Bundeskriminalamt

Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes

Ergebnisbericht einer Sekundäranalyse

Kurzversion

Karsten Kasper

unter Mitarbeit von Valentina Thürnau

Stand: August 2014

Das Kriminalistische Institut des Bundeskriminalamts ist zertifiziert nach DIN EN ISO 9001 (TÜV Nord CERT, Zertifikat-Registrier-Nr. 44 100 081125)

Inhaltsverzeichnis

1. Einleitung

Die vorliegende Zusammenfassung stellt die Ergebnisse einer **Sekundäranalyse** zum Thema Wirtschaftsspionage und Konkurrenzausspähung dar. Sie wurde geleitet von der **zentralen Frage**, wie sich die Phänomene Wirtschaftsspionage und Konkurrenzausspähung aus Sicht deutscher Unternehmen aktuell darstellen. Im Fokus der Analyse standen aktuelle Beiträge aus der Fachliteratur sowie **empirische Studien**, in deren Rahmen Unternehmensbefragungen durchgeführt wurden. Anlass zu dieser Untersuchung boten einerseits die intensive und zum Teil überspitzte mediale Berichterstattung und andererseits, ein Kenntnisstand der Sicherheitsbehörden, der den Veröffentlichungen, die von einem dramatischen Anstieg der beiden Phänomene ausgehen, nicht entspricht, was vor allem auf die geringe Bereitschaft der Unternehmen zurückzuführen ist, Sachverhalte mit Verdacht auf Wirtschaftsspionage oder Konkurrenzausspähung zu melden. Auch umfangreiche Abfragen im Auftrag des Bundesministeriums des Inneren bei deutschen und ausländischen Behörden und Dienststellen im Hinblick auf eine Verbesserung des Kenntnisstandes haben nicht die erwünschten Ergebnisse erbracht. Auf der Grundlage der Hellfelderfassung sowie der medialen Berichterstattung können jedoch keine zuverlässigen **Erkenntnisse zu der Phänomenentwicklung** gewonnen und polizeiliche Maßnahmen begründet werden, weswegen die Ergebnisse von empirischen Studien, in deren Rahmen sich Unternehmen anonym zu dem Thema äußern konnten, besonders relevant erscheinen.

2. Begrifflichkeiten

Das Bundesamt für Verfassungsschutz definiert **Wirtschaftsspionage** als „…die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben“ (BfV 2008: 9).[1] Wirtschaftsspionage muss von der **Konkurrenzausspähung** (manchmal auch als Industrie-, Betriebs- oder Konkurrenzspionage bezeichnet) abgegrenzt werden, bei der Unternehmen durch andere Unternehmen, Einzelpersonen oder organisierte Gruppen ausgeforscht werden. Die Ergebnisse der Studien zeigen, dass die strafrechtlich relevante Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung für viele Unternehmen weniger bedeutsam ist und eher eine akademische als eine praktische Bedeutung hat.

[1] Auf Quellenangaben wurde in der Kurzversion weitestgehend verzichtet, diese sind im Ergebnisbericht dokumentiert.

3. Methodisches Vorgehen

Mit Hilfe einer schlagwortgestützten Recherche konnten ca. 440 auswertungsrelevante Quellen ab dem Erscheinungsjahr 1999 identifiziert werden. Aus diesen wurden für die weitere Auswertung Quellen ab 2007 mit unmittelbarem Themenbezug und wissenschaftlichem Charakter ausgewählt. Mit Hilfe dieser Kriterien konnte die Zahl der **auswertungsrelevanten Quellen** auf 148 reduziert werden. Da sich die betrachteten Befragungen in Vorgehen und methodischer Qualität sowie bei den thematischen Schwerpunkten zum Teil stark unterscheiden, sollten die folgenden Erkenntnisse eher als Tendenzen verstanden werden, ebenso wie die quantitativen Ergebnisse nicht als feste statistische Größen interpretiert werden sollten. Ferner sollte auch bedacht werden, dass private Unternehmen oder Netzwerke (wie Unternehmensberatungen oder Hersteller von Computersicherheitssoftwares) mit ihren Befragungen spezifische Eigeninteressen verfolgen können und dementsprechend möglicherweise andere Schwerpunkte setzen und Empfehlungen aussprechen als öffentliche Einrichtungen.

4. Zusammenfassung der zentralen Ergebnisse

4.1. Bedrohungswahrnehmung deutscher Unternehmen

Die **Sensibilität** der deutschen Unternehmen für die Gefahren von Ausforschung **ist hoch**. So schätzten zwischen 2010 und 2013 im Durchschnitt ca. **60 Prozent** der Befragten die **Bedrohung durch Ausforschung** für ihr eigenes Unternehmen als bedeutsam ein. In mehreren Studien wurde zudem festgestellt, dass der Anteil der Befragten, die Ausforschungsangriffe als eine große Bedrohung für das eigene Unternehmen wahrnehmen, über die letzten Jahre **zunahm**. Im Vergleich zu Unternehmen aus anderen europäischen Ländern gaben deutsche Firmen am häufigsten an (19,5 Prozent der Unternehmen), dass Ausforschung ein *wichtiges* Mittel ist, um in der jeweiligen Branche Informationen über Konkurrenten zu erhalten. Demgegenüber stimmten im Durchschnitt aller befragten europäischen Unternehmen nur 8,9 Prozent dieser Aussage zu. Diese Zahlen zeigen, dass das Problembewusstsein deutscher Unternehmen **im europäischen Vergleich** überdurchschnittlich hoch ist, was die Vermutung zulässt, dass sie auch überdurchschnittlich oft von Ausforschung betroffen sein könnten. Zudem nahmen im Durchschnitt der Studien ca. **60 Prozent** der Unternehmen an, dass auch das **zukünftige Risiko**, ausgeforscht zu werden, ansteigen wird. In mehreren Befragungen konnte eine **Diskrepanz** zwischen der individuellen und der gesamtwirtschaftlichen Bedro-

hungswahrnehmung festgestellt werden: So waren viele Unternehmen der Ansicht, dass ihr individuelles Risiko geringer sei als das der Gesamtwirtschaft. Sie nahmen also durchaus ein allgemeines Risiko wahr, wähnten sich selbst jedoch in Sicherheit. Ein möglicher Interpretationsansatz für diese Diskrepanz ist, dass sich viele Unternehmen nicht als Angriffsziel sehen.

4.2. Betroffenheit deutscher Unternehmen

In den Studien konnten zum Teil sehr **unterschiedlich hohe Betroffenheitswerte** festgestellt werden: so lag der Anteil der Unternehmen, die in mindestens einem Fall eine Ausforschung feststellen konnten, zwischen **7 und 85 Prozent**. Diese breite Streuung kann u. a. auf Unterschiede in den Forschungsdesigns der verschiedenen Befragungen zurückgeführt werden. Da die Werte in dieser Form für eine Interpretation zu ungenau sind, müssen die verschiedenen Angriffe auf die Unternehmen **differenzierter betrachtet** werden. Hierfür wurden die Vorfälle unter drei Oberbegriffen zusammengefasst, die sich an dem Wortlauf der Befragungen orientieren: a) **Verrat von Geschäfts- und Betriebsgeheimnissen**, b) **Datendiebstahl**, c) **Wirtschaftsspionage/Konkurrenzausspähung**[2]. Zu jedem Oberbegriff wurden Mittel- und Zentralwert gebildet (vgl. Tabellen 1a-c), Berechnungen, die in diesem Zusammenhang durchaus als problematisch angesehen werden können, da sich die verschiedenen Werte u. a. auf teilweise unterschiedliche Zeiträume und Methoden der Ausforschung beziehen. Die Mittel- und Zentralwerte können deshalb nicht als statistisch belastbare Zahlen verstanden werden und sollen lediglich ein besseres Verständnis und einen leichteren Überblick ermöglichen. Beispielhaft werden im Folgenden ausgewählte Ergebnisse dargestellt:

Im Durchschnitt der aktuellsten Studien verzeichnete zwischen 2010 und 2013 ca. **jedes vierte Unternehmen** mindestens einen Fall von Verrat von Geschäfts- und Betriebsgeheimnissen, ebenfalls ca. **jedes vierte Unternehmen** mindestens einen Fall von Datendiebstahl und ca. **jedes sechste Unternehmen** mindestens einen Fall von Wirtschaftsspionage/Konkurrenzausspähung.

[2] In diesem Fall wird ausdrücklich nach der Betroffenheit von Wirtschaftsspionage und/oder Konkurrenzausspähung gefragt.

Tabelle 1a: Betroffenheit von Verrat von Geschäfts- und Betriebsgeheimnissen

Konkret genannter Vorfall	Anteil der Unternehmen	Zeitraum	Quelle
Verrat von Geschäfts- und Betriebsgeheimnissen	16 %	in verg. 2 Jahren	KPMG 2013a: 15
Verrat von Geschäfts- und Betriebsgeheimnissen	21 %	in verg. 2 Jahren	KPMG 2013b: 33
Verrat von Geschäfts- und Betriebsgeheimnissen	48 %	in verg. 4 Jahren	Sicherheitsforum 2010: 47
Arithmetisches Mittel	**28,3 %**		
Median	**21 %**		

Quelle: Eigene Darstellung

Tabelle 1b: Betroffenheit von Datendiebstahl

Konkret genannter Vorfall	Anteil der Unternehmen	Zeitraum	Quelle
Datendiebstahl	8 %	k. A.	BMWi 2012: 55
Datendiebstahl	15,8 %	im letzten Jahr	IHK Nord 2013: 9
Entwendung von Geschäftsgeheimnissen	17,1 %	in verg. 10 Jahren	Europäische Kommissi-on 2013b: 19
Diebstahl vertraulicher Daten	20 %	in verg. 2 Jahren	PwC 2013: 18
Ausspähen, Abfangen von Daten	27 %	in verg. 2 Jahren	KPMG 2013a: 15
Datendiebstahl/ Datenmissbrauch	31 %	in verg. 2 Jahren	KPMG 2013b: 33
Vertraulichkeitsbruch/ Datendiebstahl	53 %	in verg. 2 Jahren	kes 2012/4: 10
Ausspähung und Abhörangriffe	73 %	in verg. 2 Jahren	WIK 2013/2: 12
Arithmetisches Mittel	**30,61 %**		
Median	**23,5 %**		

Quelle: Eigene Darstellung

Tabelle 1c: Betroffenheit von Wirtschaftsspionage/Konkurrenzausspähung allgemein

Konkret genannter Vorfall	Anteil der Unternehmen	Zeitraum	Quelle
WS/KA allgemein	1 %	k. A.	BMWi 2012: 55
WS/KA allgemein	7 %	in verg. 3 Jahren	Ernst & Young 2013: 18
WS/KA allgemein	12 %	in verg. 2 Jahren	PwC 2013: 17 f.
WS/KA allgemein	54,6 %	in verg. 3 Jahren	Corporate Trust 2012: 13
Arithmetisches Mittel	**18,65 %**		
Median	**9,5 %**		

Quelle: Eigene Darstellung

In sieben Befragungen gaben **größere Unternehmen** deutlich häufiger als kleine Unternehmen an, dass sie Opfer von Ausforschung wurden. Das sollte jedoch nicht zu der Annahme führen, dass die Wahrscheinlichkeit der Ausforschung mit der Größe eines Unternehmens zunimmt. Vielmehr gibt es weitere Aspekte, die die **Wahrscheinlichkeit** von Wirtschaftsspionage und/oder Konkurrenzausspähung erhöhen können, wie z. B. die Investitionen eines Unternehmens in die **Forschung und Entwicklung** oder seine Bemühungen bzgl. der Sensibilisierung der **Beschäftigten**. So konnte in mehreren Studien gezeigt werden, dass forschungsintensive Unternehmen deutlich häufiger Opfer von Ausforschung wurden als Unternehmen, die wenig oder keine Forschung und Entwicklung betrieben. Einen zusätzlichen Einfluss auf die Betroffenheit kann auch die **Branchenzugehörigkeit** eines Unternehmens haben. In mehreren Studien waren überdurchschnittlich häufig Unternehmen aus der Automobil-, der Luftfahrt-, der Maschinenbau- und der Pharma-/Chemiebranche betroffen.

Im Gegensatz zur von den Unternehmen wahrgenommenen Bedrohung, die während der letzten Jahre zugenommen hat, **sank die Anzahl der tatsächlich festgestellten Angriffe zu Ausforschungszwecken** im Laufe der letzten Jahre. In den aktuellsten Studien gaben tendenziell weniger Unternehmen an, ausgeforscht geworden zu sein, als noch in den direkten Vorgängerstudien (vgl. Tabelle 2). Diese Abnahme hängt nicht unbedingt mit einem Rückgang der tatsächlichen Ausforschungsaktivitäten zusammen, sondern sie könnte auch darauf zurückzuführen sein, dass Angreifer immer professioneller werden und Vorfälle somit unbemerkt bleiben. Aber auch die im Rahmen dieser Arbeit festgestellte Zunahme der Bedrohungswahrnehmung und die damit einhergehende **erhöhte Sensibilisierung** der Unternehmen für Ausforschung, können zu einer Abnahme der Betroffenheit führen. Es kann davon ausgegangen werden, dass Unternehmen, die für eine bestimmte Bedrohung sensibilisiert sind, tendenziell eher konkrete Abwehrmaßnahmen treffen werden, als solche Unternehmen, die diese Bedrohung weder wahrnehmen noch bewerten.

Tabelle 2: Längsschnittvergleich der Betroffenheit

Studien	Konkret genannter Vorfall	Jahr (Zeitraum)	Anteil Unternehmen	Veränderung
Corporate Trust 2007 und 2012	WS/KA	2007 (k. A.) 2012 (3 Jahre)	54 % 54,6 %	↑
kes 2010 und 2012	Vertraulichkeitsbruch/ Datendiebstahl	2010 (2 J.) 2012 (2 J.)	84 % 85 %	↑
PwC 2011 und 2013	Diebstahl vertraulicher Daten	2011 (2 J.) 2013 (2 J.)	35 % 20 %	↓
	WS/KA	2011 (2 J.) 2013 (2 J.)	18 % 12 %	↓
KPMG 2010b und 2013b	Datendiebstahl/ Datenmissbrauch	2010 (3 J.) 2013 (2 J.)	53 % 31 %	↓
	Verrat von Geschäfts- und Betriebsgeheimnissen	2010 (3 J.) 2013 (2 J.)	24 % 21 %	↓
KPMG 2010a und 2013a	Datendiebstahl	2010 (3 J.) 2013 (3 J.)	61 % 24 %	↓
	Verrat von Geschäfts- und Betriebsgeheimnissen	2010 (3 J.) 2013 (3 J.)	51 % 16 %	↓
	Ausspähen, Abfangen von Daten	2010 (3 J.) 2013 (3 J.)	44 % 27 %	↓
Ernst & Young 2011 und 2013	WS/KA	2011 (3 J.) 2013 (2 J.)	10 % 7 %	↓
WIK 2011 und 2013	Ausspähen	2011 (2 J.) 2013 (2 J.)	51,2 % 51 %	=
	Abhören	2011 (2 J.) 2013 (2 J.)	10 % 22 %	↑

Quelle: Eigene Darstellung

Auch die Herausgeber der Studien sind sich darin einig, dass aufgrund dieses Rückgangs festgestellter Angriffe zu Ausforschungszwecken **keine Entwarnung** gegeben werden kann, da die Unternehmen selbst angeben, dass ca. **ein Drittel** der Ausforschungsangriffe nur **per Zufall** entdeckt wurde. Ein Rückgang der festgestellten Vorfälle bedeutet somit nicht, dass auch tatsächlich weniger Angriffe erfolgten.

Viele Vorfälle werden von den Unternehmen **überhaupt nicht** oder erst sehr spät **bemerkt**. Die wichtigsten **Verdachtsmomente**, die auf einen bereits eingetretenen Ausforschungsvorfall hindeuteten, waren das Auftauchen von Teilinformationen bei Mitbewerbern, der nicht erklärbare Verlust von Aufträgen sowie das Erscheinen von ähnlichen Konkurrenzprodukten. Häufig entdeckten Unternehmen den Verlust von sensiblem Know-how erst aufgrund von **Hinweisen** von internen oder externen Tippgebern. Nur **selten** wurden die Unternehmen von den **Sicherheitsbehörden** aufmerksam gemacht. Auch **unternehmensinterne Kontrollen** deckten nur einen kleinen Teil der Angriffe auf.

4.3. Schäden

Die Ausforschung deutscher Unternehmen schadet nicht nur dem jeweils betroffenen Unternehmen, sondern sie kann sich auch negativ auf die deutsche Gesamtwirtschaft auswirken. So sind laut dem Bayrischen Landesamt für Verfassungsschutz in Deutschland jährlich über **50.000 Arbeitsplätze** mittelbar durch Ausforschung gefährdet.

Die möglichen negativen Auswirkungen eines Angriffs zu Ausforschungszwecken auf ein Unternehmen können vielfältig sein. Ein betroffenes Unternehmen kann **direkte finanzielle Schäden** und/oder **indirekte immaterielle Schäden** verzeichnen. Die Mehrheit der Unternehmen, die Opfer von Ausforschung wurden, verzeichneten **häufiger immaterielle Schäden** als direkte Umsatzeinbußen. Immaterielle Schäden, wie z. B. Imageschäden bei Kunden und Geschäftspartnern, negative Medienberichterstattung oder sinkende Attraktivität als Arbeitgeber sollten von den Unternehmen nicht unterschätzt werden, da sie zum Teil schwerwiegendere Konsequenzen haben als die direkten finanziellen Schäden. Welche Schäden einem Unternehmen entstehen, kann auch von der **Unternehmensbranche** abhängen.

Auch wenn die **wirtschaftlichen Auswirkungen** von Wirtschaftsspionage und/oder Konkurrenzausspähung auf die deutsche Wirtschaft nur **schwer bestimmt** werden können, werden sie in der Öffentlichkeit (von politischen und wirtschaftlichen Entscheidungsträgern, der Presse etc.) mehrheitlich als **sehr bedeutsam *eingeschätzt***. In der Presse finden sich regelmäßig Schadensschätzungen zwischen **20 bis 100 Milliarden Euro**. Auch viele Unternehmen gingen davon aus, dass sich der jährliche finanzielle Schaden für die deutsche Wirtschaft auf mehr als 10 Milliarden Euro beläuft. Meistens wird jedoch nicht näher erläutert, wie diese Schätzungen zustande gekommen und welche Elemente in die Berechnung eingeflossen sind.

Auch wenn auch die von den Unternehmen gemachten **Angaben zu den Schadenshöhen** häufig nur auf groben Schätzungen beruhen, da es ihnen selbst oft schwer fällt den Schaden eines Ausforschungsangriffs genau zu quantifizieren, sind sie dennoch **aussagekräftiger** als reine Spekulationen und sie bieten bei **methodisch sauberem Vorgehen** eine gute Möglichkeit, um eine Berechnungsgrundlage für die Gesamtwirtschaft zu schaffen. Hochrechnungen auf die Gesamtwirtschaft auf der Grundlage dieser Schadensangaben ergaben **deutlich niedrigere Schadenshöhen**, die zwischen jährlich **2,8 und deutlich unter 20 Milliarden Euro liegen**. So errechnet das Sicherheitsforum Baden-Württemberg einen jährlichen

Schaden für die deutsche Wirtschaft durch Know-how- und Informationsverluste in Höhe von ca. 7 – 8 Milliarden Euro. Diese **Hochrechnungen stehen in keinem Verhältnis zu den weit höheren Schätzungen**, die in den Presseartikeln genannt werden.

4.4. Täter

Bei Wirtschaftsspionage und/oder Konkurrenzausspähung ist es oft **schwer**, den oder die Täter sofort und eindeutig zu bestimmen. Das gestaltet sich noch schwieriger, wenn die Täter über **Informations- und Kommunikationstechnologien** angreifen. Experten schätzen, dass die Mehrheit der Ausforschungsangriffe auf deutsche Unternehmen von Wettbewerbern, Kunden und Lieferanten ausgehen und dass nur ein kleiner Teil durch ausländische Nachrichtendienste initiiert wird. Diese Einschätzung kann sich aber im Zuge der NSA Überwachungs- und Spionageaffäre und den Enthüllungen durch Edward Snowden ändern.

In den meisten Befragungen wurden am häufigsten **aktuelle bzw. ehemalige Mitarbeiter** als Täter identifiziert. Diese arbeiteten absichtlich mit externen Tätern zusammen oder sie wurden, z. B. über **Social Engineering**[3]**,** unbeabsichtigt zu Mittätern. Weitere Möglichkeiten, wie Mitarbeiter unbeabsichtigt zu Tätern werden können, sind der Verlust von mobilen elektronischen Endgeräten oder die leichtfertige Weitergabe von internen Informationen auf Reisen oder in sozialen Netzwerken.

In mehreren Studien konnten die befragten Unternehmen nationale und ausländische **Wettbewerber** als **zweithäufigste Tätergruppe** feststellen. Weitere häufig genannte Tätergruppen waren **Kunden, Lieferanten und Kooperationspartner** und somit Personen, die den Unternehmen **persönlich bekannt** waren. **Ausländische Nachrichtendienste** konnten nur von einem kleinen Teil der Unternehmen als Angreifer identifiziert werden. Das bedeutet jedoch nicht, dass sie nicht auch versuchen würden, an Know-how aus deutschen Firmen zu gelangen. Vielmehr ist davon auszugehen, dass sie aufgrund einer besseren finanziellen und materiellen Ausstattung **professioneller vorgehen** können und deswegen seltener als Täter erkannt werden. Zudem muss bedacht werden, dass Tätern nicht immer eine Verbindung zu einem ausländischen Nachrichtendienst nachgewiesen werden kann.

Die Ergebnisse in Bezug auf die **Herkunft** der Täter waren **wenig eindeutig**. Zwar vermutete in vielen Befragungen die Mehrheit der betroffenen Unternehmen, dass Angriffe vor allem von Tätern aus China, anderen asiatischen Ländern, den USA und Russland durch-

[3] Beeinflussung durch soziale Manipulation.

geführt wurden, in zwei Studien gab jedoch jeweils die Mehrheit der Unternehmen an, dass die Täter aus Deutschland stammten und nur jeweils eine Minderheit der Befragten stellte Täter aus China und dem restlichen Asien fest. Das zeigt, dass die Gefahr, die von **deutschen Wettbewerbern** ausgeht, nicht unterschätzt werden sollte. Zudem sollte nicht außer Acht gelassen werden, dass von der (deutschen) Nationalität der Tatausführenden nicht unbedingt auf die Nationalität der Auftraggebenden geschlossen werden kann.

Zu den **Gründen**, die die Weitergabe von unternehmensinternem Know-how begünstigten, zählten u. a. finanzielle und materielle Anreize, unzureichende unternehmensinterne Kontrollen, berufliche Enttäuschung, Erpressung oder Bestechung. Sind alle drei Voraussetzungen des **Betrug-Dreiecks** erfüllt (Motivation, Rechtfertigung und Gelegenheit), ist die Wahrscheinlichkeit hoch, dass ein Beschäftigter seinem Unternehmen, z. B. durch das Weiterleiten von unternehmensinternen Daten an Dritte, Schaden zufügt.

4.5. Sicherheitsvorkehrungen der Unternehmen

Aus der Fachliteratur und der Selbsteinschätzung der Unternehmen ging hervor, dass bei vielen deutschen Unternehmen die **Schutzvorkehrungen** gegen Ausforschung **verbesserungsbedürftig** waren. Ein effektiver Schutz vor Ausforschung erschien vielen Unternehmen wie der sprichwörtliche „Kampf gegen Windmühlenflügel“, denn häufig waren eigene Beschäftigte am Know-how-Verlust beteiligt und neue technische Entwicklungen erschwerten ein Erkennen der Angriffe zudem noch. Zwar ist maximale Sicherheit nicht praktikabel, das sollte aber nicht als Grund gesehen werden, überhaupt keine Sicherheitsvorkehrungen zu treffen, da sonst die **Existenz** eines Unternehmens **gefährdet** ist. Nach dem *Verizon Data Breach Investigations Report 2011* wären beispielsweise **96 Prozent der „data breaches“** (Datenkompromittierungen z. B. durch Cyber-Ausforschung, Hacking oder Malware) mit Hilfe einfacher Sicherheitsvorkehrungen **vermeidbar** gewesen.

Um sich effektiv vor Angriffen zu Ausforschungszwecken zu schützen, sollten Unternehmen einen **ganzheitlichen Ansatz** zum Schutz vor Ausforschung verfolgen, der zugleich Schutzvorkehrungen in den Bereichen Prozesse, Personal und Technik vorsieht. Denn obwohl Ausforschungsangriffe vermehrt über das **Internet** durchgeführt werden, reicht es nicht aus, wenn in einem Unternehmen lediglich die IT-Abteilung für die Abwehr von Ausforschung verantwortlich ist.

Bezüglich der von den Unternehmen getroffenen **strukturellen und organisatorischen Schutzvorkehrungen** kommen die Autoren der Studien zu folgenden Ergebnissen: Häufig verfügte weniger als ein Drittel der Unternehmen über ein schriftlich fixiertes Informationsschutzkonzept, in dem die Verantwortlichkeiten und Aufgaben im Bereich der Abwehr von Ausforschung sowie Handlungsempfehlungen im Falle eines Ausforschungsvorfalls aufgeführt werden. Ferner hatte rund die Hälfte der Unternehmen noch keine Schutzbedarfsanalyse durchgeführt, mit deren Hilfe die „Kronjuwelen" (wettbewerbsentscheidende Daten) eines Unternehmens bestimmt werden können. Immerhin verfügten zwischen 30 und 80 Prozent der Unternehmen über schriftlich verfasste Vorgaben, die den richtigen Umgang mit schützenswerten Informationen regeln.

Viele Unternehmen haben auch bzgl. der **personellen Maßnahmen** deutlichen Nachholbedarf. Zwar integrierten zwischen 80 und 90 Prozent der Unternehmen Geheimhaltungsverpflichtungen in die Arbeitsverträge, jedoch wurden Integritätstests für neue Beschäftigte nur von 6 bis 20 Prozent der Unternehmen durchgeführt. Um zu verhindern, dass Beschäftigte unbewusst und bewusst Ausforschungsangriffe unterstützen, ist es wichtig, dass sie einerseits für die Gefahren von Wirtschaftsspionage und Konkurrenzausspähung sensibilisiert werden und dass andererseits ihre Identifikation mit dem Unternehmen gestärkt wird. Jedoch sensibilisierten lediglich zwischen 13 und rund 50 Prozent der Unternehmen ihre Beschäftigten für die Gefahren von Ausforschung und auch nur ca. 40 bis 50 Prozent der Unternehmen führten Maßnahmen zur Loyalitätssteigerung durch. Zugangs- und Zugriffsbeschränkungen sind eine weitere Möglichkeit, um sensibles Unternehmens-Know-how zu schützen. Rund 30 bis 60 Prozent der Unternehmen gaben an, dass sie solche Beschränkungen nutzten.

Während **technische *Standard*maßnahmen** zum Schutz vor Ausforschung bei der großen Mehrheit (rund 90 Prozent) der Unternehmen Anwendung fanden, wurden umfassendere IT-Schutzvorkehrungen von deutlich weniger Unternehmen umgesetzt. So führte nur ein kleiner Teil der Unternehmen (17 bis 30 Prozent) ein kontinuierliches Monitoring der Log-Daten durch, deren regelmäßige Auswertung auf ungewollte Zugriffe auf das IT-System aufmerksam machen kann. Die technisch aufwendigere Verschlüsselung des E-Mail-Verkehrs, die einen sehr effektiven Schutz vor Ausforschung bieten kann, wurde von 18 bis 27 Prozent der Unternehmen genutzt. Aber selbst relativ einfach umsetzbare Maßnahmen,

wie beispielsweise das Verbot der Nutzung von USB-Sticks oder CD-Brennern am Arbeitsplatz, wurden von weniger als jedem dritten Unternehmen (18 bis 27 Prozent) ergriffen.

4.6. Kooperation der Unternehmen mit den Sicherheitsbehörden

In der Fachliteratur geht man davon aus, dass in den meisten Fällen von Ausforschung die betroffenen Unternehmen zur Aufklärung des Vorfalls eher ein **privates Sicherheitsunternehmen** einschalten als die Polizei. Werden Ausforschungsvorfälle ausschließlich von privaten Sicherheitsunternehmen oder dem Verfassungsschutz behandelt, **erscheinen sie nicht in der Polizeilichen Kriminalstatistik**. Eine konsequente Lagebeschreibung könnte den Unternehmen dabei helfen, kostenintensive und nicht unbedingt notwendige Sicherheitsvorkehrungen einzusparen. Zudem ist es wichtig, dass sich die betroffenen Unternehmen auch an die Strafverfolgungsbehörden wenden, da eine **konsequente Strafverfolgung** ihre Glaubwürdigkeit nach innen und nach außen unterstützt und auch bei den eigenen Beschäftigten zu einem verbesserten Werte- und Unrechtsbewusstsein führt. Werden die Strafverfolgungsbehörden von Ausforschungsvorfällen in Kenntnis gesetzt, kann auch verhindert werden, dass Kriminelle mit der gleichen Vorgehensweise mehrere Unternehmen schädigen.

Wie in der Fachliteratur geschildert, zeigt auch der Vergleich der Studienergebnisse, dass die **Meldebereitschaft** der Unternehmen bei Ausforschung **sehr niedrig** ist. In den Studien gaben zwischen **4 und 33 Prozent der Unternehmen** an, sich im Verdachts- oder Schadensfall an die Sicherheitsbehörden gewandt zu haben. Ein wichtiger **Grund** für die Zurückhaltung der Unternehmen beim Einschalten der Sicherheitsbehörden war, dass sie die Zuständigkeiten, Aufgaben und Sicherheitsangebote der Behörden **nicht** ausreichend gut **kannten**. 33 bis 50 Prozent der deutschen und 85 Prozent der österreichischen Unternehmen machten diese Angabe. Das führt folglich auch dazu, dass Unternehmen ungenaue oder falsche Vorstellungen vom Ablauf der Ermittlungen haben. Ein weiterer Grund für die geringe Kooperation (bei rund 50 Prozent der Unternehmen) war die Angst, dass der Ausforschungsvorfall durch die Kooperation mit den Strafverfolgungsbehörden automatisch an die Öffentlichkeit gelangt und dass auf diese Weise dem Unternehmen ein **Reputationsschaden** entstehen könnte. Ferner gaben erneut ca. 50 Prozent der Unternehmen an, dass sie eine Meldung eines Vorfalls unterließen, da ihnen der **Aufwand zu hoch** und der Nutzen zu gering erschienen.

4.7. Wichtige Akteure im Bereich der Abwehr von Ausforschung und im Informationsschutz

Es ist wichtig, dass sich Unternehmen im Sinne wirkungsvoller Schutzmaßnahmen vor Ausforschung mit anderen Akteuren **austauschen** und mit ihnen **kooperieren**, denn eine effektive Abwehr von Ausforschung kann weder von Sicherheitsbehörden, noch von Wirtschaftsverbänden und Unternehmen allein geleistet werden. Beratungs- und Informationsangebote werden von unterschiedlichen Akteuren (Privatwirtschaft, Behörden und Verbände) bereitgestellt. Unternehmen können somit auf eine große Bandbreite an **Beratungsmöglichkeiten** zurückgreifen, die ihnen dabei helfen, Kenntnisse zu Handlungsoptionen zu verbessern und vorhandene Netzwerke besser zu nutzen. Die Ergebnisse der Studien zeigen, dass Unternehmen bei der Abwehr von Ausforschung **häufiger mit privaten Akteuren zusammenarbeiten** als mit Behörden. So nutzten etwa zwei Drittel der Unternehmen Beratungs- und Informationsangebote privater Akteure, während die Angebote öffentlicher Einrichtungen nur von rund 30 Prozent in Anspruch genommen wurden. Das kann u. a. daran liegen, dass es deutlich mehr private als öffentliche Einrichtungen im Bereich Wirtschaftsschutz und Spionageabwehr gibt, die dementsprechend auf das jeweilige Unternehmen zugeschnittene Angebote erarbeiten können.

Die Hilfestellungen von **privaten Akteuren** wurden von den Unternehmen **häufig besser** und manchmal ähnlich bewertet wie die Angebote öffentlicher Akteure. Während z. B. ca. 60 Prozent der Unternehmen die Angebote privater Akteure als geeignet zur Erhöhung der IT-Sicherheit im Unternehmen einstuften, wurde die Unterstützung durch die Polizei und die Verfassungsschutzbehörden in diesem Bereich nur von ca. jedem fünften Unternehmen als hilfreich eingeschätzt.

5. Empfehlungen

Folgende Empfehlungen lassen sich aus der Fachliteratur und den empirischen Studien für die Sicherheitsbehörden ableiten:

Häufig empfehlen Experten den Unternehmen, sich im Verdachtsfall nicht sofort an die Strafverfolgungsbehörden zu wenden, da es diesen nicht immer möglich sei, die Interessen der Unternehmen zu berücksichtigen und die Gefahr bestehe, dass Vorfälle unfreiwillig öffentlich gemacht werden. Gerät ein Ausforschungsvorfall aber an die Öffentlichkeit, führt das fast immer zu Umsatzeinbußen und einem hohen Reputationsschaden für das betroffe-

ne Unternehmen. Bei einem Verdacht wenden sich Unternehmen somit häufiger an **professionelle Sicherheitsunternehmen**. Diese Einschätzung der Verfahrensweise der Strafverfolgungsbehörden erscheint jedoch obsolet. Gerade bei Vorfällen von Wirtschaftsspionage und Konkurrenzausspähung achten die Strafverfolgungsbehörden heutzutage auf eine besondere Sensibilität im Umgang mit betroffenen Unternehmen, da sie deren Sorgen vor einem Imageverlust und Wunsch nach Schadensbegrenzung kennen.

Gemäß dem **Legalitätsprinzip** sind die Strafverfolgungsbehörden verpflichtet, bei Kenntnis einer Straftat tätig zu werden. Für die Staatsanwaltschaft bestehen jedoch auch gesetzlich geregelte Ausnahmen vom Verfolgungszwang. Staatsanwaltschaft und Polizei ist es wichtig, den betroffenen Unternehmen den Handlungsspielraum aufzuzeigen und eine abgestimmte Vorgehensweise zu erarbeiten.

Auch unternehmensinterne Sanktionen im Rahmen von **Compliance Management Systemen** können ausschlaggebend dafür sein, dass Vorfälle nicht den Strafverfolgungsbehörden gemeldet werden. Die Strafverfolgungsbehörden können über andere Wege Erkenntnisse zu der Phänomenentwicklung von Wirtschaftsspionage und Konkurrenzausspähung erhalten: Eine Möglichkeit wäre die **Schaffung von Plattformen**, die Unternehmen für einen vertrauensvollen Austausch mit den Strafverfolgungs- und Verfassungsschutzbehörden nutzen können. Denkbar wäre auch eine **Datenbank**, in der die von Unternehmen anonym und freiwillig gemeldeten Ausforschungsvorfälle erfasst werden. Aber auch **großangelegte repräsentative Opferbefragungen** können den Sicherheitsbehörden relevante Informationen u. a. in Bezug auf die Betroffenheitsrate, das Anzeigeverhalten und die Schadenshöhe liefern. Der Bedarf für weitere empirische Forschung ist durchaus vorhanden. Die Sicherheitsbehörden sollten ***eigene*** **Dunkelfeld- und Opferbefragungen** in Auftrag geben, um eine methodisch abgesicherte und transparente Vorgehensweise unter Berücksichtigung der eigenen Interessenslage gewährleisten zu können. Im Rahmen einer *eigenen* Unternehmensbefragung könnten die Sicherheitsbehörden darüber hinaus darauf achten, dass genauer zwischen den verschiedenen Akteursgruppen unterschieden wird (Strafverfolgungsbehörden, Verfassungsschutzbehörden, Netzwerke, private Unternehmen etc.), da solche Unterscheidungen in der Mehrzahl der ausgewerteten Befragungen fehlen. Zudem wäre es den Sicherheitsbehörden möglich, die Gründe der Unternehmen für eine unterbliebene Meldung eines Ausforschungsvorfalls sowie Empfehlungen und Vorschläge der Unterneh-

men zur Verbesserung des Schutzes vor Wirtschaftsspionage und Konkurrenzausspähung zu erheben – qualitative Aussagen, die bislang von den wenigsten Studien abgefragt wurden.

Häufig gaben Unternehmen an, dass ihnen die Arbeit der Sicherheitsbehörden sowie die zentralen Ansprechpartner im Bereich der Abwehr von Wirtschaftsspionage und/oder Konkurrenzausspähung **nicht bekannt sind**. Es ist wichtig, dass die Sicherheitsbehörden ihre Angebote und Maßnahmen optimieren. So fordert der DIHK z. B., dass die Bundesregierung die Sicherheitsbehörden personell und materiell dazu befähigt, wirksamer gegen Ausforschung vorgehen zu können. Optimierungsmöglichkeiten gibt es u. a. in Bezug auf die **Handlungsfähigkeit und Reaktionsgeschwindigkeit** der Strafverfolgungsbehörden bei Straftaten im IT-Bereich, vor allem auch, wenn über Landesgrenzen hinweg agiert werden muss.

Auch wünschen sich viele Unternehmen einen **gemeinsamen Ansprechpartner** im Bereich Wirtschafts- und Informationsschutz, der die verschiedenen Behörden koordiniert. Es sollte für die Unternehmen leicht ersichtlich sein, wer bei einem Ausforschungsvorfall der richtige Ansprechpartner ist. Alle regionalen Ansprechpartner könnten z. B. auf einer **zentralen Website** zusammengefasst werden.

Damit die Angebote und Maßnahmen der Sicherheitsbehörden im Bereich der Abwehr von Ausforschung besser bekannt werden, sollten die Behörden vermehrt in **direkten Kontakt** mit der Wirtschaft treten. Auf diese Weise können falsche Vorstellungen oder mögliche Ängste aus dem Weg geräumt werden. Eine Kooperation mit **Verbänden** und **Kammern** ist zu empfehlen, da sie in dieser Hinsicht oft den engsten Kontakt zu Unternehmen pflegen und ihre wichtigsten Ansprechpartner sind. Auch eine Teilnahme an nationalen oder europäischen öffentlich-privaten Partnerschaften, die u. a. von der Europäischen Agentur für Netz- und Informationssicherheit initiiert werden, könnte dabei helfen, die Belange und Interessen der Sicherheitsbehörden bekannter zu machen.