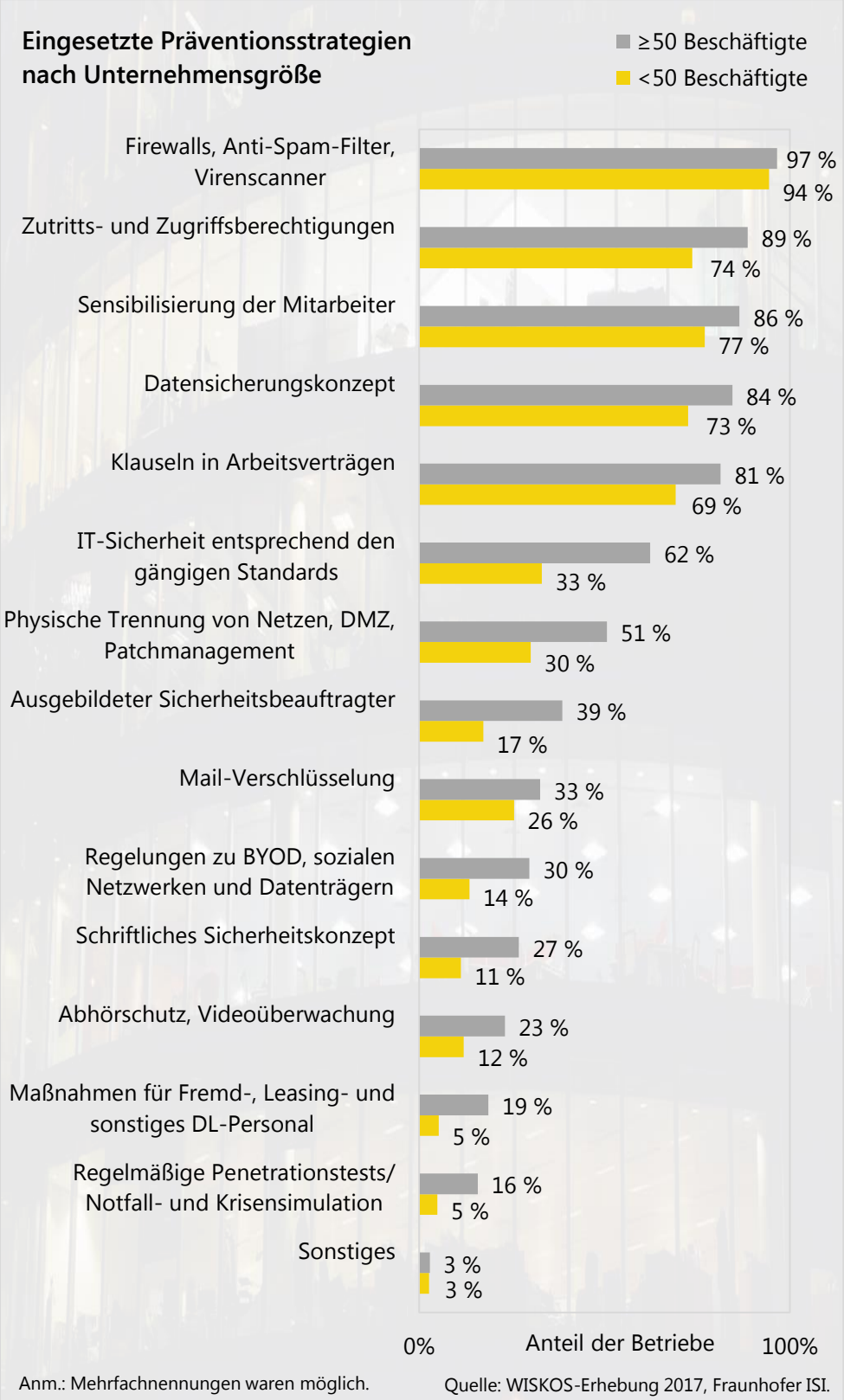


Ein Blick auf die Ebene der einzelnen Maßnahmen lässt auch hier z.T. gravierende Unterschiede zwischen den kleinen Unternehmen und den Mittelständlern ab 50 Beschäftigten erkennen (s. Abbildung 30):

Während die Basis-Maßnahmen der IT-Sicherheit in Form von Firewalls, Virenscannern und automatischer E-Mail-Filterung tatsächlich fast überall im Einsatz sind, lichten sich die Reihen – insbesondere bei den kleinen Unternehmen – danach sehr rasch. So haben z.B. nur knapp drei Viertel der Kleinunternehmen organisatorische Maßnahmen für Zutritts- oder Zugriffsbeschränkungen realisiert. Dabei ist zumindest die Beschränkung der Zugriffsberechtigungen auf Daten in Netzwerken leicht und ohne großen Aufwand umzusetzen. Ähnliches gilt für die Sensibilisierung der Beschäftigten. Dieser Bereich bietet vielfältige und kostengünstige Möglichkeiten, die wirksam umsetzbar sind. Unternehmen können hier nicht ex ante auf ein gemeinsames Verständnis vertrauen, da nicht alle Beschäftigten den gleichen Weitblick in Bezug auf die Sensibilität der Informationen haben. Mit einer klaren Vorgabe, was schutzwürdig ist und wie mit den Informationen umzugehen ist, ggf. unterteilt in mehrere Schutzstufen, kann ein einheitliches Basis-Schutzniveau im Unternehmen geschaffen werden.

Offene Tore finden Angreifer vor allem im Bereich der IT-Sicherheit vor: Hier reichen der betriebene Aufwand und die bereits getätigten Investitionen der Unternehmen bei weitem nicht aus. Während bei den größeren Mittelständlern immerhin noch 62 Prozent die gängigen Standards der IT-Sicherheit umgesetzt haben, so sind dies bei den kleinen Unternehmen nur 33 Prozent. Diese Beobachtung setzt sich im Bereich IT bzw. Digitalisierung in der Produktion fort: Bei den größeren Unternehmen praktiziert nur jedes zweite eine physische Trennung der Netze bzw. nutzt eine demilitarisierte Zone (DMZ) für die Systeme der Produktion. Bei den kleinen trifft dies sogar nur auf jedes dritte Unternehmen zu. Fehlende Präventionsmaßnahmen bei der Mehrzahl der Unternehmen ziehen sich durch alle Bereiche hindurch. Sofern diese mit größeren Investitionen oder einer starken Bindung von personellen Ressourcen (z.B. Ausbildung und Beschäftigung eines Sicherheitsbe-

Abbildung 30: Eingesetzte Präventionsmaßnahmen nach Unternehmensgröße



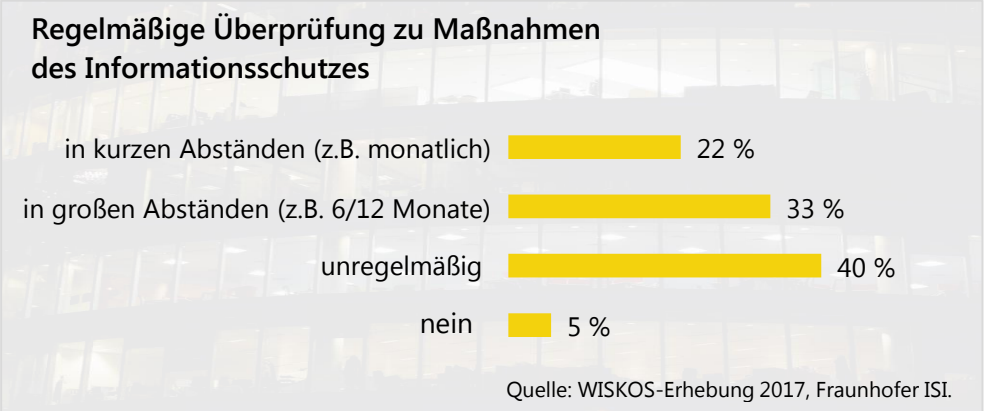
Anm.: Mehrfachnennungen waren möglich.

Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

auftragten) einhergehen, mag das noch nachvollziehbar sein, nicht jedoch bei wiederkehrenden und standardisierbaren Aufgaben, wie z.B. regelmäßigen Penetrationstests oder einmalig einzuführenden und nachzuhaltenden Regelungen zur Nutzung eigener IT-Geräte oder zu Informationsschutzregeln in Bezug auf Dritt- und Fremdpersonal. Hier ist die Lücke zwischen Soll- und Ist-Zustand so groß, dass unmittelbarer Handlungsbedarf besteht.

Auch in Sachen der Fortschreibung bzw. der Überprüfung der Maßnahmen sind KMU deutlich zu abwartend und zu passiv: Nur jedes fünfte Unternehmen überprüft seine Maßnahmen im Monatsrhythmus, ein Drittel aller Unternehmen überprüft diese immerhin noch ein- bis zweimal pro Jahr, knapp 40 Prozent nur unregelmäßig und fünf Prozent nehmen überhaupt keine Überprüfung oder Aktualisierung ihrer Maßnahmen vor (s. Abbildung 31).

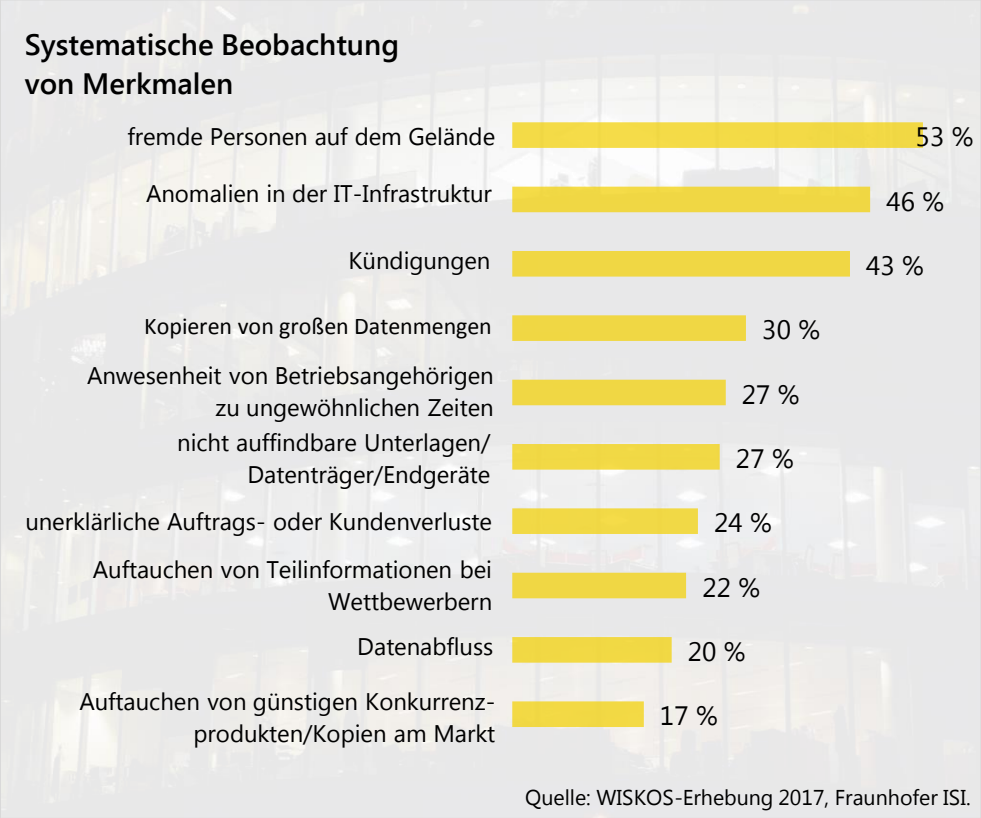
Abbildung 31: Häufigkeit der Überprüfung von Maßnahmen



Ebenfalls Nachholbedarf besteht in Sachen Monitoring. Die Beobachtung einfacher Indikatoren kann ein Unternehmen dazu befähigen, einen Angriff schnell zu identifizieren und den Schaden zu verhindern bzw. zu begrenzen. In fast allen durch die Unternehmen berichteten Fällen wurde deutlich, dass einem identifizierten Vorfall ein auffälliges Verhalten oder eine entsprechende Aktion vorausging, dem

oder der keine oder nicht genügend Aufmerksamkeit zugemessen wurde. Abbildung 32 zeigt, dass bei jedem zweiten Unternehmen fremden Personen auf dem Betriebsgelände keine Aufmerksamkeit zukommt. In ähnlich geringer Größenordnung werden Anomalien in der IT-Infrastruktur systematisch beobachtet, auch wenn hier die größeren noch etwas besser aufgestellt sind als die kleinen Unternehmen.

Abbildung 32: Arten der Überprüfung



Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

Die permanente Marktbeobachtung sollte eigentlich eine Standard-Aufgabe für Marketing und Vertrieb darstellen. Es ist daher nicht rational zu erklären, warum Auftrags- und Kundenverlusten nicht aufmerksam nachgegangen wird, ebenso der Feststellung, dass interne Informationen beim Wettbewerber auftauchen. Besonders erschreckend ist, dass nur knapp 17 Prozent der Unternehmen systematisch

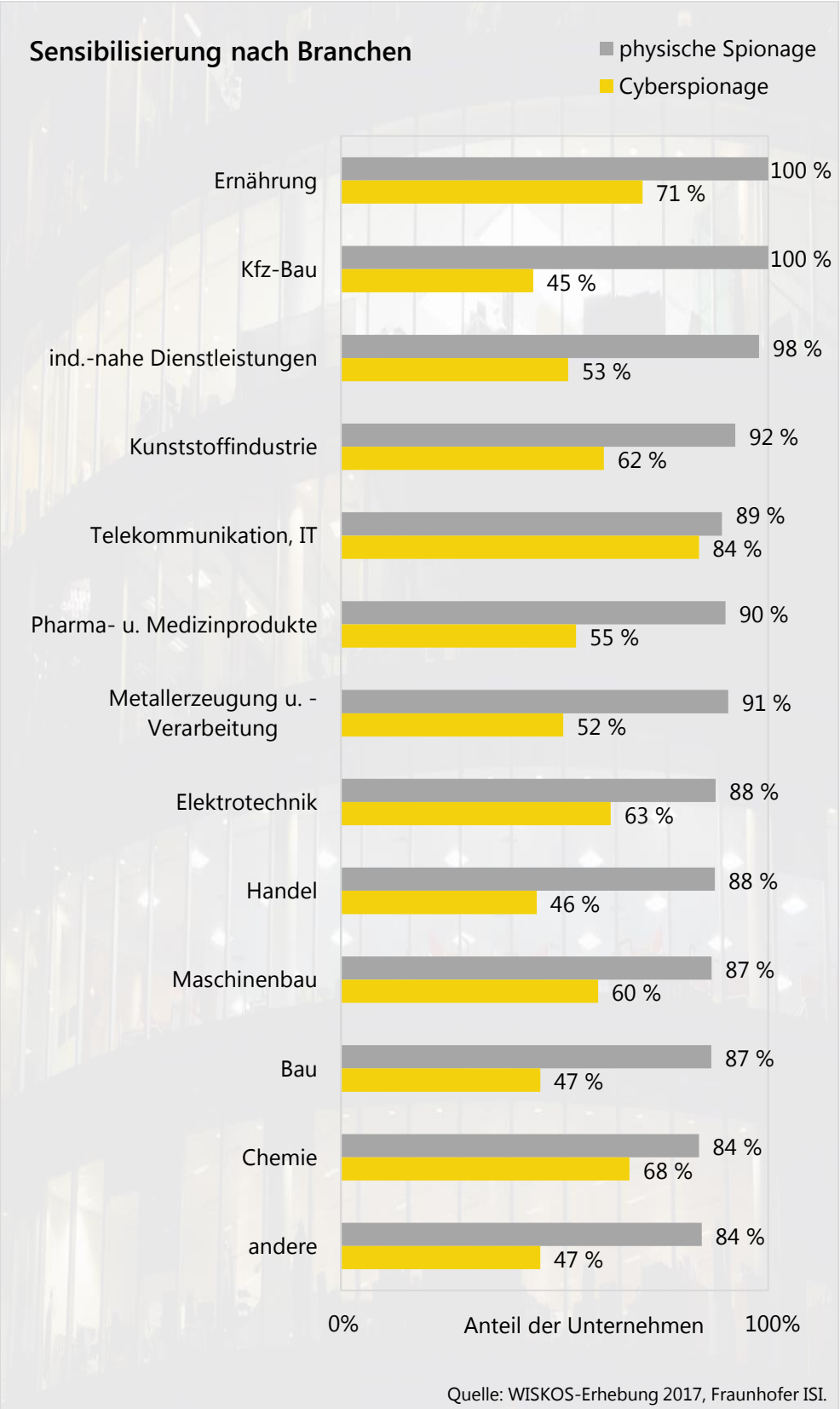
das Auftauchen von Konkurrenzprodukten oder gar Kopien auf dem Markt beobachten, um frühzeitig agieren zu können.

Auch den eigenen Beschäftigten wird (zu) wenig Aufmerksamkeit zuteil: Bei weniger als einem Drittel der Unternehmen werden Indikatoren wie das Kopieren großer Datenmengen, der Verlust von Unterlagen, Datenträgern oder Endgeräten oder die Anwesenheit von Betriebsangehörigen zu ungewöhnlichen Zeiten beobachtet.

Zusammengefasst zeigt sich, dass es gerade bei den kleinen Unternehmen an Präventionsstrategien fehlt: Jedes fünfte Unternehmen unter 50 Beschäftigten hat noch gar keine Strategie gegen physische Spionage, nur wenige mehr verfügen über eine Präventionsstrategie gegen Cyberspionage, wie Abbildung 29 verdeutlichte. Die dabei zugrunde gelegte Annahme ist, dass ein systematisches Handeln bereits dann vorliegt, wenn mindestens drei der Maßnahmen und/oder Merkmale einer Kategorie bejaht wurden.

Eine branchendifferenzierte Betrachtung (s. Abbildung 33) zeigt auf, dass in allen Branchen das Bewusstsein für physische Spionage stärker ausgeprägt ist als das für Cyberspionage. Dies entspricht auch der oben untersuchten Nutzung der Präventionsstrategien. Auffallend gering ist jedoch das Bewusstsein für Cyberspionage: In den meisten Branchen ist hierfür nur jedes zweite Unternehmen sensibilisiert. Über die Gründe lässt sich nur mutmaßen: Zum einen ist die Bedrohung diffus und meist zunächst nicht von alltäglichen Spam- und Virenangriffen zu unterscheiden, zum anderen stimmt der Zeitpunkt des Angriffs oftmals nicht mit dem Zeitpunkt des Bemerkens des Vorfalls bzw. des Schadens überein, so dass es schwerfällt, die Verknüpfung herzustellen. Berichterstattungen in der Fachpresse scheinen für KMU inhaltlich aus diversen Gründen, wie z.B. der Unternehmensgröße oder Markt- und Markenpräsenz, nicht anzusprechen, sodass sie sich nicht im Fo-

Abbildung 33: Sensibilisierung nach Branchen



Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

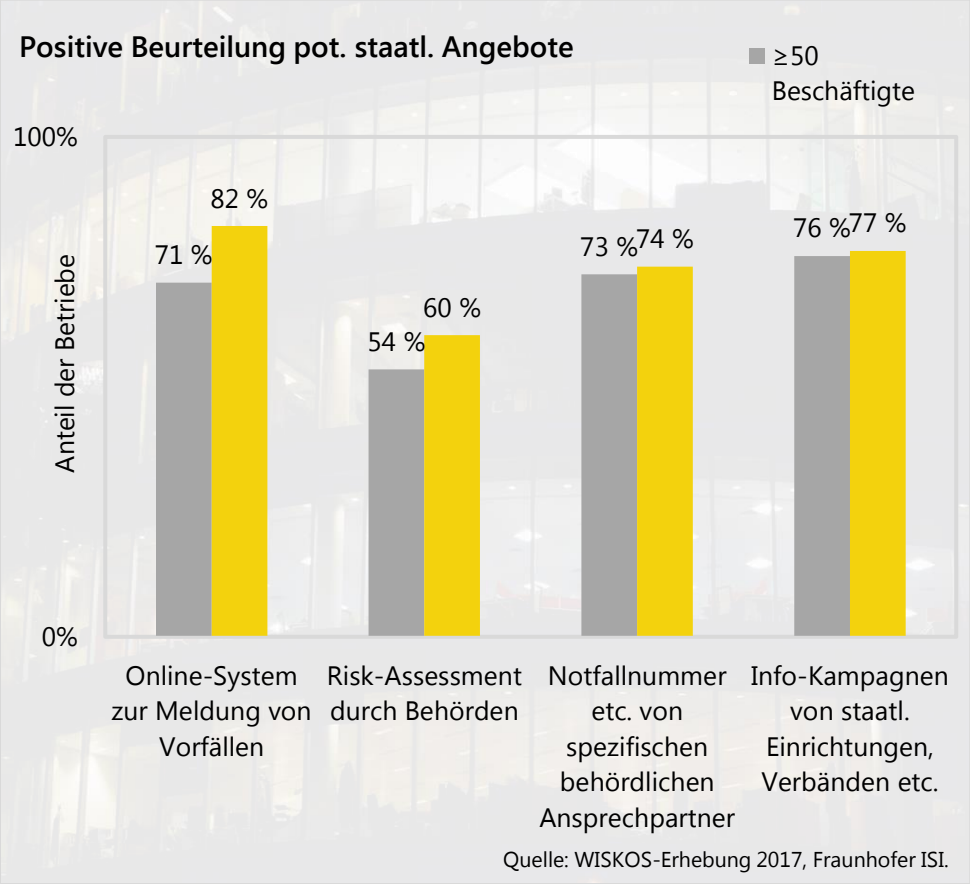
kus der Angreifer vermuten. Gerade für die Gruppe der Hidden Champions und der zahlreichen Technologieanbieter in Nischenmärkten könnte dies jedoch schnell zum Verhängnis werden.

Vor diesem Hintergrund stellt sich die Frage, welche Rolle staatliche Behörden im Kontext von Präventionsarbeit spielen können und sollten. Diese kann und darf nicht allein auf die Strafverfolgung reduziert werden, zumal sich in der Vergangenheit gezeigt hat, dass das entstehende Dunkelfeld kaum noch zu überblicken ist im Sinne der Aufgabe der Gefahrenabwehr. Wie die Vorarbeiten[1] zu dieser Studie gezeigt haben, bieten sich große Potenziale in der aktiven Präventionsarbeit der Behörden, um Vertrauen zu etablieren und Kooperationen anzubahnen. Diese Potenziale wurden nun erstmals hinsichtlich ihrer Akzeptanz durch Unternehmen überprüft. Es zeigt sich eine durchaus sehr positive Beurteilung von exemplarischen staatlichen Angeboten über alle Branchen und Unternehmensgrößen hinweg (s. Abbildung 34).

Eine im Vorfeld geäußerte Vermutung, deutsche Unternehmen würden staatliche Einblicke in die Unternehmen, wie sie z.B. in der Schweiz durch den Verfassungsschutz üblich sind, ablehnen, konnte nicht bestätigt werden. Im Gegenteil: Am Beispiel des abgefragten (und in Dänemark in bestimmten Unternehmensgruppen bereits etablierten) Risk-Assessments durch Behörden ist eine große Zustimmung ersichtlich. Mehr als jeder zweite der größeren Mittelständler und sogar mehr als 60 Prozent der kleinen Unternehmen bewerteten eine solch tiefgreifende Maßnahme als positiv (in Schulnoten 1 bis 3), selbst wenn sie hierfür den Staatsorganen Einblick in die unternehmensinternen Prozesse und Daten geben müssten.

1 | *Wallwaey, E., Bollhöfer, E. & Knickmeier, S.* (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin 2018 (Duncker & Humblot).

Abbildung 34: Zustimmung zu möglichen staatlichen Angeboten



Ergänzend sei angemerkt, dass Unternehmen, die bereits einen Vorfall der Konkurrenzausspähung oder der Wirtschaftsspionage zu verzeichnen hatten, in ihrer Beurteilung nicht von jenen. die nicht bzw. noch nicht betroffen waren oder sind, abweichen.

Im Einzelnen wurden die verschiedenen potenziellen Angebote wie folgt bewertet (s. Abbildung 35 bis Abbildung 38):

Abbildung 35: Bewertung von Informationskampagnen

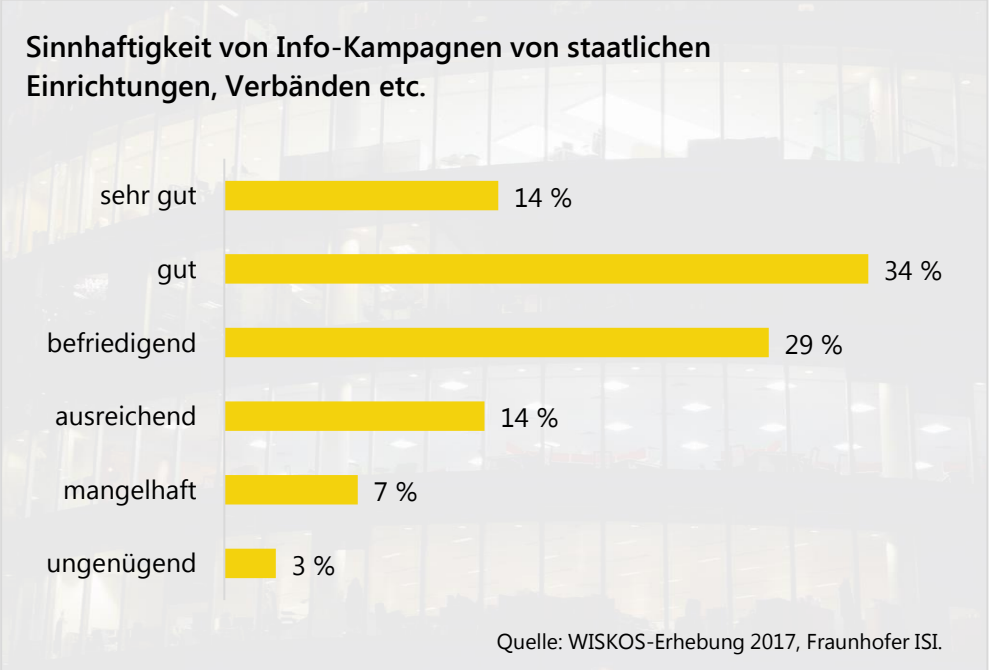
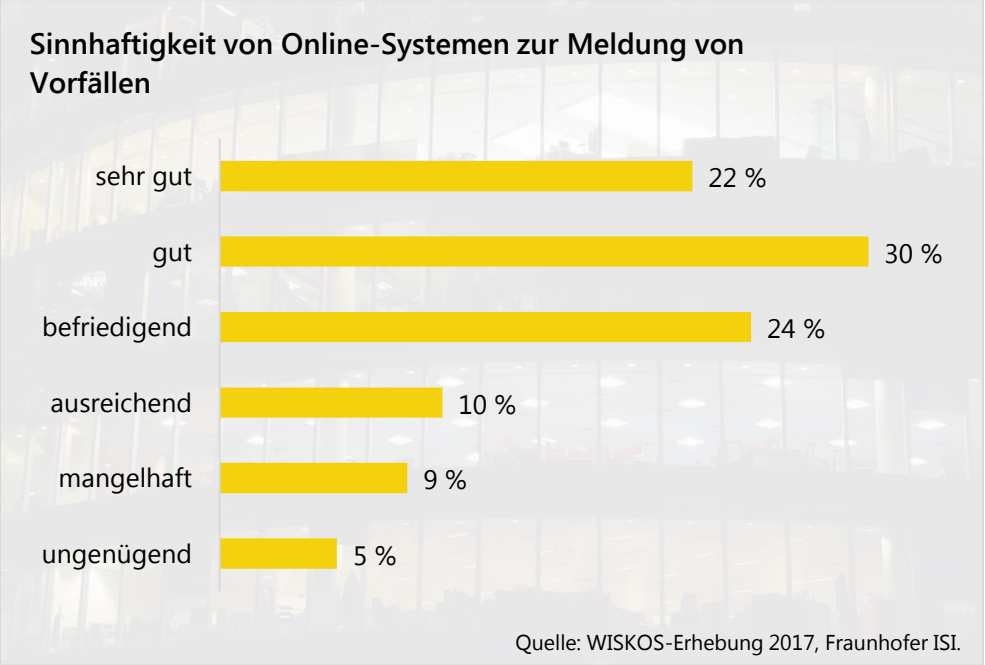


Abbildung 36: Bewertung von spezifischen Notfallnummern und Ansprechpartnern

Abbildung 37: Bewertung von Online-Systemen zur Meldung von Vorfällen



Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

Abbildung 38: Bewertung von Risk-Assessments durch Behörden

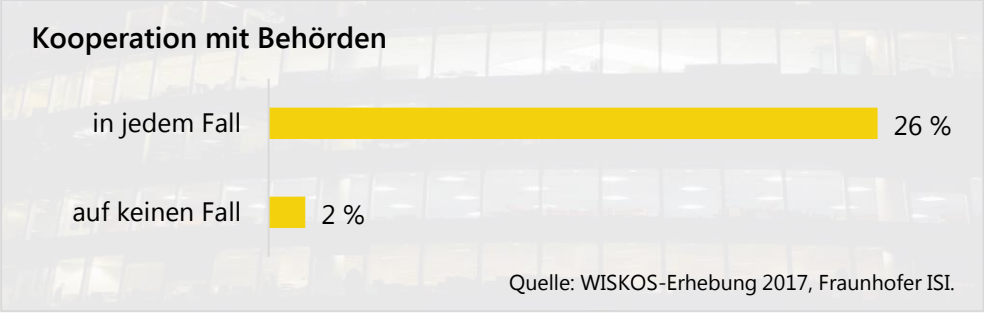
Quelle: WISKOS-Erhebung 2017, Fraunhofer ISI.

3.5 Potenziale für Kooperationen mit Behörden

Die oben angesprochenen bestehenden Potenziale für die Verbesserung der Kooperation zwischen Unternehmen und Behörden sollen im Folgenden (Kapitel 3.5.1) näher beleuchtet werden, bevor dann in Kapitel 3.5.2 noch auf die zu überwindenden Hemmschwellen eingegangen wird.

Die Unternehmen stehen einer Kooperation mit Behörden in Fragen der Wirtschaftsspionage und Konkurrenzausspähung sehr positiv gegenüber: lediglich zwei Prozent lehnen eine Kooperation kategorisch ab, mehr als ein Viertel der Unternehmen würde sogar in jedem Fall kooperieren (s. Abbildung 39). Hier gilt es anzusetzen, um das große Mittelfeld zu erreichen.

Abbildung 39: Bereitschaft zur Kooperation mit Behörden



3.5.1 Pro Kooperation

Im Bereich der Möglichkeiten für eine zukünftige Kooperation wurden die Unternehmen aufgefordert anzukreuzen, unter welchen Voraussetzungen sie zukünftig eine Kooperation mit Behörden anstreben werden. Mehrfachnennungen waren hier möglich. Zur Kooperation

motivierende Faktoren können in verschiedenen Bereichen ausgemacht werden. Eine primär wirtschaftliche Kosten-Nutzen-Betrachtung konnte nicht festgestellt werden, wenn auch bei über der Hälfte der Nennungen der Schaden mit dem Aufwand für die Kooperation korrelieren sollte (s. Abbildung 40). Von ähnlich hoher Relevanz sind Überlegungen, die im Behördenbild begründet sind: der Glaube an die Erfolgschancen der Ermittlungen, die zeitnahe Bearbeitung der Vorfälle und eine unbürokratische Meldung von Vorfällen fördern die Kooperationsbereitschaft. Erst danach folgen Erwägungen zum eigenen Nutzen durch die Kooperation in Form von Erwartungen bezüglich der Verbesserung der eigenen Präventionsstrategien mit 42 Prozent.

42 Prozent der Unternehmen lassen sich durch einen existenzbedrohenden Schaden von einer Kooperation überzeugen. Dies kann in zweierlei Richtung interpretiert werden: Zum einen, dass das Unternehmen dann aus eigener Kraft nicht mehr handlungsfähig ist und sich in dieser Situation an den Staat als Notnagel klammert, oder aber, dass erst ab einer gewissen Relevanz des Vorfalls auf staatliche Ressourcen zurückgegriffen wird unter billigender Inkaufnahme der ggf. damit verbundenen Nachteile/Probleme. Andersherum ist es erschreckend, dass knapp 60 Prozent der Unternehmen in einer solchen Situation NICHT kooperieren würden.

Ebenso zeigt sich, dass Unternehmen die Kooperation mit Behörden als verbesserungswürdig erleben und dies nicht nur vermuten. Unternehmen, die bereits einen Vorfall erlebt und im Zuge dessen mit Behörden kooperiert haben, stellen deutlich höhere Anforderungen an eine erneute Kooperation, als diejenigen, die bislang noch keinen Vorfall erlebt haben. Entweder wurde in den Fällen die erlebte Kooperation nicht den Erwartungen gerecht oder der Vorfall selbst wurde anders erlebt als erwartet bzw. befürchtet, sodass sich dies in den Anforderungen an eine zukünftige Kooperation widerspiegelt.

Etwaige formale oder rechtliche Vorgaben bei Vorfällen der Wirtschaftsspionage oder Konkurrenzausspähung würden nur ein Drittel der Betroffenen zur Kooperation bewegen. Hierzu gehören z.B. eine polizeiliche Anzeige als Bedingung für den Eintritt eines Versicherungsschutzes (29 Prozent) und eine etwaige Meldepflicht für derartige Vorfälle (24 Prozent). Eine Kooperation auf der Basis einer freiwilligen Verpflichtung der Industrie zur Meldung von Vorfällen würden sogar nur acht Prozent der Unternehmen anstreben. Dies ist einerseits eine klare Positionierung zwischen der Brisanz des Themas für die Unternehmen und des Legalverhaltens im Einzelfall, aber andererseits auch ein deutlicher Hinweis für die Behörden. Sollen das Dunkelfeld kleiner und die Gefahrenabwehr gestärkt werden, müssen sie sich auf die Unternehmen zubewegen, um diese von einer Kooperation zu überzeugen und Vertrauen zu schaffen. Über Vorschriften und Gesetze lässt sich die Kooperationsbereitschaft nicht erhöhen.

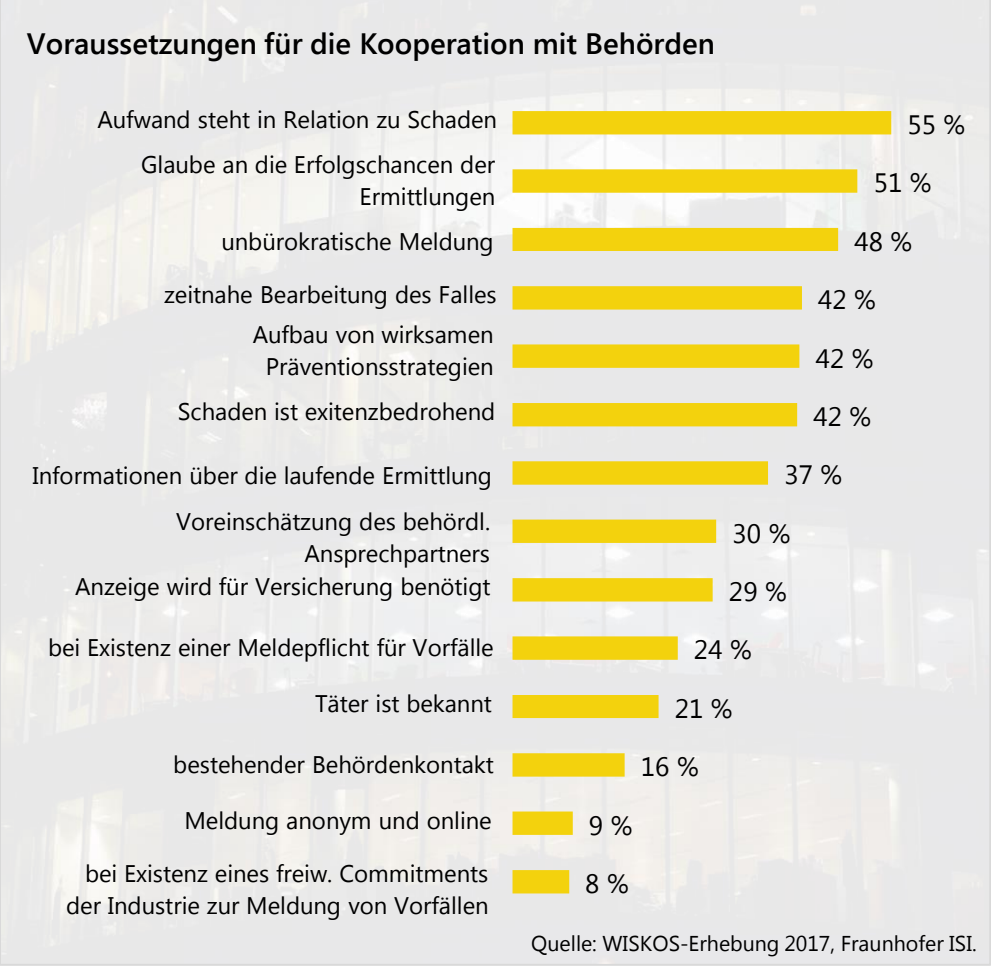
Die Bereitschaft zu kooperieren hängt nur zu einem geringen Anteil von der Kontaktform ab: Weder besteht der Wunsch nach Anonymität bei der Meldung eines Vorfalls, noch der nach einem bestehenden (aktiven) Behördenkontakt. Wobei natürlich nicht von der Hand zu weisen ist, dass ein bestehender Behördenkontakt die Kooperation bzw. die Kontaktaufnahme in Grenz- oder Verdachtsfällen auf jeden Fall deutlich erleichtert. Hier wurde jedoch nur nach der Kooperation nach einem Angriff gefragt, wobei es dann im konkreten (Schadens-) Fall nicht relevant zu sein scheint, ob bereits ein Kontakt besteht, sofern der Leidensdruck hoch genug ist.

Bei 37 Prozent der Unternehmen fördert es die Kooperationsbereitschaft, wenn sie Informationen über den Stand der laufenden Ermittlungen erhalten, 16 Prozent erwarten im Vorfeld einer Kooperation eine Voreinschätzung der Situation durch den behördlichen Ansprechpartner. Diese Zahlen stellen eindrucksvoll dar, dass die Unternehmen die behördliche Tätigkeit derzeit als Black Box wahrnehmen: Sie treten

mit einem Vorfall oder einem Verdachtsfall an die Behörden heran, ohne jedoch einschätzen zu können, was auf sie zukommt, wie die Informationen behandelt werden, welchen weiteren Aufwand sie leisten müssen und wie die Erfolgschancen tatsächlich zu beurteilen sind. Hier sind die Behörden aufgerufen, aktiv zu werden mit transparenten Prozessen und offener Kommunikation z.B. über lange Bearbeitungszeiten.

Insgesamt ist festzustellen, dass die Bereitschaft zur Kooperation bei den Unternehmen durchaus gegeben ist. Auch die Voraussetzungen, unter denen eine Kooperation bejaht wird, sind nachvollziehbar und Stück für Stück umsetzbar.

Abbildung 40: Voraussetzungen für die Kooperation



3.5.2 Hemmschwellen

So, wie es Befähiger für Kooperationen (s.o. Kapitel 3.5.1) gibt, so existieren auch Hemmschwellen für ebendiese. Daher wurden die Unternehmen explizit nach diesen befragt (s. Abbildung 41). Auch hier waren Mehrfachnennungen möglich.

Es ist nicht primär die Angst vor negativen Konsequenzen (z.B. für die eigene Fahrlässigkeit), wie es oft durch die Presse dargestellt wird, und auch nicht die Angst vor der Öffentlichkeit, vor eventuellen Imageschäden. Diese Gründe rangieren mit 21 Prozent (Reaktion der Öffentlichkeit) bzw. elf Prozent (negative Konsequenzen durch eigene Fahrlässigkeit) eher am Ende der Skala. Auch die begrenzten eigenen Kapazitäten spielen mit 17 Prozent eine geringere Rolle, als im Vorfeld der Untersuchung vermutet.

Die primäre Hemmschwelle stellen wirtschaftliche Betrachtungen dar; allem voran ein als lediglich gering eingeschätzter Schaden (58 Prozent), gefolgt von dem nur schwer einzuschätzenden Aufwand für die Kooperation mit den Behörden (50 Prozent). Neben diesem Aufwand spielen auch das Behördenbild und die Informationen über die Zuständigkeiten innerhalb der Behörden eine entscheidende Rolle: 32 Prozent gaben an, dass sie die Unklarheit über die Zuständigkeiten an einer Kooperation hindert, bzw. 29 Prozent, dass sie durch Zweifel an der Kompetenz der Behörde von einer Kooperation abgehalten werden. In denselben Bereich fallen die 31 Prozent, die die eigene Mitwirkung an der Strafverfolgung als sehr aufwändig ansehen und daher eigene Lösungen bevorzugen, und die 22 Prozent, die in „unkontrollierbaren Ermittlungen“ ein Hindernis für Kooperationen sehen.

Genau an dieser Stelle bieten sich sehr große Chancen, Hemmnisse abzubauen und Kooperationen zu fördern: Wie bereits an anderer

Abbildung 41: Hemmnisse für die Kooperation

Stelle[1] dargestellt, muss kurz- bis mittelfristig in Präventionsarbeit seitens der Behörden investiert werden. So können Informationen verbreitet und Kontakt zu den Unternehmen hergestellt werden, mit dem Ziel, eine vertrauensvolle Zusammenarbeit bereits im Vorfeld eines Vorfalls zu etablieren. Neben der direkten Kontaktaufnahme über In-

1 | *Wallwaey, E., Bollhöfer, E. & Knickmeier, S.* (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin 2018 (Duncker & Humblot).

formationsmaterialien, eigenen Veranstaltungen, Foren auf diversen Internetplattformen etc. besteht natürlich auch die Möglichkeit, über die bereits von den Unternehmen genutzten Kanäle der Verbände und Interessengemeinschaften zu agieren, ggf. diese sogar in einer Mediatorfunktion in ein Präventionskonzept zu integrieren. Nicht vermeiden lassen wird sich der Personalaufwand in dem Bereich; über einen „greifbaren" Ansprechpartner wird Vertrauen aufgebaut – sei es im Rahmen von Vorträgen, der Teilnahme an regionalen oder themenbezogenen Veranstaltungen oder informellen Treffen.

Es gilt auch auf der Seite der Unternehmen mit einigen Vorurteilen abzuschließen: Inzwischen sind die Cybercrime-Abteilungen der Landeskriminalämter (LKA) und auch die Wirtschaftsschutz-Referate bei den Verfassungsschützern des Bundes und der Länder gut auf Vorfälle des ungewollten Informationsabflusses vorbereitet und können schnell und flexibel innerhalb der Rechtsordnung reagieren.

Abbildung 42: Gruppierte Hinderungsgründe für Kooperationen

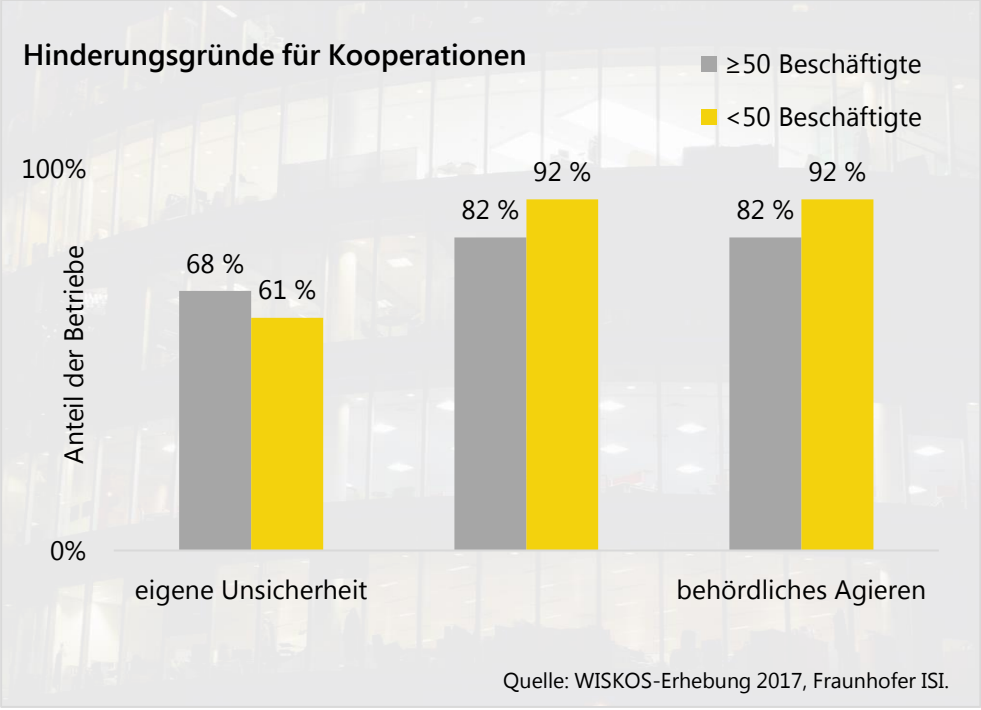
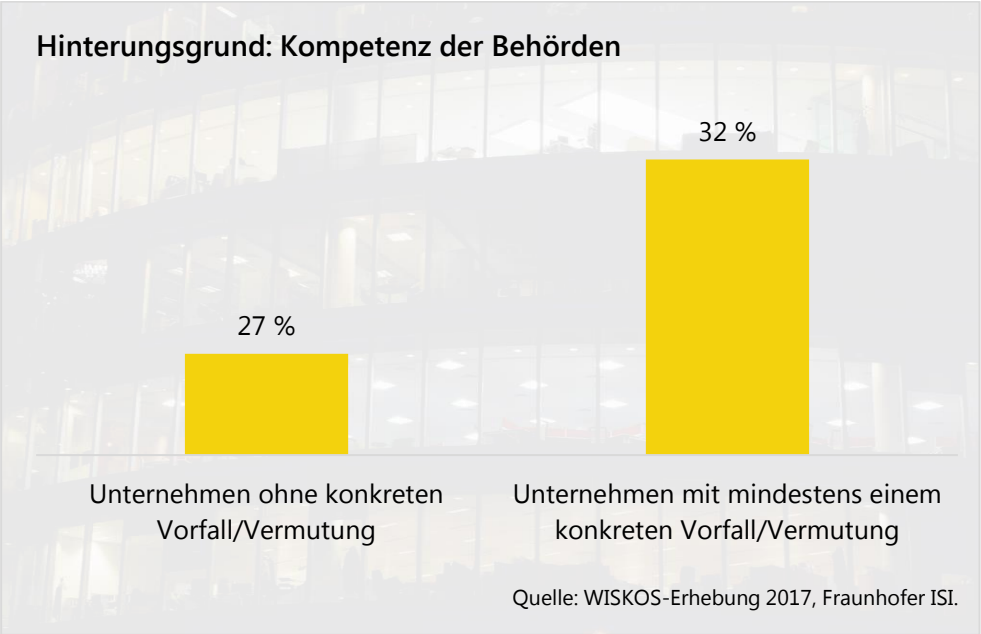


Abbildung 42 zeigt noch einmal die Hinderungsgründe für Kooperationen, gruppiert nach den drei wesentlichen Motivationsrichtungen, die gegen eine Kooperation sprechen: eigene Unsicherheit bei den Unternehmen, schlechte (erwartete) Aufwand-Nutzen-Relation und Gründe, die in der Art des behördlichen Agierens liegen. Deutlich wird, dass bei allen Unternehmen vorrangig eine schlechte Aufwand-Nutzen-Relation und die Art des behördlichen Agierens dominieren, wohingegen sich Gründe der eigenen Unsicherheit nicht ganz so stark kooperationshindernd auswirken. Ein im Ergebnis gleichlautendes Bild ergibt sich, wenn statt nach Unternehmensgröße nach Branchen (Produktion, industrienahe Dienstleister, Sonstige) oder nach bisheriger Betroffenheit (kein Vorfall, mindestens ein Vorfall oder Verdachtsfall) differenziert wird (ohne Abbildung).

Ein Hinderungsgrund soll an dieser Stelle noch detailliert betrachtet werden: die wahrgenommene Kompetenz der Behörden (s. Abbildung 43, n=452). Es zeigt sich, dass Unternehmen, die bereits einen Vorfall oder Verdachtsfall hatten, das Thema Behördenkompetenz verstärkt als Hinderungsgrund wahrnehmen. Dabei lässt sich keine Aussage treffen, ob es bei dem Vorfall tatsächlich einen Kontakt zu den Strafverfolgungsbehörden gab, oder ob lediglich von Dritten davon abgeraten wurde und dieser Rat sich meinungsbildend bei dem betroffenen Unternehmen ausgewirkt hat. Unabhängig von der tatsächlich erlebten Situation kann festgehalten werden, dass das Bild der Strafverfolgungsbehörden in der Öffentlichkeit dringend überarbeitet werden muss. Zudem wirken sich auch die unterschiedlichen Aufträge der Verfassungsschützer und der strafverfolgenden Behörden und die damit einhergehenden behördeninternen Diskussionen, die auch in Form von diametral unterschiedlichen Empfehlungen in den Außenraum gelangen, nicht förderlich für die Wahrnehmung der Kompetenz der Strafverfolgungsbehörden aus.

Abbildung 43: Kompetenz der Behörden als Hinderungsgrund



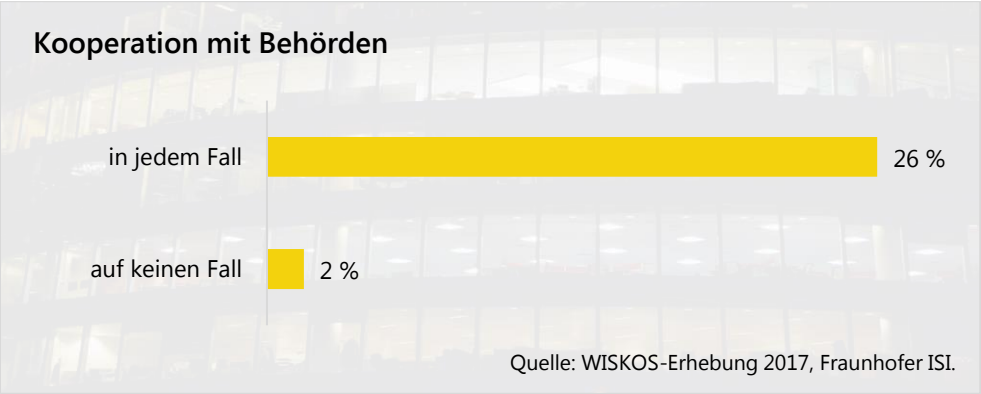
Zusammenfassend lässt sich festhalten, dass die Unternehmen auch Mehrwerte in der Kooperation mit Strafverfolgungsbehörden sehen und eine solche nicht ausschließlich auf Basis einer Kosten-Nutzen-Relation betrachten. Es bleibt jedoch die Problematik, dass die Unternehmen keinen Anlass dazu sehen, mehr als derzeit zu kooperieren, wenn nicht entweder die Motivation verstärkt oder die Hemmnisse erlebbar abgebaut werden können. In der derzeitigen Situation greifen sie auf die ihnen geläufigen Schemata zurück und bewältigen Vorfälle vorrangig mit eigenen Mitteln oder mit der Hilfe externer Dritter (s.o. Abbildung 22 ff.). Das zukünftige Verhalten ist nicht vorherzusehen und kann sich in verschiedene Richtungen entwickeln. Wahrscheinlich ist aber, dass die Anzahl an schwer zu verfolgenden, z.T. diffusen Cyberangriffen zunehmen wird und die Unternehmen sich im Schadensfall den Maßnahmen zuwenden, die ihre Bedürfnisse nach Wiederherstellung der Sicherheit, Sanktionierung des Täters/der Täter und zukünftiger wirksamer Prävention am besten erfüllen. Die Strafverfolgungsbehörden sind daher gut beraten nicht abzuwarten bis ein Unternehmen den

Kontakt herstellt, sondern aktiv und zielgruppenspezifisch auf diese zuzugehen.

3.5.3 Grenzen des Legalverhaltens

Prinzipiell sind die Unternehmen bereit, mit den Behörden zu kooperieren, um Fälle des Informationsverlustes verfolgen und aufklären zu können (s.o. Kap. 3.5). Lediglich zwei Prozent der Unternehmen lehnen eine Kooperation pauschal ab (s.u. Abbildung 44). Diese Aussage erfolgte unabhängig von einer gesetzlichen Meldepflicht.

Abbildung 44: Bereitschaft zur Kooperation mit Behörden



Fraglich ist, ob gesetzliche Regelungen in der Lage sind, die Kooperationsbereitschaft signifikant zu erhöhen. Da eine direkte Frage danach im Rahmen dieser Befragung rein hypothetisch und im Ergebnis nicht belastbar wäre, wurde der Versuch gemacht, die Grenzen des Legalverhaltens über andere Indikatoren zu ermitteln. Es wurde die Frage nach der Kooperation bei einer hypothetisch existierenden Meldepflicht sowohl bei den Befähigern für eine Kooperation, wie auch bei den Hemmnissen für diese gestellt. Im Ergebnis ist festzuhalten, dass die Existenz einer Meldepflicht für Vorfälle die Kooperationsbereitschaft nicht signifikant fördert: Nur 24 Prozent der Unternehmen würden dies als Anlass für eine Kooperation nehmen (s.o. Abbildung 40).

15 Prozent der Unternehmen räumen freimütig ein, dass sie selbst bei Existenz einer Meldepflicht nicht kooperieren würden, sofern sie den Vorfall selbst als nicht relevant einstufen.

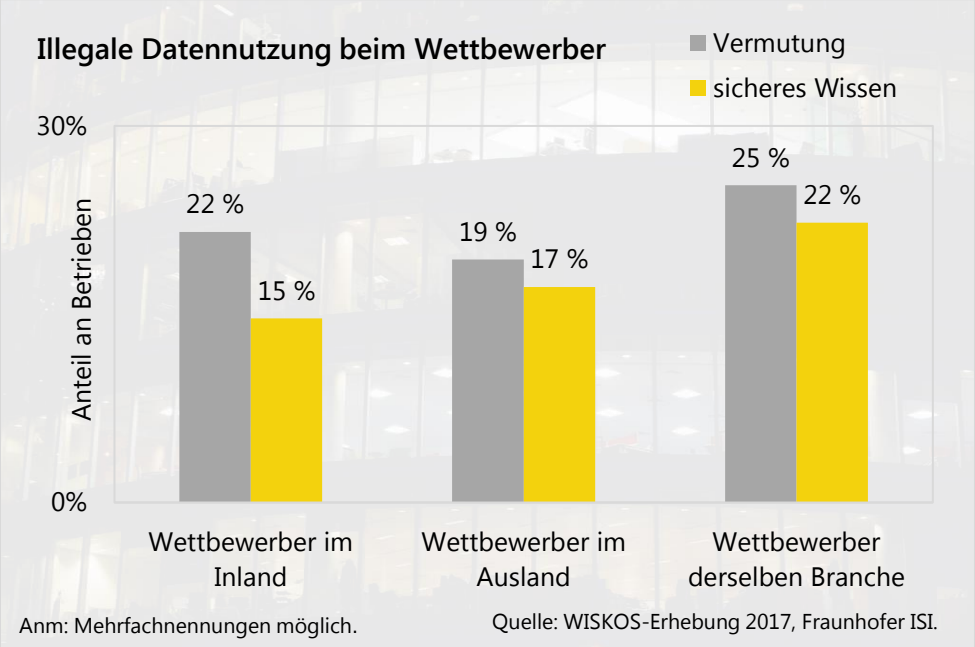
Daraus lässt sich zwar keine eindeutige Tendenz des Legalverhaltens erkennen, es wird aber deutlich, dass es auch zukünftig auf die Umstände des Einzelfalls ankommt und die oben angesprochenen Probleme der geringen Kooperationsbereitschaft nicht pauschal durch weitere Vorschriften und Meldepflichten gelöst werden können. Bei der Diskussion für oder wider weiterer Meldepflichten sollte jedoch beachtet werden, dass die Existenz formaler Vorschriften, die natürlich auch mit Konsequenzen versehen sind, bei Vorfällen automatisch weitere Kommunikation mit Rechtsberatern, anderen Stellen und/oder Dritten hervorruft. Die Strafverfolgungsbehörden würden vermutlich erst nachrangig informiert.

Wie sich jedoch oben (s. Abbildung 41) gezeigt hat, steigen die Zweifel an der Kompetenz der Behörden nicht nur durch eigene Erfahrungen, sondern u.U. auch durch Empfehlungen Dritter, nicht zu kooperieren. Eine stärkere Regulierung an dieser Stelle könnte sich also sogar kontraproduktiv auswirken.

3.6 Einflüsse durch Wettbewerber und aus dem Ausland

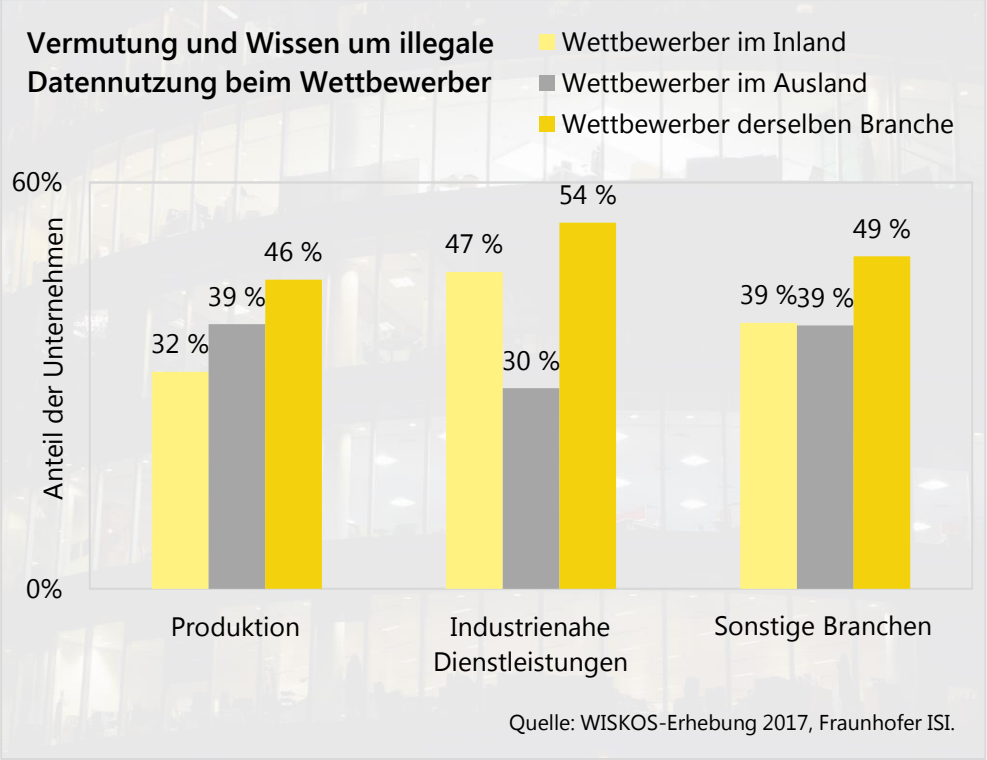
Über die Hälfte aller Unternehmen verfügen über sicheres Wissen darüber, dass mindestens ein Wettbewerber illegal beschaffte Daten und Informationen nutzt. Der Schwerpunkt liegt dabei auf Wettbewerbern der eigenen Branche, die naturgemäß auch am gründlichsten beobachtet werden. Beim Vergleich zwischen Wettbewerbern aus dem Ausland und solchen aus dem Inland ist ersichtlich, dass die Gefahr aus dem Ausland noch stärker bewertet wird als die aus dem Inland (s. Abbildung 45).

Abbildung 45: Nutzung illegal beschaffter Daten durch Wettbewerber



Dabei fürchten vor allem die industrienahen Dienstleister die Wettbewerber aus dem Inland besonders (s. Abbildung 46). Begründet sein kann dies durch die Sprache, aber auch durch den Kundenkreis. Industrienahe Dienstleister agieren (noch) vorrangig lokal und nur selten global. Vorhandenes Anwendungs- und Prozesswissen ist daher nicht immer übertragbar, jedoch wertvoll beim Kampf um denselben Kunden. Trotzdem ist diese Erkenntnis sehr interessant, denn laut den vorhergegangenen Experteninterviews fühlen sich gerade diese Dienstleister sehr gut geschützt. Dies wurde damit begründet, dass viel Wissen zu Vorgehen und Prozessen in den Köpfen stecke und damit kaum für Dritte zugänglich sei. Zusammen mit dem Wissen, dass viele Wettbewerber Daten illegal nutzen, reift die Erkenntnis, dass es in diesem Sektor doch viel relevantes Know-how zu geben scheint, das abfließen kann und dann auch von Wettbewerbern genutzt wird. Die industrienahen Dienstleister sollten daher nicht in der scheinbaren Sicherheit verharren, sondern die eigenen Prozesse unter Sicherheitsaspekten hinterfragen.

Abbildung 46: Vermutung und Wissen um illegale Datennutzung beim Wettbewerber



Im Bereich der Produktion sind es verstärkt Wettbewerber aus dem Ausland, die die Daten und Informationen anderer gezielt nutzen. 39 Prozent der Unternehmen gaben an, bei mindestens einem Wettbewerber im Ausland zumindest stark zu vermuten, dass dieser unlauter Daten und Informationen nutzt, wohingegen nur 32 Prozent dies von Wettbewerbern im Inland vermuten (s. Abbildung 46).

Spätestens ein Vorfall oder ein Verdachtsfall öffnet den Unternehmen die Augen für die unlautere Datennutzung eines oder mehrerer Wettbewerber. Abbildung 47 zeigt, dass die Unternehmen zunächst verhalten hinsichtlich eines Verdachts reagieren, das Bewusstsein jedoch durch einen Vorfall oder Verdachtsfall deutlich gesteigert wird. Dies kann bis zu 28 Prozentpunkte an Differenz ausmachen (s. Abbildung 47 – Wettbewerber im Inland). Unabhängig vom Tätigkeitsbereich müssen sich die Unternehmen jedoch fragen lassen, wie es sein

kann, dass trotz dieses Bewusstseins der Schutz der eigenen Informationen erhebliche Mängel aufweist (s.o. Abbildung 29 und Abbildung 30).

Abbildung 47: Vermutung und Wissen um illegale Datennutzung beim Wettbewerber nach Betroffenheit

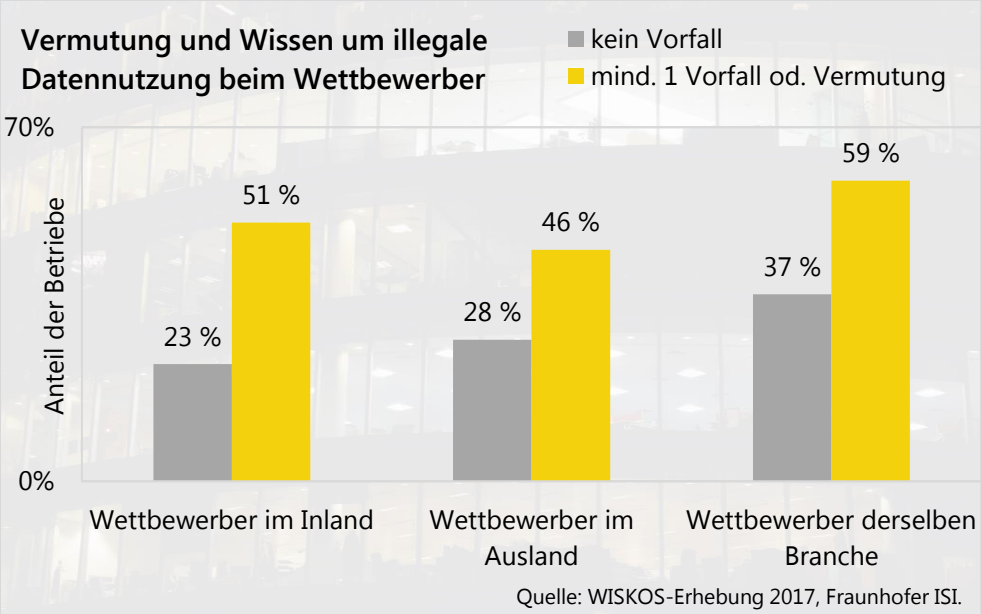
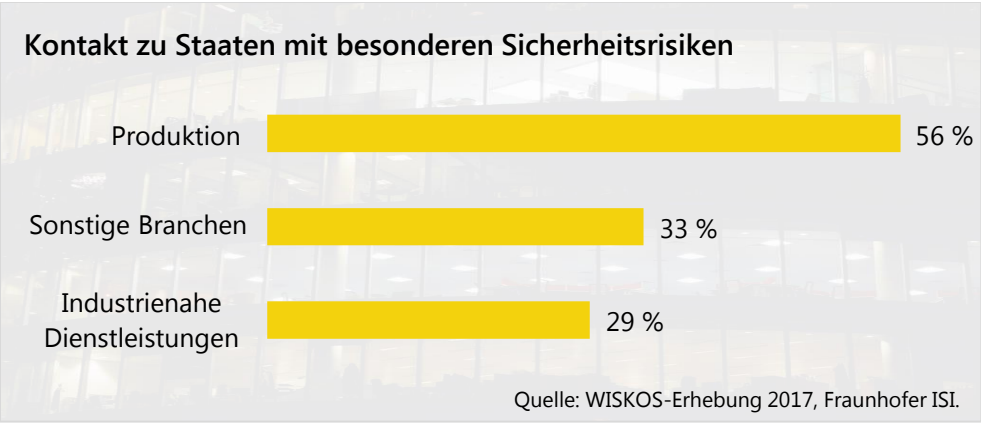


Abbildung 48: Kontakte zu Risikostaaten

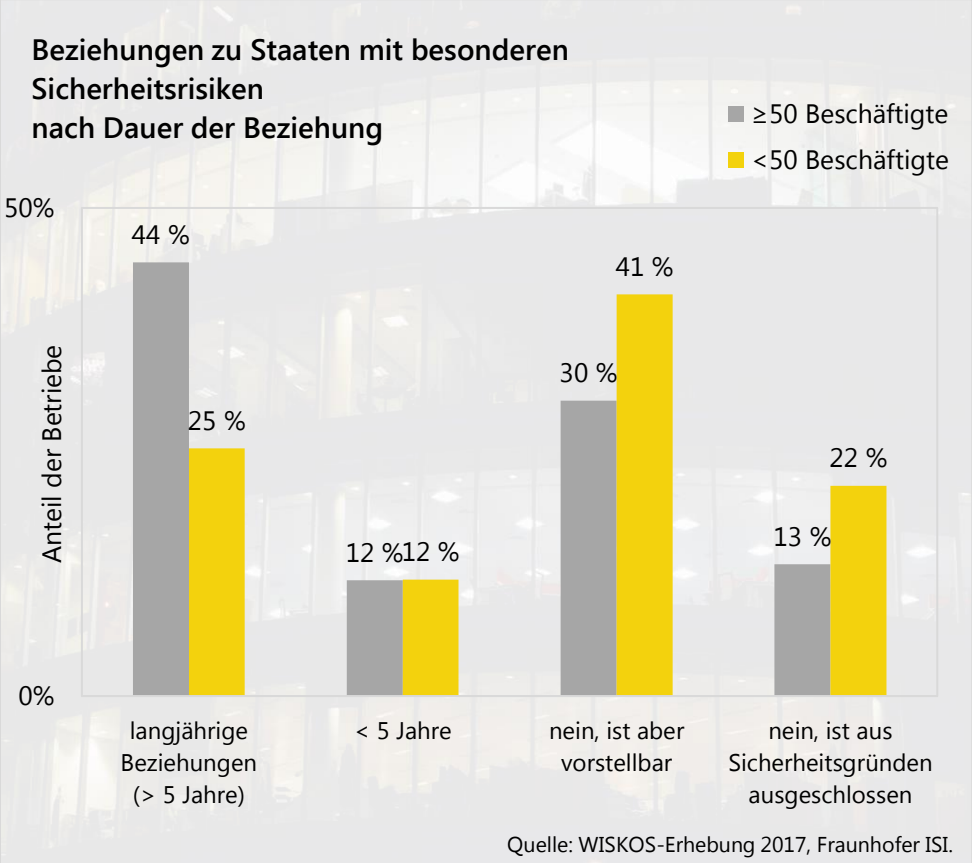


Viele Unternehmen unterhalten geschäftliche Kontakte zu anderen Unternehmen oder Organisationen in Staaten, die besondere Sicherheitsrisiken aufweisen. Dies betrifft vorrangig die produzierenden Unternehmen mit 56 Prozent (s. Abbildung 48). Diese Geschäftskontakte ergeben sich zu großen Teilen direkt aus der Wertschöpfungskette – entweder auf der Seite der Zulieferer oder der Kunden. Daraus resultiert kein direkter Handlungsbedarf, nur müssen diese Rahmenbedingungen in die Entwicklung einer Präventionsstrategie mit einfließen. Hier ist vor allem an Maßnahmen bei Geschäftsreisen und auch bei Geschäftsbesuchen bzw. Werksführungen etc. zu denken.

In Abbildung 49 wird dargestellt, wie sich die Geschäftsbeziehungen und deren strategische Planung nach Unternehmensgrößen darstellen. Die größeren Unternehmen schließen nur selten (13 Prozent) Geschäftsbeziehungen zu Staaten mit besonderen Sicherheitsrisiken pauschal aus, wohingegen hier die Hemmschwelle für kleinere Unternehmen unter 50 Beschäftigten mit 22 Prozent größer ist. Die überwiegende Anzahl an KMU (87 Prozent mit ≥ 50 Beschäftigten und 78 Prozent der kleinen Unternehmen) kann sich derartige Geschäftsbeziehungen mindestens vorstellen bzw. praktiziert sie bereits, wenn auch der Großteil der derzeitigen Geschäftsbeziehungen sich auf die EU-Staaten zu konzentrieren scheint. Unter Berücksichtigung der obigen Ergebnisse (s.o. Kapitel 3.3) ist es daher umso wichtiger, eine Strategie zur Prävention vor Wirtschaftsspionage und Konkurrenzausspähung zu entwickeln und konsequent umzusetzen.

Allerdings kann auch belegt werden, dass Unternehmen, die Geschäftsbeziehungen in Risikostaaten unterhalten, nicht mehr Vorfälle oder Verdachtsfälle als jene ohne diese Geschäftsbeziehungen zu verzeichnen haben (ohne Abbildung). Es liegt die Vermutung auf der Hand, dass Unternehmen, die solche Geschäftsbeziehungen unterhalten, eher sensibilisiert sind und daher verstärkt Maßnahmen zum In

Abbildung 49: Kontakte zu Risikostaaten nach Dauer der Beziehung

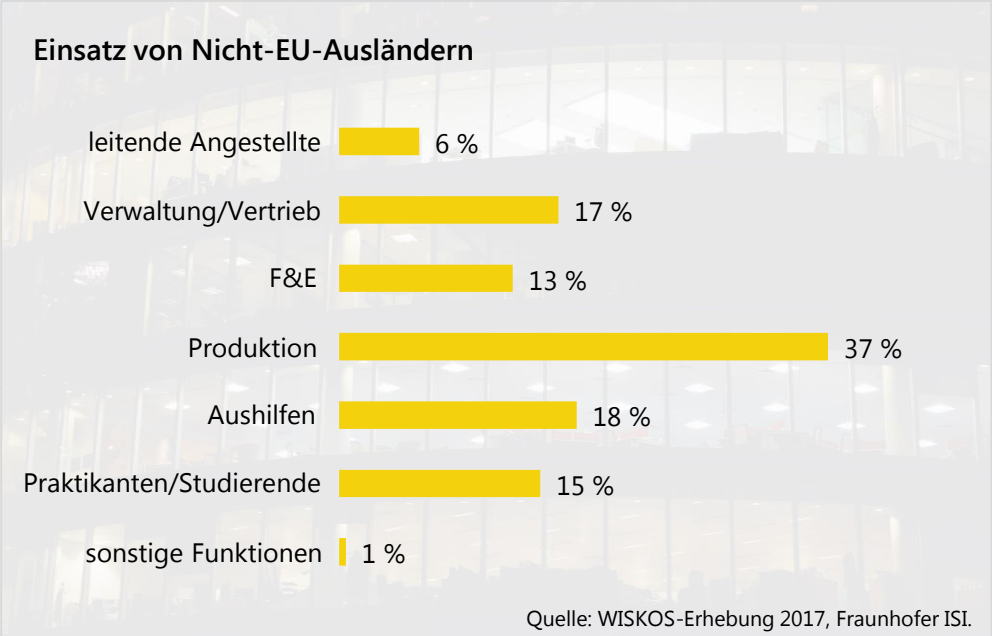


formationsschutz einsetzen. Dies konnte jedoch nicht bestätigt werden. Die Präventionswerte sind bei den Unternehmen mit Geschäftsbeziehungen in Risikostaaten nahezu identisch mit denen ohne Geschäftsbeziehungen in Risikostaaten (ohne Abbildung). Auch in der zusätzlichen Unterscheidung nach Größenklassen der Unternehmen lässt sich kein abweichendes Verhalten in diesem Kontext feststellen (ohne Abbildung). Diese Feststellungen berechtigen allerdings nicht zu der Folgerung, dass Geschäftsbeziehungen in Risikostaaten unbedenklich unter dem Aspekt der Informationssicherheit sind.

Die Beschäftigung von Nicht-EU-Ausländern in den befragten KMU steht in keinem messbaren Zusammenhang mit Vorfällen oder Verdachtsfällen der Wirtschaftsspionage und Konkurrenzausspähung

(ohne Abbildung). Der Einsatz von Nicht-EU-Ausländern erfolgt in verschiedenen Unternehmensbereichen, oftmals getrieben durch Auslandsniederlassungen, Beteiligungsverhältnisse und natürlich durch die Branchenzugehörigkeit und die Tätigkeit im individuellen Fall. Erwartungsgemäß findet sich der größte Anteil im Bereich der Produktion/Fertigung und damit im Schwerpunktbereich der angelernten/ungelernten Kräfte (s. Abbildung 50). Danach – wenn auch mit Abstand – folgen die Aushilfen, ebenfalls oftmals angelernte/ungelernte Kräfte. Im Bereich der Fachkräfte (leitende Angestellte und Forschung und Entwicklung) sind Nicht-EU-Ausländer deutlich weniger vertreten.

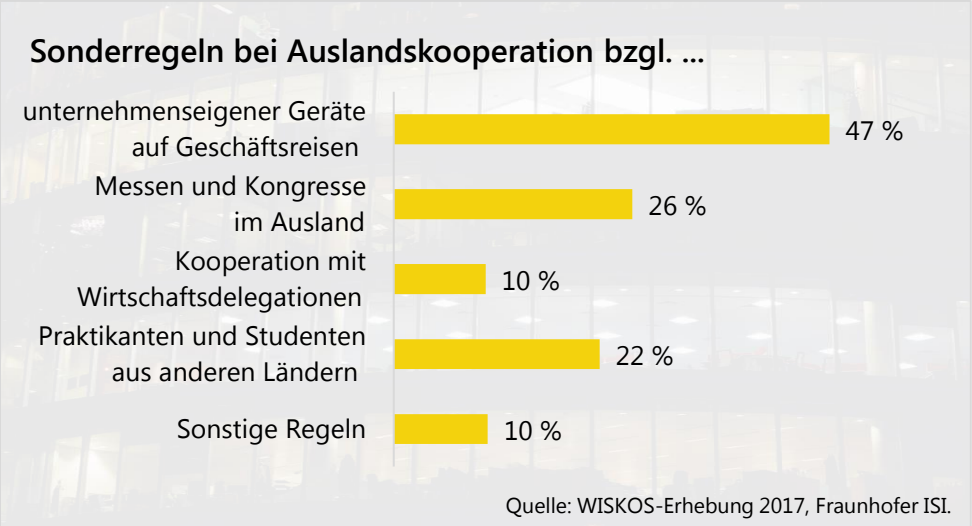
Abbildung 50: Einsatz von Nicht-EU-Ausländern



Besondere Vorsicht ist geboten bei allen Berührungspunkten mit den ehemaligen GUS-Staaten, den USA und asiatischen Ländern, deren Geheimdienste dafür bekannt sind, auf dem Gebiet der Wirtschaftsspionage besonders aktiv zu sein. Insbesondere bei Reisen in die genannten Staaten sollten Unternehmen vorsichtig sein und dafür

eigene Präventionsmaßnahmen entwickeln und umsetzen. Zum Zeitpunkt der Befragung hatte noch nicht einmal jedes zweite KMU Regelungen zur Mitnahme und Nutzung unternehmenseigener Geräte (insbesondere Laptops, Datenträger, Smartphones, Tablets) in die Risikoländer (s. Abbildung 51). Dabei sollte z.B. längst bekannt sein, dass bei der Einreise in die VR China sämtliche Datenträger ausgelesen und kopiert werden. Es empfiehlt sich daher unbedingt, mit "leeren" Geräten einzureisen und ggf. vor Ort über eine verschlüsselte Kommunikationsleitung die benötigten Daten aus der Unternehmenscloud zu laden und vor der Abreise wieder auf demselben Weg zu überspielen.

Abbildung 51: Sonderregeln



Ebenfalls wichtig und wenig beachtet sind organisatorische Regelungen für ausländische Praktikanten und Studenten aus den genannten Ländern im eigenen Betrieb. Gerade Studenten aus dem asiatischen Raum dürfen laut Experten der deutschen Behörden oftmals nur unter "Auflagen" in europäische Länder ausreisen. Diese Auflagen stellen sich z.B. so dar, dass Praktika oder Werkstudententätigkeiten in Industrieunternehmen bestimmter Branchen und/oder Forschungsorganisationen während des Auslandsaufenthaltes absolviert und innerhalb

dieser dann regelmäßig Daten von (Unternehmens-) Servern übermittelt werden müssen. Auch hier lassen sich mit einfach umzusetzenden Regeln Strukturen schaffen, die ungewollten Informationsabfluss verhindern.

Ausblick

4 Ausblick

Die Untersuchungen haben mit aller Deutlichkeit gezeigt, dass der Mittelstand, insbesondere die produzierenden Unternehmen und deren Dienstleister, in Sachen Prävention großen Nachholbedarf hat. Die IT-Sicherheit ist in Zeiten der Digitalisierung zwar in aller Munde, doch ist diese nur ein Baustein im Rahmen eines nötigen Präventionskonzeptes für KMU. Das Thema Prävention von Wirtschaftsspionage und Konkurrenzausspähung muss zur Chefsache werden und auch von der Unternehmensspitze aus nachdrücklich und wiederholend kommuniziert werden. Hierzu bieten sich Versammlungen, Infowände und das Intranet an. Neben technischen Sicherheitsmaßnahmen müssen aufeinander abgestimmte organisatorische und personelle Vorkehrungen getroffen werden.

Entscheidend ist es, weder den Wert der eigenen Informationen für Wettbewerber und Geheimdienste anderer Länder, noch den möglicherweise entstehenden Schaden zu unterschätzen. Die Untersuchungen haben gezeigt, dass KMU nicht weniger gefährdet sind als andere Unternehmen und auch ähnlich oft angegriffen werden. Kein KMU kann sich daher in Sicherheit wiegen, dass es zu klein oder zu uninteressant für Angreifer sei. Selbst die industrienahen Dienstleister, die nach eigenen Angaben viele Informationen überhaupt nicht strukturiert abgelegt haben, sondern in den Köpfen der Mitarbeiter vorhalten, wissen um die Nutzung illegal erworbener Informationen durch Wettbewerber und sind dementsprechend angehalten, sich zu schützen.

Beim Thema Informationssicherheit und Informationsschutz müssen die Beschäftigten mit einbezogen und sensibilisiert werden. Somit sollten im Rahmen des Präventionskonzepts auch Mitarbeiterschulungen zum Thema Sicherheitsverhalten und zu Verdachtsindikatoren vorgesehen werden. Diese und andere Arten von Awareness-Maßnahmen kommen derzeit noch viel zu kurz und müssen unbedingt mehr

Beachtung finden. Ein gesteigertes Bewusstsein für Sicherheitsaspekte und der bewusste Einsatz von Präventionsmaßnahmen bzw. Monitoring-Werkzeugen können den Schutz eines Unternehmens verbessern.

Staatliche Behörden können nur dann wirkungsvoll arbeiten, wenn sie auch Kenntnis von möglichen Vorfällen und Verdachtsfällen erhalten. Die Vertrauensbasis zwischen den Behörden und den KMU ist jedoch nicht ausreichend entwickelt. Hier sind beide Seiten zur Mitwirkung aufgerufen: Die Unternehmen tragen mit der Meldung von Vorfällen zur Verbreiterung der Informationsbasis und damit letztlich zur Entwicklung von übergreifenden Konzepten zu Prävention und Strafverfolgung bei; die Behörden können Vorfälle und Angriffswellen im Kontext einschätzen und die Unternehmen bei der Aufklärung und auch bei Sicherheitsmaßnahmen unterstützen. Mittel- bis langfristig werden so beide Seiten profitieren.

5 Abbildungsverzeichnis

Autorinnen

Esther Bollhöfer

Dr. Esther Bollhöfer ist seit 10 Jahren wissenschaftliche Projektleiterin am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. Ihre Arbeitsschwerpunkte sind die Gestaltung und Bewertung von industriellen Geschäftsmodellen und Kooperationen zur Erschließung und Ausweitung neuer Geschäftsfelder, Industrie 4.0 sowie alle Forschungsfragen rund um den Schutz von Informationen und Know-how in der Industrie - aus organisatorischer wie aus rechtlicher Perspektive.

Angela Jäger

Angela Jäger ist als wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für System- und Innovationsforschung ISI tätig. Nach dem Studium der Sozialwissenschaften an der Universität Mannheim arbeitete sie am Mannheimer Zentrum für Europäische Sozialforschung (MZES) zur Analyse sozialer Netzwerke. 2006 wechselte sie als Expertin für empirische Methoden der Sozial- und Wirtschaftsforschung ans Fraunhofer ISI. Ihre Arbeitsschwerpunkte liegen im Bereich Forschungsdesign, betriebliche Befragungen und quantitative Analysen. Sie koordiniert den *European Manufacturing Survey* (EMS).

Das Projekt WISKOS: Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa

Modul 1: Länder-Screening

> **Länderberichte** aus allen 28 Mitgliedsstaaten der Europäischen Union und der Schweiz zu den rechtlichen Regelungen, dem verfahrensrechtlichen Rahmen und statistischen Basisdaten

Modul 2: Mehrebenen-Evaluation

> **Literatur- und Dokumentenanalyse**

> **Strafaktenanalyse** (n=713 Strafakten zur Konkurrenzausspähung aus Deutschland)

> **Exemplarische Fallstudien** (n=50 Fallstudien aus Bulgarien, Dänemark, Österreich, der Schweiz und dem Vereinigten Königreich)

> **Experteninterviews** (n=62 mit Vertretern von Behörden, KMU, Kammern, Verbänden, Wissenschaftsorganisationen in Deutschland sowie Bulgarien, Dänemark, Österreich, der Schweiz und dem Vereinigten Königreich)

Modul 3: Dunkelfeldbefragung

> **Erhebung** *Modernisierung der Produktion* 2015 (n= 1.282 Betriebe)

> **Erhebung** bei produzierenden Betrieben und industrienahen Dienstleistern bis zu 250 Mitarbeitern 2017 (n=583)

Projektpartner

> Max-Planck-Institut für ausländisches und internationales Strafrecht
> Fraunhofer-Institut für System- und Innovationsforschung

Assoziierte Partner

> Bundeskriminalamt
> Landeskriminalamt Baden-Württemberg
> Sächsische Hochschule der Polizei

WISKOS

Publikationen mit Ergebnissen aus dem Projekt WISKOS

Wissenschaftliche Publikationen

> *Carl, S. & Kilchling, M.* (Hrsg.): Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin 2018.
> *Wallwaey, E., Bollhöfer, E. & Knickmeier, S.* (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin 2018.
> *Bollhöfer, E. & Jäger, A.*: Wirtschaftsspionage und Konkurrenzausspähung: Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Freiburg i.Br. 2018.

Praxisorientierte Informationsmaterialien

Für KMU

> **Faltblatt** „Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how!"
> **Bildergalerie** „Wirtschaftsspionage und Konkurrenzausspähung" Warnhinweise zur Verwendung als Startbildschirm, Sperrbildschirm oder Pop-up-Fenster
> **Broschüre** „Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how!"

Für Wissenschaftsorganisationen

> **Faltblatt** „Wissenschaftsspionage: Schützen Sie Ihre Forschungsdaten!"
> **Bildergalerie** „Wissenschaftsspionage" Warnhinweise zur Verwendung als Startbildschirm, Sperrbildschirm oder Pop-up-Fenster
> **Handlungsleitfaden** „Risiken für den deutschen Forschungsstandort"

Für Polizeibehörden

> **Faltblatt** „Wirtschaftsspionage und Konkurrenzausspähung: Was ist zu tun, wenn sich ein Unternehmen an Sie wendet?"
> **Broschüre** „Wirtschaftsspionage und Konkurrenzausspähung: Strategische Aspekte für die polizeiliche Arbeit"
> **Poster** „Wirtschaftsspionage und Konkurrenzausspähung: Was ist zu tun, wenn sich ein Unternehmen an Sie wendet?"

Die Informationsmaterialien für KMU und Wissenschaftsorganisationen und weitere Informationen zu dem Forschungsprojekt WISKOS finden Sie kostenlos zum Download unter:

http://wiskos.de

WISKOS

Die vorliegende Studie ist ein Ausschnitt aus dem wissenschaftlichen Projekt "Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa – WISKOS", das von 2015 bis 2018 gemeinsam vom Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg i.Br., und dem Fraunhofer Institut für System- und Innovationsforschung ISI, Karlsruhe, durchgeführt wurde. Sie präsentiert die Ergebnisse aus zwei quantitativen Unternehmensbefragungen im Verarbeitenden Gewerbe sowie bei produzierenden kleinen und mittelständischen Unternehmen und industrienahen Dienstleistern in Deutschland. Die umfangreichen Ergebnisse liefern ein Bild über den aktuellen Status Quo bei kleinen und mittelständischen Unternehmen zur Bedrohungslage im Hinblick auf illegalen Knowhow-Abzug, ihre Wahrnehmung und Interessenlage sowie einen Einblick in die praktizierten Abwehrmaßnahmen.

Die Ergebnisse bieten nicht nur Handlungsansätze für Unternehmen zur Optimierung ihrer Schutzstrategien. Sie ermöglichen es auch den zuständigen staatlichen Behörden, die Bedarfe der Unternehmen besser kennenzulernen und darauf Kooperationen aufzubauen, um dem staatlichen Auftrag der Gefahrenprävention besser nachkommen zu können.

ISBN 978-3-86113-270-7

WISKOS