UNIVERSITÄT BERN

Rechtswissenschaftliche Fakultät

Institut für Strafrecht und Kriminologie

Bern, 20.1.2020

Wirtschaftsspionage in der Schweiz

Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB)

Fabienne Zwahlen[1], Irene Marti[2], Marina Richter[3], Cathrine Konopatsch[4], Ueli Hostettler[5]

[1] MSc Erziehungswissenschaft, Projektkoordinatorin

[2] MA Sozialanthropologin, Projektmitarbeiterin

[3] PD Dr. Soziologie und Geographie, Projektmitarbeiterin

[4] Dr. LL.M. Rechtswissenschaft, Projektbeirat

[5] PD Dr. Sozialanthropologie, Projektverantwortung (ueli.hostettler@krim.unibe.ch)

Zitiervorschlag:
Zwahlen, Fabienne, Marti, Irene, Richter, Marina, Konopatsch, Cathrine & Hostettler, Ueli (2020). Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB). Bern: Universität Bern – Institut für Strafrecht und Kriminologie.

UNIVERSITÄT
BERN

Inhaltsverzeichnis

Management Summary

Zwahlen, Fabienne, Marti, Irene, Richter, Marina, Konopatsch, Cathrine & Hostettler, Ueli (2020). Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB). Bern: Universität Bern – Institut für Strafrecht und Kriminologie.

Ausgangslage

Wirtschaftsspionage ist eine komplexe Thematik (siehe Fleischer 2016; Tsolkas & Wimmer 2013). Zum einen ist dies der Tatsache geschuldet, dass in der Praxis die Übergänge zwischen Wirtschaftsspionage und Industriespionage aufgrund der in vielen Bereichen vorhandenen engen Verknüpfungen zwischen staatlichen und privaten Aktivitäten nicht trennscharf sind, zum anderen fehlt es an verlässlichen Daten bezüglich Fallzahlen, Täterschaft oder den tatsächlichen Schäden. Dies hängt auch damit zusammen, dass es für die betroffenen Unternehmen schwierig ist, Wirtschaftsspionage von Industriespionage oder sonstigen kriminellen Handlungen (z. B. Erpressung) zu unterscheiden. Zudem sind die Urheber und deren Intentionen oft nur schwer zu eruieren und in vielen Fällen bleiben Angriffe gänzlich unbemerkt. Gleichzeitig scheuen sich viele Firmen vor einer Meldung von Verdachtsmomenten und entdeckten Fällen von Spionage, da sie oft Reputationsschäden oder wirtschaftliche Einbussen befürchten, wenn solche Informationen an die Öffentlichkeit gelangen. Entsprechend hoch ist die Dunkelziffer und entsprechend lückenhaft ist das Wissen über Wirtschaftsspionage (siehe Kaspar 2014; Wimmer 2015).

Neben Studien von Consultingfirmen wie KPMG und PWC (KPMG 2019; PWC 2016) gibt es für den deutschsprachigen Raum derzeit vor allem eine aktuelle wissenschaftliche Studie, die vom Max-Planck-Institut für ausländisches und internationales Strafrecht gemeinsam mit dem Fraunhofer Institut für System- und Innovationsforschung durchgeführt wurde. Die WISKOS-Studie (Bollhöfer & Jäger 2018) zeigt, dass in Deutschland in der Vergangenheit jedes dritte KMU bereits einmal Opfer von Wirtschaftsspionage geworden ist oder von Konkurrenzausspähung betroffen war. Für die Schweiz bestehen solche Studien derzeit nicht. Um das Ausmass der Wirtschaftsspionage in der Schweiz gründlicher zu erforschen, hat der Nachrichtendienst des Bundes (NDB) das Institut für Strafrecht und Kriminologie der Universität Bern beauftragt, bei Unternehmen in der Schweiz eine Studie zu diesem Thema durchzuführen. Ziel der Studie ist es, eine detaillierte Bestandsaufnahme der Thematik zu erstellen, die finanziellen und andere Schäden einzuschätzen sowie die Qualität der Zusammenarbeit zwischen den Unternehmen und den Behörden zu eruieren. Die Ergebnisse sollen dem NDB zudem Hinweise für die Steuerung der Spionageabwehr und für die Weiterentwicklung des Präventions- und Sensibilisierungsprogramms Prophylax geben. Konkret sollen sie es ermöglichen, den Schutz vor Spionage, u. a. durch die Sensibilisierung des Werk- und Forschungsplatzes Schweiz, zu verbessern.

Design der Studie und methodisches Vorgehen

Die Studie umfasst zwei Teile:
1) Eine **qualitative Befragung** der zuständigen EntscheidungsträgerInnen auf der Basis von Einzelinterviews
2) Eine **quantitative Befragung** im Rahmen einer repräsentativen Stichprobe von relevanten Firmen verschiedener Grösse und aus verschiedenen Tätigkeitsbereichen.

Die Erhebungsinstrumente (Leitfaden für die Interviews und Onlinefragebogen) wurden in Zusammenarbeit mit dem NDB entwickelt.

Tabelle 1: Übersicht Datengrundlage Teilstudie 1 (qualitativ)

	Anzahl	Anzahl Teilnehmende/Dauer der Gespräche
ExpertInnen	8	8 * 60–90 Min.
KMU	27	27 * 60–90 Min.
Grossunternehmen	13	15 * 60–90 Min.
Hochschulen/Forschungsinstitute	3	4 * 60–90 Min.

Studie «Wirtschaftsspionage in der Schweiz», Universität Bern, 2020

Tabelle 2: Übersicht Datengrundlage Teilstudie 2 (quantitativ)

	Anzahl	Prozent
Stichprobe	**3065**	**100%**
Rücklauf	**362**	**12%**
Nach Wirtschaftssektor	Anzahl	Prozent
Primärer Wirtschaftssektor (Rohstoffgewinnung)	19	5%
Sekundärer Wirtschaftssektor (Fabrikation/Materialverarbeitung)	145	40%
Tertiärer Wirtschaftssektor (Dienstleistungen)	156	43%
Keine Angaben	42	12%
Nach Unternehmensgrösse	Anzahl	Prozent
Kleinstunternehmen: weniger als 10 Mitarbeitende	33	9%
Kleine Unternehmen: 10–49 Mitarbeitende	250	69%
Mittlere Unternehmen: 50–249 Mitarbeitende	62	17%
Grossunternehmen: mehr als 250 Mitarbeitende	14	4%
Keine Angaben	3	1%

Studie «Wirtschaftsspionage in der Schweiz», Universität Bern, 2020

Konkrete Spionagevorfälle und Verdachtsfälle in Unternehmen

Von den befragten Unternehmen gaben in der quantitativen Studie **15%** an, von einem Wirtschaftsspionagevorfall betroffen worden zu sein. Im Rahmen der Einzelinterviews zeigte sich, dass **1/3 der Unternehmen** schon mindestens einmal **Opfer von Wirtschaftsspionage** geworden sind. Es handelt

sich um Vorfälle, welche von der Firma selbst und/oder vom NDB als Wirtschaftsspionage identifiziert wurden. Die Unternehmensgrösse spielt aber keine wesentliche Rolle: Von Wirtschaftsspionage betroffen sind sowohl KMU als auch Grossunternehmen. Die Ergebnisse der vorliegenden Studie zeigen, dass insbesondere die Branchen Baugewerbe/Bau, Information, Kommunikation und Verlagswesen, Maschinenbau und Industrie, Luft- und Raumfahrttechnik, Rüstungsindustrie, Pharma und Life Science, Elektronik sowie die Branche Messtechnik von Wirtschaftsspionage betroffen sind. Die Branchen Maschinenbau und Industrie (Ergebnis quantitative Studie) und Pharma und Life Science (Ergebnis qualitative Studie) sind am stärksten von konkreten Spionagevorfällen betroffen.
Wenn es zu einem Spionagefall kommt, stellt sich rasch die Frage des Schadens. Dieser ist sowohl durch die Betroffenen wie auch durch externe ExpertInnen nur sehr schwer zu beziffern. Einige Studien nehmen zwar solche Einschätzungen für Branchen oder die nationale Wirtschaft und Gesellschaft vor (bspw. Bitkom 2016; PWC 2016), doch sind diese aus praktischen und methodischen Gründen wenig verlässlich und deshalb mit Vorsicht zu geniessen. Einfacher zu beziffern ist der direkte materielle Schaden wie ein Produktionsausfall, der Verlust eines Geschäfts oder ein Mehraufwand für die Bekämpfung der Spionage wie der Aufwand für Informatik und Kommunikation etc. Schwierig zu beziffern ist hingegen der längerfristige Reputationsschaden, der entsteht, wenn ein Fall publik wird. Ein Reputationsschaden zieht potenziell einen grossen materiellen Verlust nach sich, wenn längerfristig Aufträge und Kunden verloren gehen. In unserer Umfrage gaben 11% der Firmen, welche einen Spionagefall bemerkten, an, der Fall habe die Existenz der Firma gefährdet. Dies deutet auf die potenziell gravierende Wirkung von Wirtschaftsspionage hin.

Prävention

Die befragten Firmen halten interne Prävention für deutlich wichtiger als die Unterstützung durch externe SpezialistInnen oder durch staatliche Stellen. Sie nutzen dafür die unterschiedlichen Bereiche von Prävention (strukturelle Aspekte und organisatorische Regelungen, Schulung und Sensibilisierung von Mitarbeitenden, Massnahmen im Bereich Informatik und Telekommunikation sowie physische und technische Sicherung). Der Grad der Präventionsbemühungen ist jedoch sehr unterschiedlich und hängt stark mit der Unternehmensgrösse und damit auch mit den vorhandenen Ressourcen für Spionageprävention zusammen. Zudem ist vor allem in KMU das Bewusstsein für die Risiken in Bezug auf Datenaustausch und digitale Kommunikation (etwa E-Mails) oft sehr wenig ausgeprägt.

Zukünftige Entwicklungen

Die befragten Firmen weisen in Bezug auf zukünftige Entwicklungen insbesondere auf die Digitalisierung und Globalisierung hin. Mit der Digitalisierung steigen die Herausforderungen für Unternehmen, ihre Daten (bspw. Produktionsdaten, aber auch Kundendaten) in digitaler Form sicher zu bewirtschaften. Wenn heute bereits eine grosse Zahl der Angriffe über den digitalen Weg führt, ist damit zu rechnen, dass in Zukunft vermehrt auf diesem Weg angegriffen wird. Ebenso stellt die Globalisierung eine Herausforderung dar. Märkte werden globaler und damit stellen sich bspw. auch neue Fragen des Patentschutzes auf internationaler Ebene. Im gleichen Zug setzen sich Geschäftspartner, Zulieferfirmen sowie die Kundschaft immer globaler zusammen und die weiterhin

vorhandenen unterschiedlichen nationalen Gesetzeskontexte und Geschäftskulturen stellen damit eine Herausforderung dar. Schliesslich wird auch die Herkunft der Mitarbeitenden globaler. Wenn einige Firmen als Strategie anführten, dass sie primär Mitarbeitende mit persönlich bekannten Referenzen rekrutieren, so schränkt dies wohl angesichts der Entwicklung die Auswahl qualifizierter MitarbeiterInnen übermässig ein. Die Gewährleistung der Sicherheit bei Neurekrutierung von Mitarbeitenden wird vor allem für KMU damit schwieriger. Schliesslich stellt sich auch die Frage der politischen Bedeutung des Themas und der Aufgaben sowie der entsprechenden institutionellen und personellen Ausstattung der Stellen auf Bundes- und Kantonsebene. Im Vergleich zu anderen Ländern verfügt die Schweiz, gemäss den von uns befragten ExpertInnen, im Bereich Prävention und Bekämpfung von Spionage über eine eher geringere institutionelle und materielle Ausstattung.

Literatur

Bollhöfer, Esther & Jäger, Angela (2018). Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Band A 8 09/2018. Freiburg i.Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Fleischer, Dirk (2016). Wirtschaftsspionage. Phänomenologie – Erklärungsansätze – Handlungsoptionen. Wiesbaden: Springer.

Kasper, Karsten (2014). Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse. Wiesbaden: Bundeskriminalamt.

KPMG (2019). Wirtschaftskriminalität und was man dagegen tun kann. *Audit Committee News – Risk Management & Compliance*. 66 (Q3 2019): 1–6. https://home.kpmg/content/dam/kpmg/ch/pdf/wirtschaftskriminalitaet-was-man-dagegen-tun-kann-de.pdf [Zugriff am 16.7.2019].

PWC (2016). Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. https://www.pwc.de/wirtschaftskriminalitaet. [Zugriff am 16.7.2019].

Tsolkas, Alexander & Wimmer, Friedrich (2013). Wirtschaftsspionage und Intelligence Gathering. Neue Trends der wirtschaftlichen Vorteilsbeschaffung. Wiesbaden: Springer.

Wimmer, Bruce (2015). Business Espionage. Risk, Threats, and Countermeasures. Waltham, MA: Elsevier.

Tabellen- und Abbildungsverzeichnis

1. Einleitung

1.1 Ausgangslage

Unter Spionage versteht man die unerlaubte Beschaffung von Informationen und Daten und unterscheidet dabei zwischen Wirtschafts- und Industriespionage: Bei der Wirtschaftsspionage geht es um die Beschaffung von bewusst vertraulich oder geheim gehaltenen wirtschaftlichen, wissenschaftlichen oder technologischen Informationen oder Daten, sofern dies zum Nachteil der Schweiz oder ihrer Unternehmen, Institutionen oder von Personen in der Schweiz geschieht und die Informationen an einen ausländischen Akteur (Staat, Gruppierung, Unternehmen, Person usw.) weitergegeben werden (siehe Fleischer 2016; Kaspar 2014) (Verstoss gegen Art. 273 Strafgesetzbuch (StGB): Wirtschaftlicher Nachrichtendienst). Bei der Konkurrenz- oder Industriespionage handelt es sich hingegen um die Ausspähung zwischen einzelnen (konkurrierenden) Unternehmen innerhalb eines Landes (siehe Fleischer 2016; Kaspar 2014) (Verstoss gegen Art. 162 StGB: Verletzung des Fabrikations- oder Geschäftsgeheimnisses).

Wirtschaftsspionage ist eine komplexe Thematik (siehe Fleischer 2016; Tsolkas & Wimmer 2013). Zum einen ist dies der Tatsache geschuldet, dass in der Praxis die Übergänge zwischen Wirtschaftsspionage und Industriespionage aufgrund der in vielen Bereichen vorhandenen engen Verknüpfungen zwischen staatlichen und privaten Aktivitäten nicht trennscharf sind, zum anderen fehlt es an verlässlichen Daten bezüglich Fallzahlen, Täterschaft oder den tatsächlichen Schäden. Dies hängt unter anderem damit zusammen, dass es für die betroffenen Unternehmen schwierig ist, Wirtschaftsspionage von Industriespionage oder anderen Formen kriminellen Handelns (z. B. Erpressung) zu unterscheiden. Zudem sind die Urheber und deren Intentionen oft nur schwer zu eruieren, oder viele Angriffe bleiben gänzlich unbemerkt. Gleichzeitig scheuen sich viele Firmen vor einer Meldung von Verdachtsmomenten und entdeckten Fällen von Spionage, da sie oft Reputationsschäden oder wirtschaftliche Einbussen befürchten, wenn solche Informationen an die Öffentlichkeit gelangen. Entsprechend hoch ist die Dunkelziffer und entsprechend lückenhaft ist das Wissen über Wirtschaftsspionage (siehe Kaspar 2014; Wimmer 2015).

Neben Studien von Consultingfirmen wie KPMG und PWC (KPMG 2019; PWC 2016) gibt es für den deutschsprachigen Raum derzeit vor allem eine aktuelle wissenschaftliche Studie, die vom Max-Planck-Institut für ausländisches und internationales Strafrecht gemeinsam mit dem Fraunhofer

Institut für System- und Innovationsforschung durchgeführt wurde (WISKOS-Studie). Diese Studie (Bollhöfer & Jäger 2018) zeigt, dass in Deutschland in der Vergangenheit jedes dritte KMU bereits einmal Opfer von Wirtschaftsspionage wurde oder von Konkurrenzausspähung betroffen war. Für die Schweiz fehlte bis anhin eine solche Studie. In Anbetracht dieser Tatsache stellt sich die Frage, wie die Situation in der Schweiz aussieht, welche Branchen betroffen sind, inwiefern sich Firmen der Gefahr bewusst sind und wieviel Ressourcen sie für Sicherheit und Prävention aufbringen.

Für die vorliegende Studie wurden zusätzlich zu den unten beschriebenen Erhebungsmethoden auch vorbereitende Gespräche mit ExpertInnen geführt. Aus diesen Gesprächen können in einer ersten Annäherung einige Eckpunkte des Phänomens Wirtschaftsspionage in der Schweiz abgeleitet werden. So sind gemäss den ExpertInnen vor allem die Branchen Industrie, Pharma und Chemie, die Banken wie auch die Wissensproduktion an ETH/EPFL, Universitäten und Fachhochschulen Ziel von Spionage. Spionage kann sowohl grosse Unternehmen mit internationaler Marktdurchdringung wie auch kleine Unternehmen betreffen, die als Nischenproduzenten mit ihrem Produkt eine global führende Rolle einnehmen und sich oft der Bedrohung durch Spionage nicht unmittelbar bewusst sind. Dies können u. U. auch kleine Start-Up-Firmen sein, die sich vor allem auf Innovation und Produktentwicklung konzentrieren und in Bezug auf die Unternehmensentwicklung noch am Anfang stehen und daher bisher wenig in Sicherheit investiert haben.

Allgemein stellen Sicherheit und Werbung/Verkauf immer entgegengesetzte Pole dar. Der Pol Sicherheit zielt auf eine Limitierung des Zugangs zu Wissen und Daten: Es geht darum, wie viel Wissen und Daten gesichert bleiben müssen und wie viele Details der Produktion geschützt werden müssen, um Spionage vorzubeugen. Demgegenüber nutzt der Pol Werbung/Verkauf Informationen zum Unternehmen und zu seinen Produkten: Es stellt sich demnach die Frage, wie viel Wissen vermittelt werden muss, um potenzielle Kunden von einem Produkt und seiner Qualität zu überzeugen, und wie viel Kenntnisse nötig sind, damit das Produkt vom Kunden auch eingesetzt und gewartet werden kann.

Gerade die zunehmende Bedeutung der Digitalisierung und damit auch des Auslagerns von Diensten (Informatik) und Daten (bspw. in Cloud-Lösungen) bedeuten eine unternehmerische Herausforderung. Digitale Netzwerke stellen eine derzeit medial intensiv diskutierte Eingangspforte für Spionage und Cyberkriminalität dar (siehe Gragido & Pirc 2011; NZZ 2018; Tages-Anzeiger 2019). Für gezielte Wirtschaftsspionage ist der Faktor Mensch jedoch nach wie vor nicht zu unterschätzen

(siehe Bitkom 2016). Die enorme Menge an Daten erfordert menschliches Wissen zur Identifizierung und Verknüpfung relevanter Informationen. Entsprechend wichtig sind neben der Investition in Informatiksicherheit auch die wiederholte Schulung und die kontinuierliche Sensibilisierung der Mitarbeitenden sowie deren sorgfältige Auswahl und Kontrolle.

Wenn es zu einem Spionagefall kommt, stellt sich rasch die Frage des Schadens. Dieser ist sowohl für die Betroffenen wie auch durch externe ExpertInnen nur sehr schwer zu beziffern. Einige Studien nehmen zwar solche Einschätzungen für Branchen oder die nationale Wirtschaft und Gesellschaft vor (bspw. Bitkom 2016; PWC 2016), doch sind diese aus praktischen und methodischen Gründen wenig verlässlich und deshalb mit Vorsicht zu geniessen. Oft lässt sich zwar der aktuelle, rein materielle Schaden, bspw. wenn es um einen Produktionsausfall geht, noch vergleichsweise einfach ermitteln. Wenn es jedoch um Folgeschäden wie den Reputationsverlust eines Unternehmens geht, lässt sich der Schaden kaum eruieren.

Schliesslich stellt sich auch die Frage der politischen Bedeutung des Themas, der Aufgaben sowie der entsprechenden institutionellen und personellen Ausstattung der Stellen auf Bundes- und Kantonsebene. Im Vergleich zu anderen Ländern verfügt die Schweiz, gemäss den von uns befragten ExpertInnen, im Bereich Prävention und Bekämpfung von Spionage über eine eher geringe institutionelle und personelle Ausstattung. Dies widerspiegelt sich auch in der Bedeutung, welche Spionagebekämpfung, Cyberkriminalität und Sicherheitsfragen in der Ausbildung haben. An den Hochschulen finden diese Thematiken ausserhalb spezialisierter Ausbildungsgänge zu Cybercrime kaum Beachtung.

1.2 Auftrag der Studie

Angesichts der mangelnden Datenlage für die Schweiz schrieb der Nachrichtendienst des Bundes (NDB) im Jahr 2017 eine Studie zur Abschätzung des Ausmasses von Wirtschaftsspionage in der Schweiz aus. Die Studie soll Folgendes leisten:

1) Eine detaillierte Bestandsaufnahme der Problematik im Kontext der relevanten schweizerischen Wirtschaftsbranchen und Unternehmen liefern.
2) Eine Einschätzung der durch die Wirtschaftsspionage entstandenen Schäden für Schweizer Unternehmen und die Schweizer Wirtschaft als Ganzes vornehmen.

3) Die Qualität der Zusammenarbeit zwischen Unternehmen und den staatlichen Organen (insbesondere dem NDB) durch die Unternehmen einschätzen und auswerten.

1.3 Design der Studie und methodisches Vorgehen

Die Studie umfasst neben der Auswertung bestehender Literatur explorative ExpertInnengespräche und zwei methodisch unterschiedliche Teilstudien:

1) Eine **qualitative Befragung (Teilstudie 1)** der zuständigen EntscheidungsträgerInnen in einer relevanten Auswahl von Firmen unterschiedlicher Grösse und in verschiedenen Tätigkeitsbereichen auf der Basis von Einzelinterviews.
2) Eine **quantitative Befragung (Teilstudie 2)** auf der Basis einer repräsentativen Stichprobe von relevanten Firmen unterschiedlicher Grösse und aus verschiedenen Tätigkeitsbereichen mittels einer Onlinebefragung.

Für die Vorbereitung wurden zuerst die bereits angesprochenen **ExpertInneninterviews** mit insgesamt acht Personen geführt (Tabelle 1). Sieben Gespräche kamen zustande, nachdem der NDB die Information zur Studie weitergeleitet hatte. Eine Person meldete sich von sich aus, nachdem sie den Fragebogen der Teilstudie 2 ausgefüllt hatte. Durch diesen explorativen Teil der Studie konnte ein erster Überblick gewonnen werden, was die Vorbereitung der Interviews der qualitativen Studie erleichterte. Die so gewonnenen Informationen sind ebenfalls in die Konstruktion des Fragebogens der Teilstudie 2 eingeflossen.

Die **Teilstudie 1 (qualitative Befragung)** umfasst Interviews mit für Sicherheit, Compliance, ITK, Spionage etc. verantwortlichen Personen in insgesamt 43 Schweizer Firmen unterschiedlicher Grösse und unterschiedlicher Branchen (Tabelle 1). Die Gespräche wurden vor Ort in den Firmen geführt. In einigen Fällen waren bei diesen Gesprächen mehrere VertreterInnen einer Firma anwesend. Der grösste Teil der Firmen (41) meldete sich als Reaktion auf den Versand der Information zur Studie durch den NDB. Zwei weitere wurden durch ExpertInnen vermittelt. Diese Interviews wurden zum Grossteil vor der Ausarbeitung des Fragebogens (quantitativ, Teilstudie 2) durchgeführt, sodass erste Erkenntnisse aus den Gesprächen ebenfalls in den Fragebogen einfliessen konnten. Als Methode wurde für die Gespräche der Teilstudie 1 das teilstandardisierte Leitfadengespräch verwen-

det, welches einerseits eine Vergleichbarkeit zwischen den Gesprächen gewährleistet und anderseits dennoch genügend Raum für Gewichtung und Vertiefung je nach Thematik erlaubt. Der Interviewleitfaden wurde nach folgenden Themen strukturiert: 1) Einleitung (inkl. Frage, was die Interviewteilnehmenden mit dem Thema Wirtschaftsspionage verbinden), 2) Präventionsmassnahmen, 3) konkrete Vorfälle, 4) potenzielle Fälle bzw. Risikosituationen, 5) branchenspezifische Einschätzungen (z. B. bzgl. der Gefahr und der Sensibilität für die Thematik), 6) Erfahrungen mit Behörden (inkl. NDB), Wünsche und Erwartungen sowie 7) zukünftige Entwicklungen und Herausforderungen. Die Gespräche dauerten zwischen 60 und 90 Minuten, wurden jeweils direkt protokolliert und zur Sicherheit und für Nachkontrollen aufgezeichnet. Die Interviewprotokolle wurden anschliessend anhand der qualitativen Analysesoftware MAXQDA kodiert und inhaltsanalytisch ausgewertet.
Das Ziel der qualitativen Befragung ist es, einen vertieften Einblick in Prävention, Verdachtsmomente und Spionagevorfälle sowie Bedürfnisse bzgl. Information und Unterstützung der einzelnen Firmen zu erhalten. Mit diesem Vorgehen konnte im Gespräch auch detailliert auf die spezifischen Situationen und Problemlagen der einzelnen Firmen eingegangen werden, wie bspw. konkrete Vorfälle oder spezifische Präventions- und Schutzdispositive. Die qualitativen Ergebnisse tragen zu einem vertieften Verständnis der Ergebnisse der quantitativen Teilstudie bei.

Tabelle 3: Übersicht Datengrundlage der ExpertInnengespräche und der qualitativen Teilstudie 1

	Anzahl	Anzahl Teilnehmende * Dauer der Gespräche
ExpertInnen	8	8 * 60–90 Min.
KMU	27	27 * 60–90 Min.
Grossunternehmen	13	15 * 60–90 Min.
Hochschulen/Forschungsinstitute	3	4 * 60–90 Min.

Studie «Wirtschaftsspionage in der Schweiz», Universität Bern, 2020

Für **Teilstudie 2** bzw. die **quantitative Befragung** mittels eines Onlinefragebogens wurde durch das Bundesamt für Statistik eine repräsentative Stichprobe aller Unternehmen in der Schweiz gezogen. Grundlage (= Grundgesamtheit) der Stichprobe sind alle in der Schweiz registrierten Firmen in durch den NDB definierten Branchen, wobei Kleinstfirmen mit weniger als 5 Mitarbeitenden nicht einbezogen wurden (Tabelle 2). Die Kontaktangaben aus der Stichprobe des Bundesamts für Statis-

tik wurden vom Projektteam telefonisch verifiziert. Dafür waren vier Personen im Einsatz: Sie überprüften die Kontaktdaten für jede Firma und nahmen telefonisch Kontakt auf, um die Firmen zu motivieren, an der Befragung teilzunehmen. Die elektronische Einladung zur Umfrage konnte anschliessend direkt an die im Telefongespräch identifizierte zuständige Ansprechperson verschickt werden. Insgesamt hat sich dieser grosse zeitliche Aufwand gelohnt, weil mit diesem Vorgehen im Vergleich zu anderen gleichgelagerten Studien ein relativ hoher Rücklauf erzielt werden konnte. Insgesamt nahmen 687 Firmen an der Umfrage teil. Für 362 Firmen liegen komplett ausgefüllte Fragebogen vor. Für die Analyse wurden alle Antworten, auch jene aus Fragebogen, die nicht vollständig ausgefüllt wurden, berücksichtigt. Deshalb ist bei einzelnen Fragen die Anzahl der Antworten grösser als 362.

Tabelle 4: Übersicht Datengrundlage Teilstudie 2 (quantitativ)

	Anzahl	Prozent
Stichprobe	**3065**	**100%**
Rücklauf	**362**	**12%**
Nach Sprachregion	Anzahl	Prozent
Deutsch	326	90%
Französisch	27	8%
Italienisch	9	2%
Nach Wirtschaftssektor	Anzahl	Prozent
Primärer Wirtschaftssektor (Rohstoffgewinnung)[1]	19	5%
Sekundärer Wirtschaftssektor (Fabrikation/Materialverarbeitung)[2]	145	40%
Tertiärer Wirtschaftssektor (Dienstleistungen)[3]	156	43%
Keine Angaben	42	12%
Nach Unternehmensgrösse	Anzahl	Prozent
Kleinstunternehmen: weniger als 10 Mitarbeitende	33	9%
Kleine Unternehmen: 10–49 Mitarbeitende	250	69%
Mittlere Unternehmen: 50–249 Mitarbeitende	62	17%

Grossunternehmen: mehr als 250 Mitarbeitende	14	4%
Keine Angaben	3	1%

[1] **Primärer Wirtschaftssektor: Rohstoffgewinnung** Branchen: Landwirtschaft, Forstwirtschaft, Energiewirtschaft, Bergbau
[2] **Sekundärer Wirtschaftssektor: Fabrikation/Materialverarbeitung** Branchen: Nahrungs-/Genussmittel, Textil/Bekleidung, Chemie, Metalle, Uhren, Elektronik, Baugewerbe usw.
[3] **Tertiärer Wirtschaftssektor: Dienstleistungen** Branchen: Handel, Banken, Versicherungen, Beratung, Tourismus, Unterrichtswesen usw.

Studie «Wirtschaftsspionage in der Schweiz», Universität Bern, 2020

Die quantitative Befragung hat zum Ziel, eine Übersicht über die Situation in der Schweiz zu erlangen und Aussagen für den Wirtschaftsstandort Schweiz formulieren zu können. Dank der repräsentativen Stichprobe auf nationaler Ebene können die Aussagen aus der qualitativen Befragung kontextualisiert und quantifiziert werden.

In über 80% der Fälle hat der/die 1) EigentümerIn, InhaberIn, TeilhaberIn (42%) oder 2) der/die angestellte GeschäftsführerIn (40%) die Umfrage für die entsprechende Firma ausgefüllt. 25% der befragten Firmen sind in den Aussenhandel involviert, von diesen gehört ein Drittel (33%, N = 33) in die Kategorie Maschinen und Apparate, elektrotechnische Waren. Die Tabelle 3 gibt eine Übersicht über die von den Befragten angegebenen Marktanteile ihres Unternehmens weltweit sowie bezogen auf die Schweiz. Der grösste Teil der Firmen weist einen Marktanteil in der Schweiz wie auch weltweit zwischen 0 und 20% aus. Ca. 12% der Firmen kontrollieren in der Schweiz den Markt ihrer Produkte zu 81 bis 100%.

Tabelle 5: Marktanteil weltweit und in der Schweiz nach Unternehmen (Teilstudie 2)

Marktanteil weltweit	Anzahl	Prozent	**Marktanteil Schweiz**	Anzahl	Prozent
0–20%	186	53.76%	0–20%	139	39.60%
21–40%	8	2.31%	21–40%	23	6.55%
41–60%	3	0.87%	41–60%	13	3.70%
61–80%	2	0.58%	61–80%	3	0.85%
81–100%	2	0.58%	81–100%	41	11.68%
Nicht bekannt	145	41.91%	Nicht bekannt	132	37.61%

Studie «Wirtschaftsspionage in der Schweiz», Universität Bern, 2020

Der Schlussbericht fasst die Ergebnisse beider Teilstudien zusammen und kombiniert so die Stärken beider methodischer Herangehensweisen.

2. Wirtschaftsspionage in der Schweiz

Das Thema Wirtschaftsspionage ist bisher in der Schweiz und auch international relativ wenig erforscht worden. Dies erklärt auch, wieso in der Öffentlichkeit kaum eine Auseinandersetzung mit der Thematik stattfindet (siehe Bollhöfer & Jäger 2018; Fleischer 2016). Die Thematik der Cyberkriminalität findet dagegen insbesondere in den Medien eine weitaus grössere Beachtung (siehe bspw. NZZ 2018, Tages-Anzeiger 2019). Die deutsche Bundesregierung hält mit Verweis auf mangelndes Grundlagenwissen dementsprechend fest: «Das Dunkelfeld im Bereich der Wirtschaftsspionage ist somit sehr gross. Belastbare statistische Fallzahlen durch Wirtschaftsspionage und Konkurrenzausspähung liegen der Bundesregierung vor diesem Hintergrund nicht vor» (Fleischer 2016). Hinsichtlich der Täterschaft kommen die wenigen bestehenden Studien überein, dass insbesondere aktuelle oder ehemalige Mitarbeitende häufig eine entscheidende Rolle spielen (siehe Bitkom 2016; Bollhöfer & Jäger 2018; Ernst & Young 2013; Kaspar 2016). Um die Situation in der Schweiz zu dokumentieren, fasst dieses Kapitel zuerst die Bedrohungswahrnehmung der Unternehmen in der Schweiz zusammen, um dann in einem zweiten Schritt von konkreten Spionagefällen ausgehend Aspekte wie Angriffsmethoden, Täterschaft oder Schaden aufzuzeigen.

2.1 Das Wichtigste in Kürze

- 15% bis 1/3 der Unternehmen in potenziell gefährdeten Branchen sind von Wirtschaftsspionage betroffen. Die Unternehmensgrösse spielt dabei keine wesentliche Rolle.
- In 11% der Fälle von Wirtschaftsspionage war die Existenz der Firma gefährdet.
- In über 40% der Angriffe, also bei knapp der Hälfte der entdeckten Fälle, waren ehemalige (25%) oder aktuelle Mitarbeitende (16.7%) des Unternehmens involviert.
- Folgende Branchen wurden von den Befragten als «hoch» gefährdet eingeschätzt: *Informatik, Telekommunikation, Life Science* (Tertiärer Wirtschaftssektor) sowie *Maschinenbau und Industrie und Pharma* (Sekundärsektor).
- Als «durchschnittlich» bis «sehr gering» gefährdet wurden folgende Branchen von den Befragten eingeschätzt: *Bergbau und Gewinnung von Steinen und Erden, Baugewerbe/Bau* (Primärer Wirtschaftssektor) sowie der *Tertiäre Bildungsbereich (Forschung und Entwicklung), Erbringung*

*von freiberuflichen, wissenschaftlichen und technischen Dienstleistung*en als auch *Handel, Verkehr und Lagerei* (Tertiärer Wirtschaftssektor).

2.2 Bedrohungswahrnehmung der Unternehmen

Gemäss den Ergebnissen aus der Teilstudie 2 (quantitative Befragung) stufen VertreterInnen der Branchen Informatik, Telekommunikation sowie Banken, Versicherungen, Immobilien als auch Maschinenbau und Industrie die potenzielle Bedrohung durch einen Wirtschaftsspionageangriff als «hoch» ein. Als «neutral» bis «sehr gering» schätzen VertreterInnen folgender Branchen das Risiko eines Angriffs ein: Bergbau und Gewinnung von Steinen und Erden; Baugewerbe/Bau; Tertiärer Bildungsbereich (Forschung und Entwicklung); Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen; Handel; Verkehr und Lagerei sowie Grundstücks- und Wohnungswesen (für eine Übersicht der Systematik der Branchen (NOGA) siehe Bundesamt für Statistik 2008).
In den Einzelinterviews mit den FirmenvertreterInnen der Teilstudie 1 (qualitative Befragung) wurden folgende Branchen als «maximal» respektive «stark» gefährdet eingeschätzt: Luft- und Raumfahrttechnik, Rüstungsindustrie, Elektroindustrie, Life Science und Pharmaindustrie, Informatik und Telekommunikationsindustrie sowie Maschinenbau (wobei diese Branche von drei Firmen auch als «durchschnittlich» bis «wenig» gefährdet eingeschätzt wurde). Als «durchschnittlich» respektive «wenig» gefährdet erachten unsere InterviewpartnerInnen die Branchen Draht- und Kabelindustrie, Uhrenindustrie, Anlage- und Gerätebau, Messtechnik, Präzisionsoptik und Feinmechanik, Baugewerbe, Industrie und Landwirtschaft, Druckerei, Energieversorgung sowie Bildung, Lehre und Forschung. Die Einschätzung der Gefährdung der letztgenannten Branche steht demnach im starken Kontrast zu den Einschätzungen der von uns interviewten ExpertInnen. Als «gar nicht» gefährdet wurden schliesslich die Branchen Entsorgungsindustrie und Kernenergie eingestuft. Die Gefährdung leitet sich zum einen aus der Branche selbst, zum anderen aus dem spezifischen Produkt ab. Wenn bspw. eine weltweit einzigartige Messtechnik Grundlage für ein Produkt ist, steigt das Risiko für Wirtschaftsspionage auch in einer ansonsten wenig gefährdeten Branche.

In den Interviews (Teilstudie 1) wurden auch Einschätzungen zu den aus Studien bekannten Risikosituationen erfragt. Solche Situationen bzw. Kontexte sind typischerweise: 1) öffentliche Veranstaltungen (Messen, Kongresse), 2) Betriebsführungen/BesucherInnen, 3) Auslandreisen, 4) Kommunikation zwischen verschiedenen Standorten sowie 5) Teil einer Lieferkette zu sein.

Bezüglich der Präsentation von Daten und Produkten bei **öffentlichen Veranstaltungen** gab die Mehrheit der Unternehmen an, über interne Standards zu verfügen. So werden bspw. Weisungen zur Kommunikation an Messen erlassen oder Vorträge im Vorfeld zusammen mit dem/der GeschäftsführerIn besprochen. Weiter existieren in vielen Firmen Standards für Ausstellungsobjekte. Manche Firmen zeigen keine Produkte, die nicht bereits auf dem Markt erhältlich sind, präsentieren Attrappen oder entnehmen dem Objekt gewisse sensible Komponenten, bevor es ausgestellt wird. Andere Firmen hingegen schätzen Messen nicht als heikle Situation ein und definieren deswegen auch keine Standards in Bezug auf Kommunikation und Ausstellungsobjekte. Dies betrifft KMU und Grossunternehmen gleichermassen.

Mehr als die Hälfte der in der Teilstudie 1 (qualitative Befragung) befragten Personen gab an, dass **BesucherInnen** (z. B. während Betriebsführungen) jeweils entlang vordefinierter Routen durch ihr Unternehmen geführt werden und dass darauf geachtet wird, sensible Bereiche bzw. Objekte nicht zu zeigen. Bei ca. einem Drittel der befragten Firmen müssen sich BesucherInnen vorgängig anmelden und beim Empfang ausweisen. Weitere, jedoch weniger verbreitete Massnahmen sind: ein Verbot von Film- und Fotoaufnahmen, Sensibilisieren und vorgängiges Informieren von Mitarbeitenden, das Verteilen von Badges oder Westen an BesucherInnen sowie ein Verbot von Mobiltelefonen. Ein kleiner Teil der befragten Firmen (bis auf eine Ausnahme alles KMU) erachteten solche Situationen als unproblematisch und gaben an, diesbezüglich keine besonderen Massnahmen zu treffen.

Auf **Auslandreisen** steht bei den interviewten FirmenvertreterInnen ein sicherer Umgang mit Laptop und Mobiltelefon im Vordergrund. Etliche Firmen verlangen bspw. von ihren Mitarbeitenden, dass sie nur firmeneigene Laptops benutzen, auf denen keine sensiblen Daten gespeichert sind. Weitere Massnahmen sind: sich nicht in öffentliche WLANs einloggen sowie das Mobiltelefon und den Laptop unterwegs ausschalten. Es werden auch personelle Massnahmen getroffen. Ungefähr ein Viertel der befragten Firmen gab an, Mitarbeitende explizit für die Thematik der Risiken bei

Auslandreisen zu sensibilisieren. Weitere, vereinzelt genannte Massnahmen betreffen die Mitnahme von Daten. Einige Firmen verlangen von ihren Mitarbeitenden, keine (Papier-)Unterlagen mitzunehmen sowie Daten auf einer (extern verwalteten oder firmeninternen) Cloud oder einem verschlüsselten USB-Stick abzulegen.

Die Mehrheit der FirmenvertreterInnen, die sich zum Thema **Kommunikation zwischen verschiedenen Standorten** äusserten, gab an, unverschlüsselt via E-Mail zu kommunizieren. Nur ein kleiner Teil der Firmen verfügt über klare Richtlinien bezüglich der Daten und Informationen, welche per Mail ausgetauscht werden dürfen. Für den Austausch von Informationen werden auch Skype, Telefon, oder Cloud-Dienste genutzt. Über ein internes, gesichertes Mail-System verfügt lediglich eine der von uns interviewten Firmen.

Als Teile einer **Lieferkette** gehen die befragten Firmen Geschäftsbeziehungen mit Lieferanten und Kunden ein. Fast die Hälfte der Interviewteilnehmenden erwähnte in diesem Zusammenhang *non-disclosure agreements* (NDA) als gängige Massnahme, um einer unerwünschten Weitergabe bzw. Verwendung von Daten durch Lieferanten oder Kunden entgegenzuwirken. Eine weitere wichtige Massnahme besteht darin, den Informationsaustausch grundsätzlich auf das Nötigste zu beschränken sowie erst nach der Lieferung eines Produkts das «fine-tuning» am Gerät vorzunehmen. Zudem erwähnten einige Firmen die bewusste Diversifikation ihrer Lieferanten. Weitere Massnahmen sind: nur im Inland bzw. in Europa mit Lieferanten Geschäftsbeziehungen eingehen, Lieferanten bzw. Kunden vorgängig überprüfen oder Lieferanten erst persönlich kennenlernen. Einige Firmen setzen stark auf die Komponente des Vertrauens und auf Stammkunden bzw. langjährige Lieferanten.

2.3 Konkrete Spionagevorfälle und Verdachtsfälle in Unternehmen

Die Frage nach konkreten Spionagefällen wurde in der Onlinebefragung (Teilstudie 2) von insgesamt 426 Personen beantwortet. Ein Grossteil (85%, N = 362) gab an, dass sie bisher keinen Vorfall von Wirtschaftsspionage in ihrer Firma bemerkt haben. 34 Personen vermuten einen Vorfall, 30 berichten von einem (13) oder mehreren Vorfällen (17). Die Firmen, die angaben, einen oder mehrere Angriffe bemerkt zu haben, gehören zu folgenden Branchen: Baugewerbe/Bau; Informatik, Telekommunikation; Maschinenbau und Industrie.

Die Branche Maschinenbau und Industrie ist demnach am stärksten von konkreten Spionagevorfällen betroffen. Die Firmengrösse bzw. die Anzahl Mitarbeitende in der Schweiz scheint keinen relevanten Einfluss auf die Anzahl Spionagefälle zu haben, im Gegensatz zur Anzahl Mitarbeitenden im Ausland: Während 82.4% der antwortenden Grossunternehmen[1] angaben, keinen Vorfall von Wirtschaftsspionage erlebt zu haben, sind es bei Unternehmen derselben Grösse mit Mitarbeitenden im Ausland nur noch 28.6%. Dagegen vermuten 57% der Grossunternehmen mit Mitarbeitenden im Ausland einen Angriff (Grossunternehmen mit Mitarbeitenden nur in der Schweiz: 11.8%) und 14.3% haben einen Angriff bemerkt (vs. 0%). Dasselbe Resultat – wenn auch weniger ausgeprägt – zeigt sich auch für Kleinstunternehmen und kleine Unternehmen. Für mittlere Unternehmen spielt die Anzahl Mitarbeitende im Ausland keine Rolle.

In den Einzelinterviews (Teilstudie 1) gaben 13 von 43 Unternehmen an, dass sie mindestens einmal Opfer von Wirtschaftsspionage geworden waren. Die betroffenen Branchen sind: Luft- und Raumfahrttechnik, Rüstungsindustrie, Messtechnik, Anlagenbau, Pharma und Life Science sowie Elektronik. Es handelte sich um Vorfälle, welche von der Firma selbst und/oder vom NDB als Wirtschaftsspionage identifiziert wurden. Weiter wurden insgesamt 25 Verdachtsmomente erwähnt. Einige dieser Vorfälle wurden den Behörden gemeldet und weiter abgeklärt. Die meisten Fälle wurden jedoch vonseiten der Firmen nicht weiterverfolgt und weder von den Firmen noch von aussenstehenden Stellen als (versuchte) Wirtschaftsspionage identifiziert. Diese als Verdachtsmomente geschilderten Situationen lassen sich grob in drei Kategorien einteilen: 1) plötzliches Auftauchen ähnlicher Produkte auf dem Markt, 2) angeblich potenzielle Kunden, die nicht nachvollziehbare Informationen verlangen, ohne eine Geschäftsbeziehung eingehen zu wollen sowie 3) Unregelmässigkeiten und aussergewöhnliche Vorfälle innerhalb der Firma.

Zu den aussergewöhnlichen Vorfällen zählen bspw. ein ungewöhnlich langsames Netzwerk über einen längeren Zeittraum hinweg, der Eindruck, dass Gespräche abgehört und E-Mails gelesen werden, sich «seltsam» verhaltende Angestellte sowie Einbruchdiebstahl.

> Wir hatten einmal einen Einbruch ganz am Anfang. Die Kaffeekasse und alles war da, aber [das neuste Produkt] wurde geklaut und ein Laptop mit der neusten Software drauf, sonst nichts. Das ist schon seltsam. [InterviewerIn: Also ein gezielter

[1] Definition Unternehmensgrösse: Kleinstunternehmen haben weniger als 10 Mitarbeitende, kleine Unternehmen 10–49 Mitarbeitende mittlere Unternehmen 50–249 Mitarbeitende und Grossunternehmen mehr als 250 Mitarbeitende (siehe KMU 2018).

> Einbruch?] Das sagt die Polizei. Ich sage, der wollte lediglich [das Produkt] klauen. Aber er kann [es] nicht brauchen. Wir haben diese Seriennummer in unseren ganzen Software-Updates gesperrt. Wenn jemand irgendwo die Software verwendet hätte, hätte man das gemerkt. Dann hätte es ihm [das Produkt] gesperrt und wir hätten eine Meldung erhalten. (KMU, 11.2.2019)

In den Interviews wurde mehrmals auf die Schwierigkeit hingewiesen, die häufigen Cyberangriffe richtig zu deuten. Im Zentrum steht hier die Frage, ob es bei solchen Angriffen darum geht, der Firma einen finanziellen Schaden zuzufügen, oder darum, an Daten zu gelangen. Die Schwierigkeit der Unterscheidung wird durch das oftmals identische Vorgehen begründet:

> Es ist schwierig zu sagen, ob es tatsächlich Wirtschaftsspionage ist. Die Fälle, die mir bis jetzt bekannt sind, da würde ich jetzt nicht sagen, dass es um Wirtschaftsspionage geht. Also am Schluss, vielleicht ist es das, ja, man müsste Wirtschaftsspionage einmal definieren. Die Angriffe, die wir tagtäglich haben, da geht es darum, Malware zu installieren, um Computer fern zu steuern. Ob dahinter wirtschaftliche Gedanken stecken, es um Intellectual Property geht, oder es darum geht, so rasch wie möglich reich zu werden? (Grossunternehmen, 4.2.2019)

2.3.1 Angriffsmethoden

Auf die Frage, in welchem Zusammenhang der Spionageangriff stattfand, antworteten in der quantitativen Befragung (Teilstudie 2) 66 Personen. Von diesen geben 39% an, dass Angriffe mittels E-Mails mit kritischem Inhalt erfolgten. An zweiter Stelle wird der Einsatz von privaten Geräten (15%) genannt, gefolgt von Investitionsabsichten von Dritten (12%). Reisen (5%) und Joint Ventures werden nur selten als Angriffsmethoden genannt (vgl. Abbildung 1).

Abbildung 1: Situationen/Kontexte von Spionageangriffen (Mehrfachantworten)

Cyberangriffe gegen das Firmennetzwerk (19%) sowie Phishing-/Spearphishing-Angriffe gelten zu den am häufigsten erwähnten Angriffsmethoden. Bei 40% der genannten Fälle waren ehemalige oder aktuelle Mitarbeitende involviert (Datendiebstahl durch eigene Mitarbeitende, Anbahnung, d. h. die vorgängige direkte Kontaktaufnahme zu (ehemaligen) Mitarbeitenden sowie Kontaktaufnahme zu (ehemaligen) Mitarbeitenden über soziale Medien) (vgl. Abbildung 2).

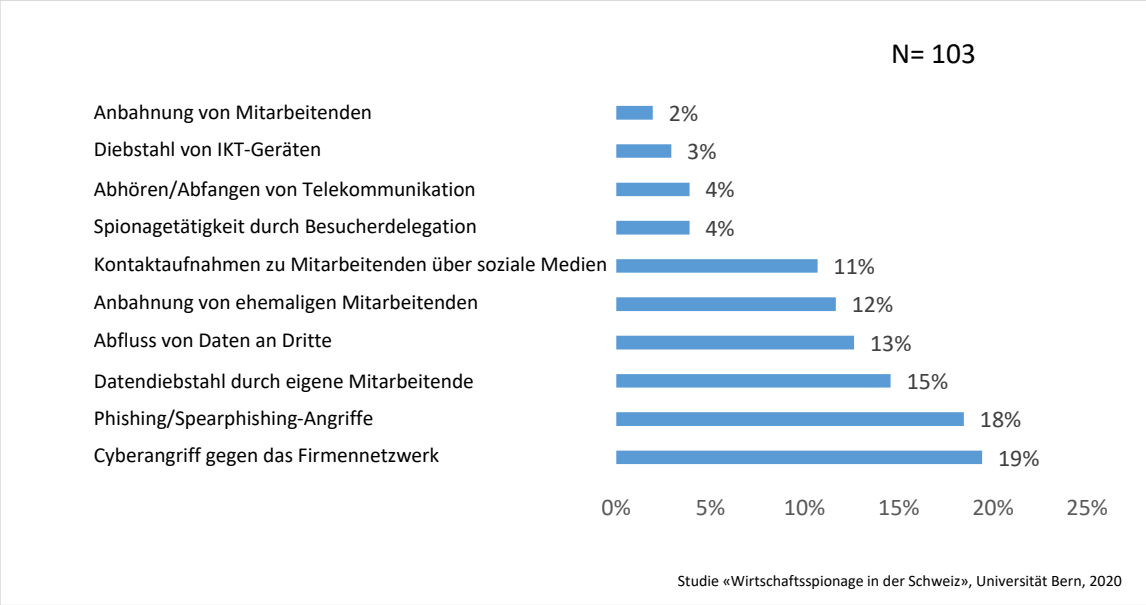

Abbildung 2: Angriffsmethoden von Spionageangriffen (Mehrfachantworten)

Erkannt wurden die Angriffe überwiegend durch Hinweise von Mitarbeitenden oder von externen Firmen wie Kunden, Lieferanten oder externen Dienstleistern (vgl. Abbildung 3).

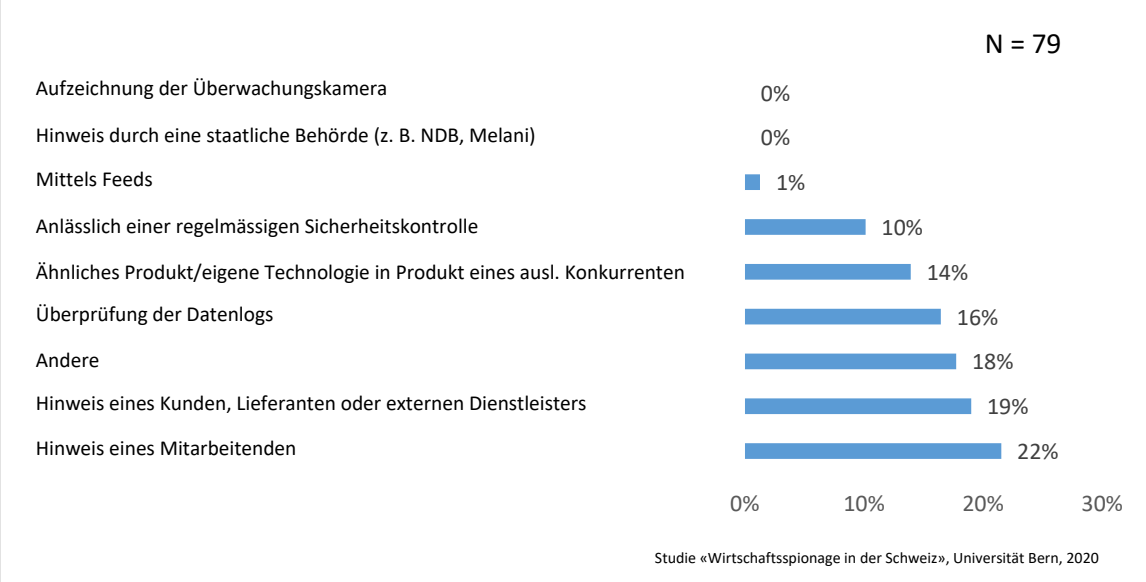

Abbildung 3: Erkennung von Spionageangriffen (Mehrfachantworten)

Die in den Einzelinterviews der Teilstudie 1 (qualitative Befragung) erwähnten Fälle von Wirtschaftsspionage erfolgten mittels folgender Methoden: Kopieren/Nachkonstruieren (wurde 4-mal genannt), Hacking (3-mal), MitarbeiterIn verwendete Informationen für eigene Zwecke (2-mal), MitarbeiterIn gab Informationen an Dritte (ausländische Konkurrenz) weiter (2-mal), PraktikantIn wurde in Firma eingeschleust (1-mal), Advanced Persistant Threat (APT) (1-mal), Einbruchdiebstahl (1-mal) und Social Engineering (1-mal). Eine der betroffenen Firmen wollte keine Angaben zur Angriffsmethode machen.

In den Gesprächen wurde auf insgesamt 104 Attacken hingewiesen. Diese fallen grösstenteils in die Kategorie Cyberangriffe (inkl. Hacking, Malware, Ransomware, Phishing), gefolgt von Kopieren bzw. Rekonstruieren von Produkten oder Daten. An dritter Stelle stehen Betrug (inkl. CEO-Fraud oder gefälschte Lieferantenrechnungen) sowie Attacken, die von Mitarbeitenden verübt wurden. Dazu zählen die Entwendung von firmeninternen Daten für eigene Zwecke (z. B. am neuen Arbeitsort) oder deren unerlaubte Weitergabe bzw. Veröffentlichung (etwa auf sozialen Netzwerken).

> Wir hatten einen Vorfall im August, da ging es um einen Wire-Fraud oder CEO-Fraud. Dabei hat ein Lieferant von uns eine Mail geschickt: Achtung Konto, wir haben da eine Anpassung. Die Bank hat gewechselt, bitte zahlen Sie das Geld dort hin. Das fanden wir seltsam und haben versucht mit dem Lieferanten Kontakt aufzunehmen. Er hat dann immer per Mail geschrieben, wir sollen jetzt das machen und wir würden ihn in den Ruin treiben, er brauche das Geld, so dass [unsere Firma] dann die Kontoanpassung gemacht hat und wir das Geld nach Hong Kong geschickt haben, anstatt in die USA. Daraufhin ist es wieder zurückgekommen, es sei irgendwie falsch, wir müssten es an einen anderen Ort schicken, dann ging schon mal eine Portion weg an US-Dollar. Drei Monate später ist wieder eine Rechnung gekommen, alles legitim, weil wir ja das Produkt erhalten haben, das Material, und dann ist der gleiche Betrag nochmals ausbezahlt worden. Bis das dann aufgeflogen ist. (Grossunternehmen, 4.2.2019)

2.3.2 Von Spionage betroffene Bereiche

Aus der Onlinebefragung (Teilstudie 2) geht weiter hervor, dass der Bereich ITK-Administration/ITK-Service am stärksten von Wirtschaftsspionage betroffen ist. Die Bereiche Fertigung/Produktion sowie Forschung & Entwicklung melden ebenfalls häufig Spionagefälle. Gar nicht betroffen von Attacken sind die Bereiche Mergers und Akquisition sowie Ausbildung (vgl. Abbildung 4).

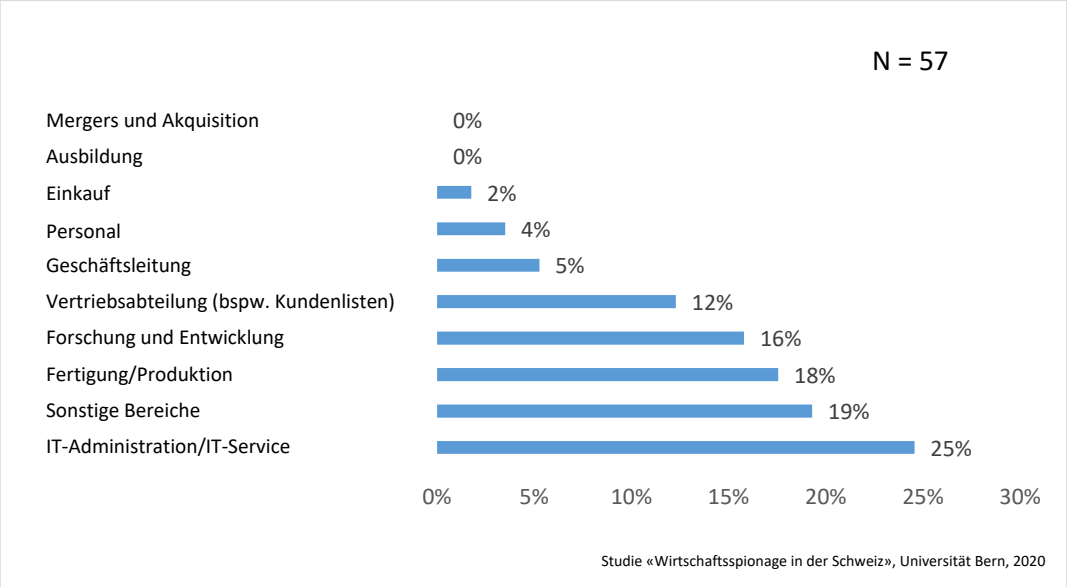

Abbildung 4: Von Spionage betroffene Bereiche

2.3.3 Täterschaft

In der quantitativen Befragung (Teilstudie 2) haben 72 Personen die Fragen zur Täterschaft beantwortet. In 37.5% der vermuteten oder bemerkten Fälle von Wirtschaftsspionage konnte die Täterschaft nicht identifiziert werden. In über 40% der Angriffe, also bei knapp der Hälfte der entdeckten Fälle, waren ehemalige (25%) oder aktuelle Mitarbeitende (16.7%) des Unternehmens involviert. Ein Konkurrent aus dem Ausland war in knapp 10% der Spionagefälle der Ursprung des Angriffs. Kunden, Lieferanten, Dienstleister/Berater oder ausländische Regierungsbehörden wurden weniger häufig als Täter genannt (vgl. Abbildung 5).

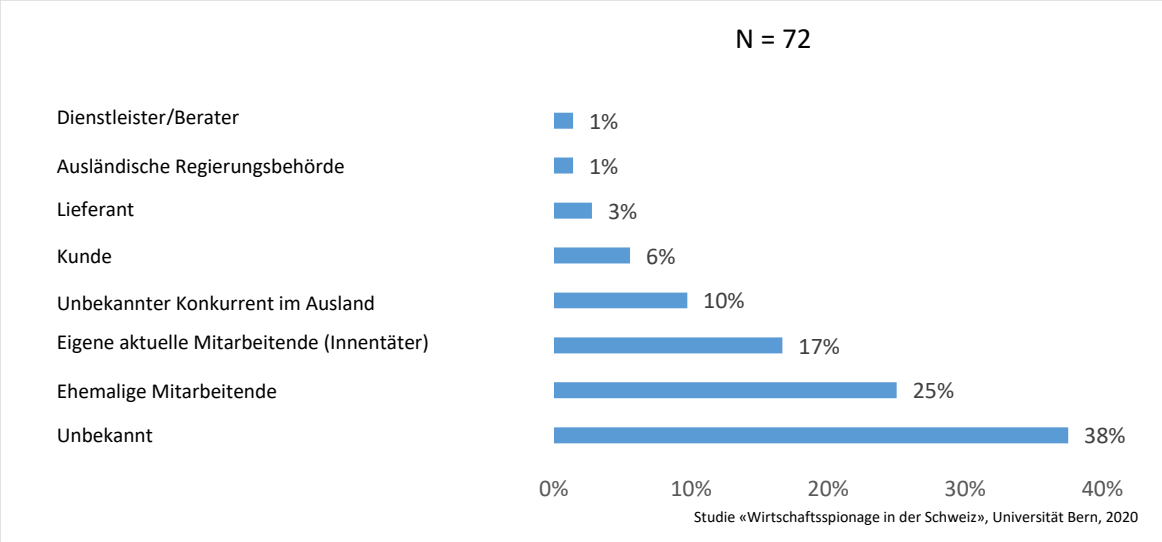

Abbildung 5: Übersicht Täterschaft (Mehrfachantworten)

In 66% der Fälle konnte die Nationalität der TäterInnen nicht identifiziert werden. Die identifizierten TäterInnen stammten zum grossen Teil aus der Schweiz (50%) und aus folgenden Ländern: Deutschland (20%), China (10%), Italien (5%), Ex-Jugoslawien (5%), Russland (5%) und England (5%).
Auch bei der qualitativen Befragung (Teilstudie 1) wurden Mitarbeitende (aktuelle wie auch ehemalige) als TäterInnen von Wirtschaftsspionage genannt. Diese handelten entweder in Eigenregie oder in Zusammenarbeit mit einem Konkurrenten des Unternehmens. Bei den TäterInnen handelt es sich also oft um einen Zusammenschluss von mehreren AkteurInnen:

> Jetzt haben wir ein paar Fälle, wo Mitarbeiter mit der Konkurrenz zusammengearbeitet haben. Auf den ersten Blick sieht man den Zusammenhang nicht, auf den zweiten merkt man, dass dahinter bspw. der Ehepartner einer Mitarbeiterin steckt, der dann die Aufträge mit unserem Know-how bekommt. (Grossunternehmen, 16.1.2019)

Weitere AkteurInnen, die in den Interviews genannt wurden, sind ausländische Konkurrenten und in einem Fall auch ein ausländischer Nachrichtendienst. Unter den ausländischen TäterInnen wurden hier, vergleichbar zur Onlinebefragung, vor allem die Nationalitäten China und Russland und vereinzelt weitere Länder aus (Süd-)Ostasien sowie des Nahen Ostens genannt.

In vielen Fällen – vor allem wenn die Firma durch Cyberattacken ausspioniert wurde – konnte die Täterschaft nicht genauer eruiert werden.

2.3.4 Handhabung von Vorfällen im Unternehmen

Bei einem entdeckten oder vermuteten Spionageangriff wurden gemäss der quantitativen Befragung (Teilstudie 2) in 20% der Fälle firmeninterne Massnahmen ergriffen. Häufig (16%) ziehen Unternehmen in solchen Fällen auch externe Beratung und Unterstützung bei. Eine Anzeige bei der Polizei/Staatsanwaltschaft hat jedoch nur knapp jedes achte Unternehmen erstattet. Schliesslich wurde gut die Hälfte der Spionagefälle aufgrund eines internen Beschlusses explizit nicht angezeigt.

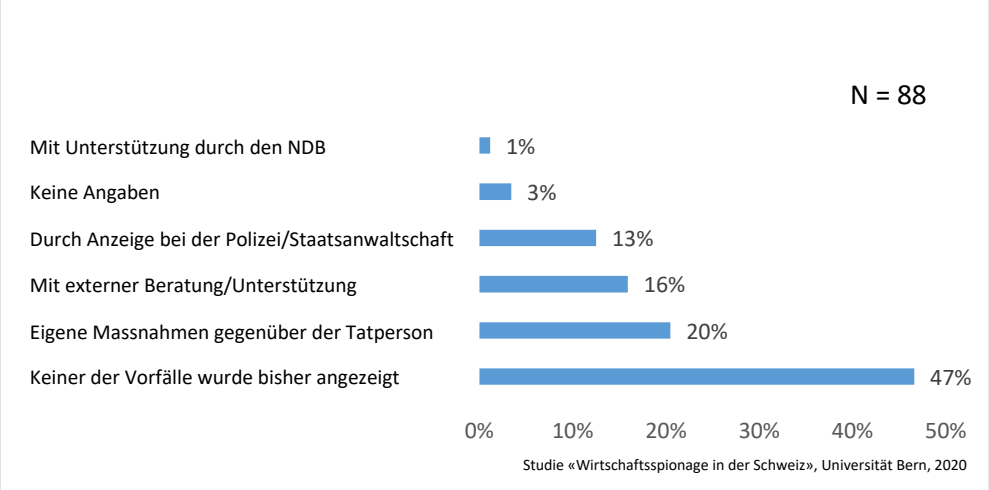

Abbildung 6: Handhabung Spionagevorfälle bzw. -verdachtsfälle im Unternehmen (Mehrfachantworten)

In der qualitativen Befragung (Teilstudie 1) gab die Mehrheit der 13 von Wirtschaftsspionage betroffenen Unternehmen an, den oder die Vorfälle einer Behörde gemeldet zu haben. Einige Unternehmen wandten sich an den NDB oder meldeten den Fall Melani, andere erstatteten Anzeige bei der Polizei oder der Staatsanwaltschaft. Firmen, die auf eine Meldung verzichteten, gaben als Begründung an, dass sie aus ihrer Sicht über zu wenig konkrete Anhaltspunkte verfügten oder der Vorfall sich an einem Standort im Ausland ereignet habe. In einigen Firmen führten erfolgte oder vermutete Spionagefälle zu Investitionen im Bereich Informatik- und Kommunikationssicherheit und/oder zur Sensibilisierung der Mitarbeitenden.

2.3.5 Schaden

Weiter ist die Frage des Schadens zentral. Ein Unternehmen, das von Wirtschaftsspionage betroffen ist, kann direkte finanzielle (materielle) Schäden und indirekte Auswirkungen (immaterielle Schäden) erleiden. In der quantitativen Befragung (Teilstudie 2) stellt der Verlust von Wettbewerbsvorteilen den am häufigsten genannten immateriellen Schaden dar, gefolgt vom Ausfall der Informatik sowie von Kunden- und Auftragsverlusten. Reputationsverluste oder negative Presse sowie Kosten für Rechtsstreitigkeiten werden ebenfalls oft genannt. Ein Teil der befragten Unternehmen gab aber auch an, dass durch den Spionageangriff kein Schaden bzw. kein messbarer Schaden entstanden sei (vgl. Abbildung 7).

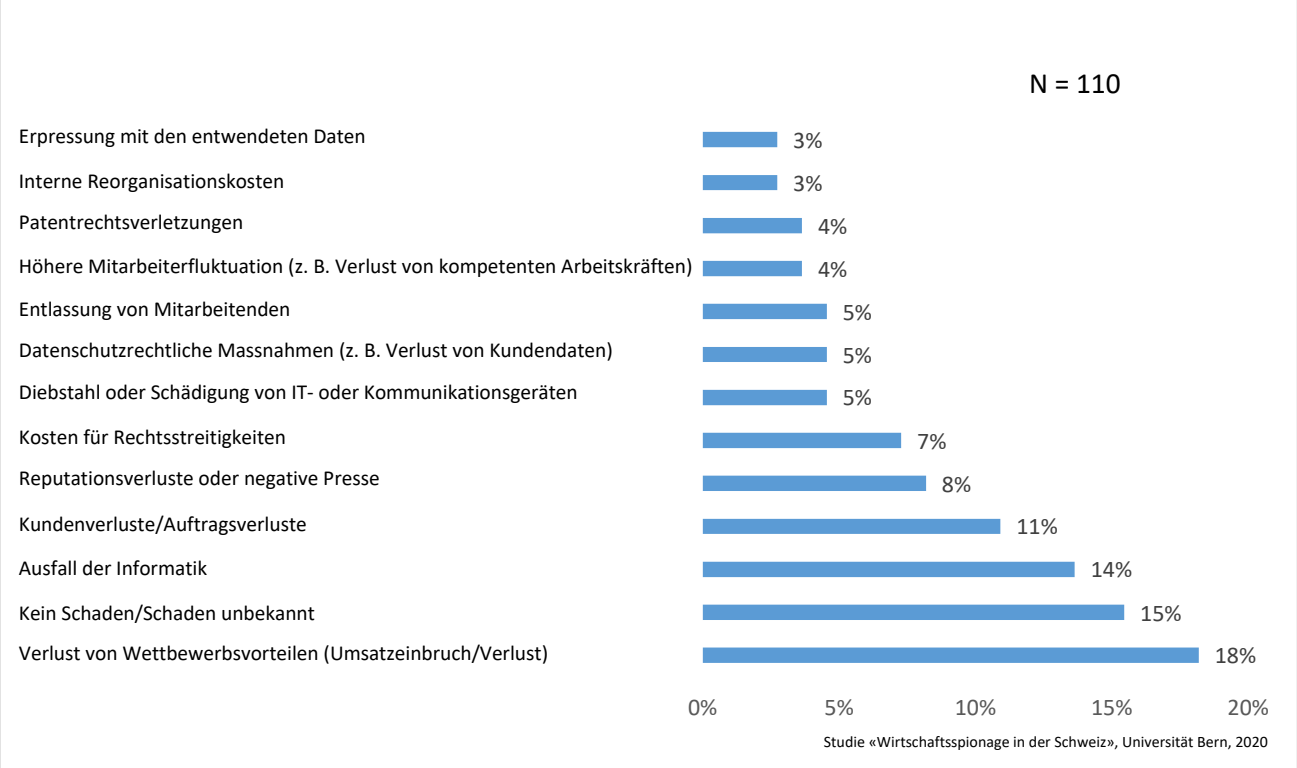

Abbildung 7: Schaden (Mehrfachantworten)

11% der von Wirtschaftsspionage betroffenen Unternehmen gaben an, dass die Existenz des Unternehmens aufgrund der Attacke in Gefahr war (Abbildung 8). Bei 30% der Firmen führte die Attacke zu Einschränkungen von mehr als 48 Stunden. Insbesondere die Gefährdung der Existenz des Unternehmens in 11% der Fälle verweist auf die potenziell gravierenden Folgen von Wirtschaftsspionage.

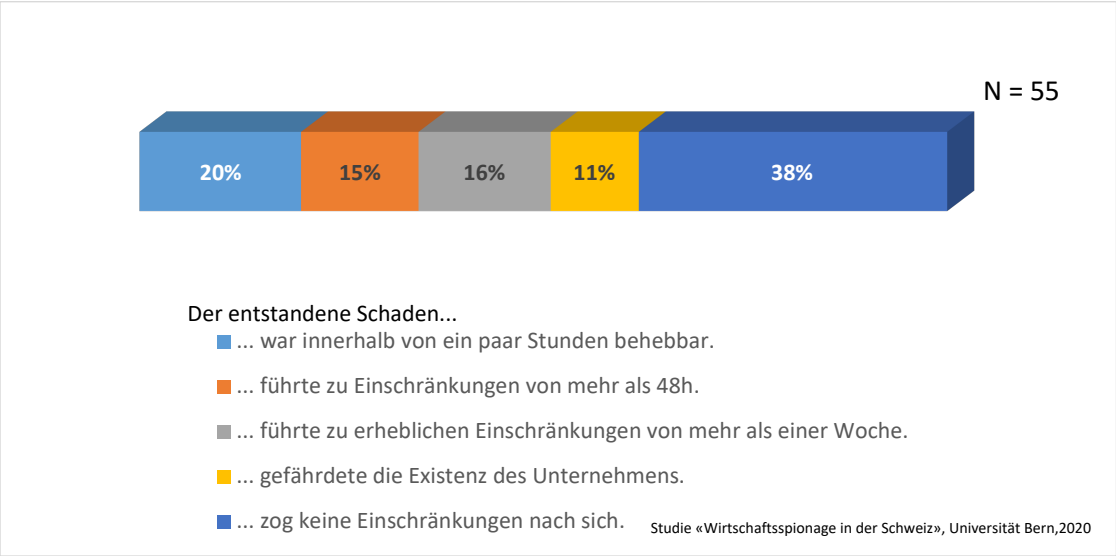

Abbildung 8: Konsequenzen des entstandenen Schadens

Aus der Abbildung 9 ist zu entnehmen, dass die genannten materiellen Schäden nur schwer zu beziffern sind. 24% der Unternehmen können dies nicht. Für 24% liegt die Schadenssumme zwischen 1 CHF und 10'000 CHF. In 9% der Fälle wird die Schadenssumme auf über 1'000'000 CHF geschätzt.

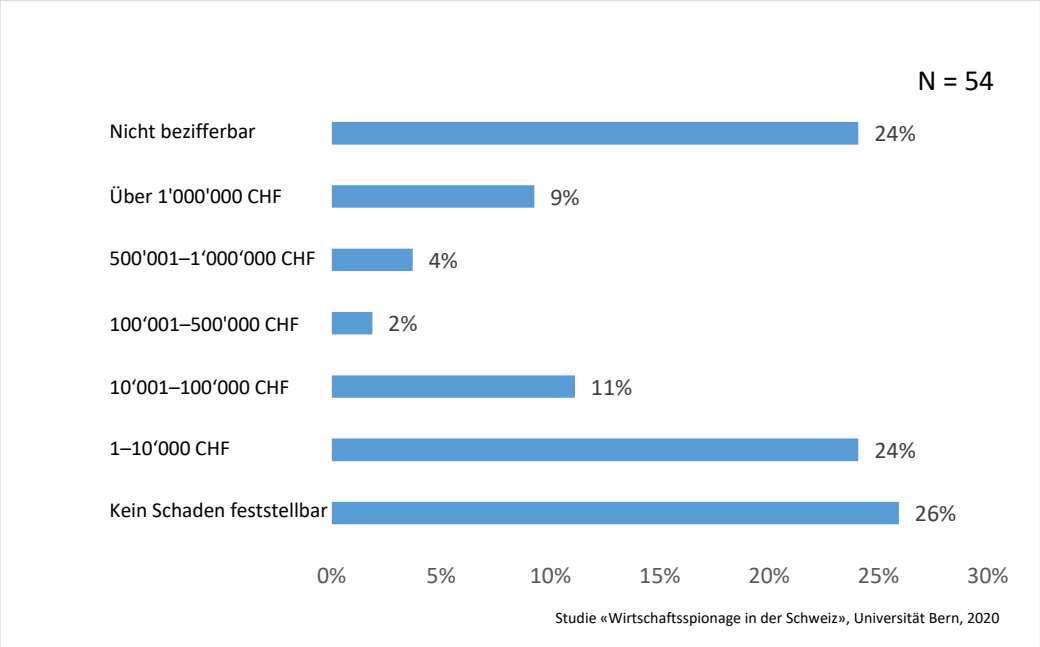

Abbildung 9: Schadenssumme

In den Einzelinterviews (Teilstudie 1) nannten die FirmenvertreterInnen vor allem finanzielle Schäden und den verursachten zusätzlichen Arbeitsaufwand (z. B., um das Informatiksystem neu aufzusetzen oder Abklärungen zu tätigen). In knapp einem Drittel der Fälle wurde entweder kein erkennbarer oder nur ein geringer Schaden festgestellt.

Nebst dem konkret entstandenen bzw. festgestellten Schaden wurde in den Interviews auch nach dem möglichen Schaden gefragt, der durch erfolgreiche Wirtschaftsspionage für die einzelnen Firmen entstehen könnte. Diesbezüglich fürchten sich sowohl KMU als auch Grossunternehmen am häufigsten vor einem Reputationsverlust der Firma sowie vor einem Verlust von Kunden bzw. Aufträgen.

> Es sind patentierte Technologien, der unmittelbare Schaden wäre nicht gross. Aber der Reputationsschaden wäre [für unsere Firma] langfristig das Schlimmste. Es ist ja nicht nur der Deal, den sie abschliessen, sondern auch ein Vertrag, der viel umfangreicher ist. Wenn man da ein Leck hat, spricht sich das herum und die Kunden sind weg. (KMU, 12.12.2018)

3. Präventionsmassnahmen in Unternehmen

Wie oben aufgezeigt, sind nicht nur Grossunternehmen, sondern auch KMU und Wissenschaftsinstitutionen von Wirtschaftsspionage betroffen. Gerade KMU scheinen sich des Werts ihres Wissens und Know-hows oft nicht bewusst zu sein (siehe Bollhöfer & Jäger 2018; Körmer & Langer 2015). Hinzu kommt, dass es vielen Unternehmen an Wissen, entsprechenden Massnahmen und Ressourcen mangelt, um erfolgreich Spionage abzuwehren (siehe Kaspar 2014: 40). Daher liegt in diesem Kapitel der Fokus auf den von den Firmen getroffenen Präventionsmassnahmen.

3.1 Das Wichtigste in Kürze

- Die Unternehmen ziehen firmeninterne Präventionsmassnahmen gegenüber den Angeboten von externen Dienstleistern und staatlichen Akteuren vor.
- Die von den Firmen getroffenen Massnahmen lassen sich unterteilen in: 1) strukturelle/organisatorische Massnahmen (z. B. ein umfangreiches Sicherheitskonzept oder eine interne, gut ausgestattete IT-Abteilung), 2) personelle Massnahmen (z. B. Sensibilisierung der Mitarbeitenden), 3) konkrete ITK-Massnahmen wie Instrumente oder Technologien, 4) physische/technische Massnahmen zum Schutz des Firmenareals, der Gebäudehülle und Innenräume sowie 5) konkreter Schutz von Produkten und Know-how (z. B. durch Patentierung).
- Die Regelung und Einschränkung der Zugriffsrechte der Mitarbeitenden auf Dokumente und Daten wird als wirksamste Massnahme wahrgenommen. In der qualitativen Studie wurden diesbezüglich sowohl Massnahmen im Bereich Zugriffrechte als auch die Sensibilisierung/Schulung von Mitarbeitenden am häufigsten genannt.

3.2 Firmeninterne Prävention, externe Dienstleister und staatliche Massnahmen

In der Onlinebefragung wurden die VertreterInnen der Firmen gefragt, von wem sie in Fällen von Spionage am ehesten Unterstützung erfragen würden. Sie konnten insgesamt 100% auf die drei Möglichkeiten interne Unterstützung, Unterstützung durch externe Akteure oder Unterstützung

durch staatliche Stellen aufteilen. Zum besseren Verständnis zeigt die Grafik (vgl. Abbildung 10), wie stark die jeweilige Möglichkeit in Anspruch genommen wird: wenig (0–25%), eher wenig (26–50%), eher stark (51–75%) oder stark (76–100%). Die Daten zeigen, dass sich ein Grossteil der Firmen vor allem auf interne Lösungen abstützt. Nur auf externe oder staatliche Unterstützung verlassen sich sehr wenige Unternehmen. Einige Firmen verbinden auch interne Lösungen mit Unterstützung durch externe Anbieter und staatliche Stellen. Der geringe Rückgriff auf staatliche Stellen und externe Anbieter zeigt, wie oft Fragen von Spionage intern behandelt werden. Ob dies mit einer Angst vor einem Reputationsverlust, mangelndem Wissen über externe und staatliche Unterstützungsmöglichkeiten oder anderen Gründen zusammenhängt, sagen die Daten nicht aus.

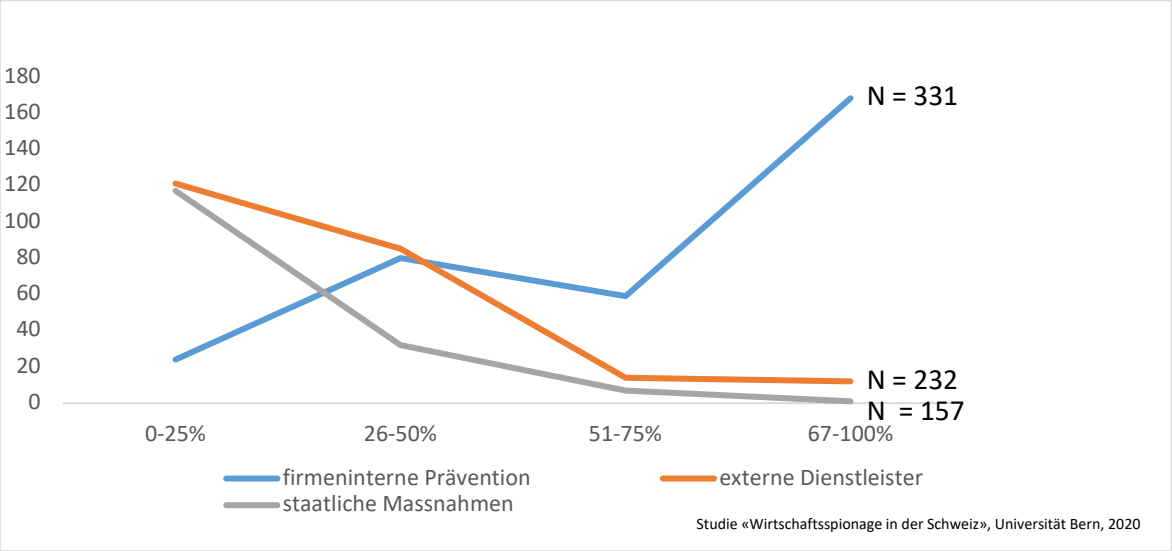

Abbildung 10: Schutzmassnahmen

3.3 Schutz unternehmenseigener Informationen und Daten

Als geeignete Massnahme zur Vermeidung eines Angriffs wird in der Onlinebefragung (Teilstudie 2) am häufigsten die Regelung und Einschränkung der Zugriffsrechte der Mitarbeitenden auf Dokumente und Daten genannt (12%). Die sichere Vernichtung vertraulicher Akten und Datenträger gehört ebenso zu den Top-5-Nennungen (8%) wie die Klassifizierung von Dokumenten und Daten

(7%), die Regelung und Einschränkung der Zutrittsrechte der Mitarbeitenden zu verschiedenen Firmenbereichen (7%) und Geheimhaltungsverpflichtungen für Mitarbeitende und Geschäftspartner (7%).

In den Interviews mit VertreterInnen von Unternehmen (Teilstudie 1) wurden die Fragen nach firmeninternen Präventionsmassnahmen zur Verhinderung von Wirtschaftsspionage in folgende Bereiche unterteilt: 1) strukturelle/organisatorische Massnahmen; 2) personelle Massnahmen; 3) konkrete ITK-Massnahmen wie Instrumente und Technologien; 4) physische/technische Massnahmen; und 5) konkreter Schutz von Produkten und Know-how. Wie sich in den Gesprächen herausstellte, werden diese Massnahmen in erster Linie getroffen, um allgemein ungewolltes bzw. illegales Abschöpfen vertraulicher Unternehmensdaten zu verhindern. Die von den Firmen erwähnten Massnahmen richten sich deshalb sowohl gegen Industrie- als auch gegen Wirtschaftsspionage.

Zu den **strukturellen/organisatorischen Massnahmen** zählen u. a. umfangreiche Sicherheitskonzepte (Spionageabwehr ist ein Teil davon). Insbesondere Grossunternehmen verfügen über solche Konzepte. Als eine weitere, auf organisatorischer Ebene anzusiedelnde Schutzmassnahme wurde in den Interviews die eigene, gut ausgestattete IT-Abteilung genannt. Über diese Massnahme verfügen fast ausschliesslich Grossunternehmen. Einige Firmen führen auch *penetration tests* und Risikoanalysen durch.

> Wir pflegen eine vier-Säulen-Strategie: 1. Prediction: Was passiert auf dem Markt, bei anderen Firmen und beim NDB? Gibt es vorhandene Cyberattacken? Vernetzt entscheiden wir, was ggf. für [unsere Firma] zu tun ist. 2. Prevention – was technische Abwehr wie Virenschutz etc. sowie auch Mitarbeiter-Awareness bedeutet, und 3. Detection: dies haben wir seit drei Jahren, dabei geht es z. B. darum, Malware frühzeitig zu entdecken. Die Gateways und Firewalls geben zudem an, welche Geräte auf Botnetzwerke zugreifen möchten, wobei der Zugriff aber gesperrt ist. Dann haben wir ein Virenbewertungssystem. Gibt dieses Alarm, so kann ein Security-Mitarbeiter diesem Vorfall nachgehen. Detection hängt auch stark mit 4. Reaction zusammen. Wir reagieren grundsätzlich auf solche Security Alarme aber auch on demand, also wenn etwas passiert ist, was nicht mit den Security Tools erkennbar war. (Grossunternehmen, 16.1.2019)

Hinsichtlich **personeller Massnahmen** gaben fast alle Unternehmen an, dass sie ihre Mitarbeitenden in vielerlei Hinsicht sensibilisieren. Die Massnahmen reichen von eher informellen, mündlichen Informationen, z. B. über Phishing-Mails, hin zu regelmässig stattfindenden Schulungen und Sensibilisierungskampagnen, teilweise auch in Zusammenarbeit mit dem NDB. Wie in Kapitel 4 erläutert

wird, sind sich viele der von uns interviewten Personen des Risikos bewusst, das von Mitarbeitenden ausgeht. Einige Firmen nannten in diesem Zusammenhang auch die Bedeutung der internen «Organisationskultur» (z. B. wertschätzende, offene Kommunikation) und der Arbeitsbedingungen (z. B. gute Entlöhnung, Selbstbestimmung etc.).

> Den wichtigsten Schutz, den wir haben, was ich in der Vergangenheit auch schon positiv erlebt habe, ist, dass wir eine wirklich sehr offene Beziehung haben, bis zum Firmenbesitzer. Das ist eigentlich ein sehr offenes Verhältnis, selbst wenn der einfachste Mitarbeiter aus der Produktion von der Spätschicht mal kommt und beim Chef anklopft, ist man sehr offen und hört zu, damit wenn sich der Druck aufbaut, die Mitarbeiter auch grad eine Ansprechstelle haben. Das Schlimme ist, wenn sich für den Mitarbeiter Druck aufbaut und er das Gefühl hat, er dürfe es niemandem erzählen und dann geht das Spiel immer weiter. Wir versuchen tolerant gegenüber Fehlern zu sein, nicht dass man zu repressiv ist. (KMU, 22.1.2019)

Ein Drittel der interviewten Firmen will genau wissen, wer sich bei ihnen um eine Stelle bewirbt. Daher nehmen sie bei der Rekrutierung von neuen Mitarbeitenden so genannte «Backgroundchecks» vor und verlangen von BewerberInnen bspw. einen Auszug aus dem Strafregister. Weiter sind sie wachsam bei gewissen Nationalitäten oder sammeln personenbezogene Informationen via Google und soziale Netzwerke. Ein kleiner Teil dieser Firmen führt bei einigen BewerberInnen zudem Personensicherheitsprüfungen (PSP) des VBS durch. Weitere Massnahmen im Personalwesen der befragten Firmen sind vertraglich festgehaltene *Codes of Conduct*. Darin enthalten sind Regeln bspw. in Bezug auf die Nutzung von *Social Media* oder dem Annehmen von Geschenken, firmeninterne Zugriffsbeschränkungen (siehe auch IT-Massnahmen weiter unten) und bewusstes Wissensmanagement (d. h. der Zugang zu sensiblem firmeninternem Wissen wird nur restriktiv gewährt). Knapp ein Viertel der Firmen gab an, auf der Ebene der Mitarbeitenden keine speziellen Vorkehrungen zur Verhinderung von Wirtschafts- bzw. Industriespionage zu treffen.

Zu den **IKT-Massnahmen** zählen u. a. Massnahmen bezüglich *Datenschutz/Datensicherheit*. Darunter verstehen wir Massnahmen, die sich auf Zugriffsmöglichkeiten und die Verfügbarkeit von Daten beziehen. Die Mehrheit der befragten Unternehmen verfügt über ein nach Funktion und Verantwortungsbereich differenziertes Zugriffsrechtsystem, wodurch u. a. der Zugriff auf sensible Daten beschränkt wird. Die Firmen sind ausserdem mit Firewalls, Spamfiltern und Virenschutzsoftware ausgestattet. Für die Ablage sensibler Daten verwenden gewisse Firmen interne, separate Server, die speziell geschützt und teilweise nicht mit dem Internet verbunden sind, sowie externe Backup-

Lösungen. Uneinig sind sich die Interviewten in diesem Zusammenhang in Bezug auf die Nutzung von Clouds. Während die einen bei der Ablage von sensiblen Daten ausschliesslich auf virtuelle Lösungen setzen, speichern andere diese ausschliesslich auf einem physisch vorhandenen (bzw. für sie zugänglichen und kontrollierbaren) Server. Ebenfalls zu den IKT-Massnahmen zählen Massnahmen im Bereich Elektronische Kommunikation/Datenaustausch. In diesem Bereich werden deutlich weniger Massnahmen getroffen als im Bereich Datenschutz/Datensicherheit. Eine Verschlüsselung des E-Mail-Verkehrs, der Festnetz- und mobilen Anrufe wird nur von einem kleinen Teil der interviewten Firmen vorgenommen. Noch weniger gaben an, den Datenverkehr zu überwachen bzw. zu kontrollieren. Das Fehlen von Massnahmen in diesem Bereich erklärten die Interviewten mit den nicht vorhandenen Ressourcen (betrifft vor allem KMU) oder der aus ihrer Sicht nicht vorhandenen Notwendigkeit. Das Risiko, das mit dem Verschicken sensibler Daten über den offenen E-Mail-Verkehr verbunden ist, wird oft unterschätzt.

> Also mit unseren Klienten kommunizieren wir natürlich [via E-Mail], wir schicken ihnen bspw. Offerten, Instruktionen, um bei Problemen zu helfen. Dabei sind wir nicht sonderlich vorsichtig. Natürlich gehen wir davon aus, dass die Informationen nicht gerade bei der Konkurrenz landen. Aber wir haben keine Vorsichtsmassnahmen dafür getroffen. (KMU, 13.3.2019)

Schliesslich werden im Bereich IKT auch Sicherheitsvorkehrungen im Umgang mit der IT-Hardware getroffen. Diese sind allerdings bei den von uns interviewten Firmen insgesamt eher spärlich vorhanden. Wie aus den Interviews hervorgeht, sind die Firmen am stärksten für die Risiken im Zusammenhang mit der Nutzung von Laptops sensibilisiert, insbesondere auf Auslandreisen. Wie bereits in Kapitel 2.2 erwähnt, verlangen einige Firmen von ihren Mitarbeitenden, dass sie nur mit firmeneigenen Laptops unterwegs sind, auf denen zudem keine sensiblen Daten gespeichert werden. Die Mitarbeitenden werden auch aufgefordert, sich nicht in öffentliche WLANs einzuloggen sowie den Laptop und das Mobiltelefon unterwegs auszuschalten. Weiter sind einige Firmen zurückhaltend in der Zulassung bzw. Nutzung von USB-Speichersticks. Einige Firmen erlauben nur die Nutzung verschlüsselter Sticks oder verbieten es ihren Mitarbeitenden, sensible Daten darauf abzuspeichern. Andere haben deren Nutzung gänzlich verboten oder die USB-Anschlüsse blockiert.

Zu den **physischen/technischen Massnahmen** zählen wir Massnahmen zum Schutz des Firmenareals, der Gebäudehülle sowie der Innenräume. Mehr als die Hälfte der interviewten FirmenvertreterInnen gab an, dass ihre Firma über ein Zutrittssystem verfügt. Das Personal hat bspw. nur via Badge Zutritt und firmenexterne Personen wie Lieferanten oder BesucherInnen (siehe Kapitel 2.2) müssen sich vorgängig anmelden und beim Empfang ausweisen. Einige Firmen, primär Grossunternehmen, schützen ihr Areal zusätzlich mit Zäunen, Kameras, Alarmanlagen und durch Einsatz von Sicherheitspersonal. Zudem gaben einige Firmen an, dass gewisse Innenbereiche speziell gesichert werden, insbesondere die Serverräume.

In den Einzelinterviews wurden auch Massnahmen erwähnt, die zum Schutz von **Produkten** und **Know-how** getroffen werden. Gewisse FirmenvertreterInnen nannten in diesem Zusammenhang die Patentierung ihrer Produkte. Immer wieder wird die Erfahrung gemacht, dass der Patentschutz nicht in allen Ländern – allen voran China – gleichermassen funktioniert bzw. respektiert wird und patentierte Produkte kopiert oder rekonstruiert werden. Manche Unternehmen verzichten deshalb bewusst darauf. Dies nicht zuletzt aufgrund der Tatsache, dass durch die Patentierung der Produktionshergang offengelegt wird:

> Wir haben ein Produkt gemacht mit dem höchsten Wirkungsgrad, wenn man dies aufmacht, muss man sehr gut schauen, wenn man dies kopieren will, sieht man das gar nicht. Aber ich bin mir sicher, in China wurde dies gekauft und geöffnet. Das sage ich aus Erfahrung mit der Patentierung. Deshalb frage ich mich, was ist besser: Patent machen oder nicht. Denn ein Patent ist wie ein Kochbuch. Und dies zu respektieren braucht Grundwerte. Es wird vielleicht aber trotzdem kopiert, deswegen sollte man das Kochbuch vielleicht schon gar nicht erst machen lassen. Deswegen haben wir auch angefangen, gewisse Sachen gar nicht erst patentieren zu lassen. Das andere ist: wie verfolgt man dies? Und wenn das Produkt ein [klein wenig] verändert wurde: ist es dann immer noch unter dem Patent? Wenn man nicht bereit ist, ein Legal Departement zu haben, das dem nachgeht ... es ist nicht einfach. [Unsere Firma] hat einen Haufen Patente, aber mir ist nicht bekannt, dass man deswegen mal in einem Rechtsstreit war. (KMU, 21.1.2019)

Weitere Massnahmen, um Produkte und Know-how zu schützen, sind eine kontrollierte Herausgabe von (teilweise bewusst lückenhaften) Plänen und Zeichnungen sowie Prototypen (bspw. an potenzielle Kunden), damit nicht im Detail verstanden werden kann, was die Firma herstellt. Während einige Firmen ihre Daten und Dokumente klassifizieren, erwähnte eine Person, dass in ihrer

Firma bewusst darauf verzichtet wird, da klassifizierte Dokumente automatisch als «interessant» gekennzeichnet werden:

> Es gab auch Bemühungen, klassifizierte Infos vom Rest zu trennen. Meine persönliche Einstellung dazu ist, dass es nicht sinnvoll ist, weil man die Information so als interessant markiert. In dem Zustand wie es jetzt ist, bleibt sie in einem Haufen von Daten versteckt und ist damit schwer zu finden. (Grossunternehmen, 11.1.2019)

Einzelne Firmen stellen zudem bewusst falsche Pläne her oder handeln Produkte unter einem anderen Namen.

4. Herausforderungen und zukünftige Entwicklungen aus Sicht der Unternehmen

4.1 Das Wichtigste in Kürze

- Die Digitalisierung wird als grosse technische und organisatorische Herausforderung gesehen.
- Weiter sehen Firmen auch Herausforderungen im Zusammenhang mit unzufriedenen oder unvorsichtigen Mitarbeitenden.
- Eine weitere Herausforderung stellt die zunehmende Globalisierung dar und die dadurch verstärkte globale Verknüpfung von betrieblichen Prozessen. Probleme können sich in diesem Zusammenhang mit länderspezifischen, von der Schweiz abweichenden Rahmenbedingungen (z. B. bezüglich geistigen Eigentums) oder bei der sicheren Rekrutierung von Personal ergeben.

4.2 Technischer Fortschritt, Mitarbeitende, länderspezifische Merkmale, Erkennung von Vorfällen, globale Vernetzung

In den Einzelgesprächen (Teilstudie 1) wurde auch nach Herausforderungen und künftigen Entwicklungen im Zusammenhang mit Wirtschaftsspionage gefragt. Die Antworten der FirmenvertreterInnen lassen sich grob in vier Kategorien unterteilen: 1) Technischer Fortschritt, 2) das Risiko, das von Mitarbeitenden ausgeht, 3) länderspezifische politische, rechtliche und kulturelle Rahmenbedingungen, 4) das Erkennen von Vorfällen sowie 5) die globale Vernetzung. Diese werden im Folgenden genauer erläutert.

Im Zusammengang mit dem **technischen Fortschritt** wurde am häufigsten die Digitalisierung als Herausforderung genannt – sowohl hinsichtlich der daraus resultierenden Vorteile (z. B. betreffend Kommunikation, Vernetzung) als auch des Risikopotenzials (z. B. bezüglich Datensicherheit). Unsere InterviewpartnerInnen gehen davon aus, dass durch die Digitalisierung auch die Spionagemöglichkeiten stets umfangreicher und technisch einfacher werden:

> Es ist inzwischen so einfach machbar […] das flächendeckende Abscannen von Sachen das läuft, und da bin ich sicher, weil es automatisiert ist und jeder kann es. […] Dann gibt es weitere Stufen, wo man vielleicht gezielt versucht via Mails anzugreifen und wenn es immer noch interessant ist, dann macht man vielleicht dritte, vierte Stufe. Aber das ist sicher ein grosses Thema. Weil es so einfach geworden ist, das ist das Problem. Die Eintrittsschwelle ist so niedrig. Und wenn man genügend Ressourcen hat, wie China, dann macht man das einfach. Da bin ich sicher, dass KMU völlig im Schilf stehen. (KMU, 15.1.2019)

Unvorsichtige oder frustrierte **Mitarbeitende** sowie Mitarbeitende, die zur Konkurrenz wechseln, wurden ebenfalls häufig als Herausforderung bzw. grosse Schwachstelle im Unternehmen bezeichnet. Weitere Herausforderungen ergeben sich für international tätige Firmen. In den Interviews wurde mehrmals auf teilweise stark vom Kontext der Schweiz abweichende **länderspezifische politische, rechtliche und kulturelle Rahmenbedingungen** hingewiesen, z. B. bezüglich des Schutzes von geistigem Eigentum:

> Die aufstrebenden Nationen wie China, die bedienen sich eigentlich ohne Hemmungen an Intellectual Property und setzen dafür alle Mittel ein. Und es sind nicht nur Firmen, sondern auch Länder, ganze Organisationen bis zu den Geheimdiensten, die da involviert sind, wenn man etwa auf Russland schaut. Da werden Angriffe gefahren, die ein Einzelner gar nicht mehr fahren kann. Da werden sehr viele Mittel und Kompetenzen reingesteckt, um an Wissen heran zu kommen. (Grossunternehmen, 4.2.2019)

> Die Regeln in China sind anders als in der Schweiz. Da darf man sich nichts vormachen. […] Klug und listig ist dasselbe, dann darf man sich auch nicht aufregen, wenn einer den anderen über den Tisch zieht, der gilt als schlau, das ist in ihrem Kulturkreis etwas Gutes und wird im Westen häufig nicht verstanden. Man muss sich dessen bewusst sein. (KMU, 21.1.2019)

Ein weiterer Punkt sind die länderspezifischen Sicherheitsstandards, welche insbesondere für Firmen relevant sind, die auf ausländische Lieferanten zurückgreifen:

> Bei strategischen Teilen will ich wissen, wer uns beliefert. Darum reise ich auch regelmässig, gehe zu strategischen Lieferanten. Z. B. Slowenien: Als ich erstmals dort war, das ist eine andere Welt, andere IT, dort kann man nichts erwarten punkto Sicherheit. Die haben Pläne und Zeichnungen von unseren Produkten, um Teile herzustellen. Frage ist immer, wie gross ist das Risiko, Kosten-Nutzen. Sollen wir in Deutschland einkaufen, wo wir mehr Sicherheit haben, aber mehr bezahlen? Es ist immer ein Abwägen. Was wir nicht machen: in China bestellen. (KMU, 14.12.2018)

Das **Erkennen von Vorfällen** und **Angriffsmustern** ist eine weitere Herausforderung. Dies betrifft sowohl die Risiken, die von Mitarbeitenden ausgehen als auch von Cyberangriffen. Besonders bei Letzteren findet ein Wissensabfluss oft unbemerkt statt und man hinkt den technischen Möglichkeiten stets hinterher.

Schliesslich wurde auch die **globale Vernetzung** als Herausforderung genannt, insbesondere im Zusammenhang mit dem globalen Austausch von Arbeitskräften sowie der Auslagerung der Produktion, die mit einem Know-how-Transfer einhergeht.

Weitere, vereinzelt genannte Herausforderungen betreffen KMU und deren (aufgrund fehlender Ressourcen) relativ geringes Schutzniveau. Eine weitere Herausforderung stellt die Schwierigkeit dar, eine Balance zwischen dem Installieren von (einschränkenden) Sicherheitsmassnahmen und dem Ermöglichen von effizientem Arbeiten zu finden.

5. Fazit und Entwicklungshinweise

5.1 Fazit

Zusammenfassend kann man festhalten, dass Wirtschaftsspionage in der Schweiz stattfindet und von den Unternehmen wahrgenommen und als Bedrohung eingeschätzt wird. Für die Behörden bleibt die Übersicht über die Fälle jedoch lückenhaft, da nur ein geringer Prozentsatz der Fälle gemeldet wird. Wie die Untersuchung zeigt, werden viele Fälle intern in der Firma ohne externe Unterstützung oder mit Unterstützung externer privater Anbieter bearbeitet. Wie hoch der Anteil an betroffenen Firmen tatsächlich ist, lässt sich ebenfalls nur schwer eruieren. Dies widerspiegelt sich auch in den unterschiedlichen relativen Anteilen betroffener Firmen in den beiden Teilstudien. In

den gefährdeten Branchen sind Firmen von Wirtschaftsspionage betroffen und es werden Fälle vermutet und auch entdeckt.

Welche Branchen sind gefährdet? Folgende Branchen sind von Wirtschaftsspionage stark gefährdet: Informatik und Telekommunikation, Life Science, Maschinenbau und Industrie sowie Pharma. In anderen Branchen finden sich zusätzlich Firmen, die ein Nischenprodukt oder ein speziell sicherheitsrelevantes Produkt herstellen, und dadurch zum Ziel von Wirtschaftsspionage werden können. Weiter kommen als potenziell gefährdete Branchen der Bankensektor, Versicherungen und Immobilien hinzu.

Welche typischen Angriffssituationen und -methoden gibt es? Typische Bedrohungssituationen charakterisieren sich durch Schwachstellen oder Öffnungen in der Abschirmung gegen aussen. Dazu zählen öffentliche Veranstaltungen wie Messen, BesucherInnen auf dem Firmengelände, Auslandreisen von Mitarbeitenden, Kommunikation zwischen Firmenstandorten, Austausch von Daten mit PartnerInnen oder KundInnen und die Lieferkette der Firma. Es zeichnen sich zwei Hauptangriffsmethoden ab: Cyberangriffe und Angriffe von aktuellen oder ehemaligen Mitarbeitenden. Daneben gibt es auch physische Angriffe wie Einbrüche. Auch in Zeiten der Digitalisierung und Automatisierung der Bearbeitung grosser Datenmengen ist der Faktor Mensch bei Spionagetätigkeiten nicht zu unterschätzen. Die Täterschaft lässt sich in den besprochenen Fällen nur zum Teil eruieren. Oft gingen die Firmen auch von einer Gruppe von TäterInnen aus (bspw. ausländische Firmen oder andere Staaten über einen Mitarbeitenden).

Wie hoch ist der Schaden? Ebenfalls schwierig zu beantworten ist die Frage nach dem Schaden, denn es lässt sich kein Vergleich zu einem Geschäftsgang ohne Spionagefall ziehen. Einfacher zu beziffern sind direkte Schäden wie ein Produktionsausfall, der Verlust eines Geschäfts oder ein Mehraufwand (z. B. bei der IT) für die Bekämpfung der Spionage usw. Schwierig in Zahlen zu fassen ist wiederum der längerfristige Reputationsschaden, der entstehen kann, wenn ein Fall publik wird. Ein Reputationsschaden zieht potenziell einen grossen materiellen Verlust nach sich, indem längerfristig Aufträge und Kundschaft verloren gehen. In unserer Umfrage erwähnten 11% der Firmen, die einen Spionagefall bemerkten, dass der Fall die Existenz der Firma gefährdet habe. Dies deutet auf die potenziell gravierende Auswirkung von Wirtschaftsspionage hin.

Wie schützen sich Firmen? Die befragten Firmen empfinden interne Prävention als deutlich wichtiger als die Unterstützung durch externe Spezialisten oder staatliche Stellen. Zur internen Prävention werden verschiedene Massnahmen ergriffen (strukturell und organisatorische Regelungen, Schulung und Sensibilisierung von Mitarbeitenden, ITK-Massnahmen sowie physische und technische Sicherung). Der Grad der Prävention ist jedoch sehr unterschiedlich und hängt stark von der Unternehmensgrösse und den vorhandenen Ressourcen für Spionageprävention ab. Insbesondere in KMU ist das Bewusstsein für Bedrohungen im Zusammenhang mit Datenaustausch und digitaler Kommunikation (v. a. E-Mails) oft relativ gering.

Welche Entwicklungen und Herausforderungen zeichnen sich ab? Die befragten Firmen weisen in Bezug auf zukünftige Entwicklungen spezifisch auf die Digitalisierung und Globalisierung hin. Mit der Digitalisierung steigen die Herausforderungen für Unternehmen, ihre Daten (bspw. Produktionsdaten, aber auch Kundendaten) in digitaler Form sicher zu bewirtschaften. Wenn heute bereits eine grosse Zahl der Angriffe über den digitalen Weg führt, so ist damit zu rechnen, dass dieser Angriffsweg in Zukunft an Bedeutung gewinnen wird. Die Globalisierung der Märkte sowie der Patentschutz auf internationaler Ebene stellen eine zusätzliche Herausforderung dar. Gleichzeitig werden auch Mitarbeitende, GeschäftspartnerInnen, Zulieferfirmen und KundInnen immer globaler, wodurch unterschiedliche nationale Gesetzeskontexte und Geschäftskulturen neue Fragen aufwerfen. Schliesslich wird auch die Herkunft der Mitarbeitenden globaler. Gewisse Firmen verfolgen die Strategie, primär Mitarbeitende mit persönlich bekannten Referenzen zu rekrutieren. Dieses Vorgehen lässt sich jedoch nur auf einen beschränkten Personenkreis anwenden. Fragen der Sicherheit bei der Neurekrutierung von Mitarbeitenden werden insbesondere für KMU damit an Bedeutung gewinnen.

Die Untersuchung zeigt, dass sich Firmen in der Schweiz der Bedrohung durch Wirtschaftsspionage zwar bewusst sind, aber sehr unterschiedlich in die Prävention investieren. Besonders betroffen sind KMU, die weniger Ressourcen in Administration und Sicherheit und mehr in Forschung und Produktion stecken. Die sich abzeichnenden Entwicklungen fordern sie daher besonders heraus. Da Prävention bis anhin vor allem firmenintern stattfindet, stellt sich die Frage, welche Rolle der Staat hier spielen soll und wie die breite Palette an bedrohten Firmen in der Schweiz unterstützt werden kann.

5.2 Entwicklungshinweise

- Sensibilisierung von Firmen

  Auch wenn die meisten Firmen mittlerweile für Risiken durch Wirtschaftsspionage sensibilisiert sind, ist das Ausmass und die konkrete Bedrohung nicht allen gleichermassen bewusst. Dies zeigt sich speziell im unterschiedlichen Grad der Präventionsmassnahmen im Bereich Kommunikation und Datensicherheit. Es braucht daher kontinuierliche und intensivere Bemühungen zur Sensibilisierung von Firmen.
- Bekanntheitsgrad des NDB und Rolle der Kantonspolizei

  Die staatlichen (nationalen und kantonalen) Stellen sind nur bei einem Teil der Firmen als Ansprechpartner bekannt, bei einer grossen Mehrheit dagegen sind diese Stellen weitgehend unbekannt. Klare Ansprechpartner, eine Hotline und eine noch aktivere Präsenz vor Ort in den Firmen und in den am stärksten betroffenen Wirtschaftsverbänden würden die staatlichen Stellen, deren Aufgaben und Dienstleistungen bekannter machen. Dies würde den Firmen einen niederschwelligen Zugang ermöglichen und die Wahrscheinlichkeit erhöhen, Firmen adäquat unterstützen zu können. Es sollte auch bedacht werden, dass viele von Wirtschaftsspionage betroffene Firmen aus Reputationsgründen vor einer Anzeige zurückschrecken. Deshalb sollte in Betracht gezogen werden, Unterstützung und Anzeige zu entkoppeln oder Letztere anonym zu ermöglichen.
- Unterstützung der Firmen bei Fragen zur digitalen Sicherheit

  Für Fragen der digitalen Sicherheit braucht es zunehmend Lösungen, die jedoch für einzelne, insbesondere kleinere Firmen zu teuer und technisch zu anspruchsvoll sind bspw. gesicherte Datenübertragungs- und Kommunikationsplattformen. Hier gilt es Lösungen zu finden, wie Schweizer Firmen unterstützt werden können. Dafür bedarf es in einem ersten Schritt einer politischen Diskussion über Möglichkeiten, Grenzen und Aufgaben staatlicher Stellen zur Unterstützung von Schweizer Firmen in Fragen digitaler Sicherheit. Mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken[2] wurde eine solche

[2] Im Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022 (https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/umsetzungsplan.html) werden diverse Massnahmen erläutert,

Grundlage geschaffen. Danach kann die Umsetzung von entsprechenden Unterstützungsmassnahmen in die Praxis folgen. Wichtig bleibt dabei, die Frage der konkreten Unterstützung insbesondere von KMU.

- Unterstützung der Firmen bei Fragen zur globalisierten Wirtschaft
  Grosse wie kleine Firmen sind mittlerweile oft global tätig. Um die aufgezeigten Herausforderungen zu bewältigen, braucht es Know-how und Ressourcen. Auch hier stellt sich die Frage, wie staatliche Stellen Firmen in einem globalisierten Umfeld unterstützen können, damit diese vor den Bedrohungen von Wirtschaftsspionage besser geschützt sind.

Literatur

Bitkom (2016). Kosten eines Cyber-Schadensfalles. Leitfaden. Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Bollhöfer, Esther & Jäger, Angela (2018). Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Band A 8 09/2018. Freiburg i.Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Bundesamt für Statistik (2008). NOGA 2008: Allgemeine Systematik der Wirtschaftszweige. Struktur. Neuchâtel: Bundesamt für Statistik.

Ernst&Young GmbH. «Datenklau: neue Herausforderungen für deutsche Unternehmen.» Ergebnisse einer Befragung von 400 deutschen Unternehmen. https://acfe.de/wp-content/uploads/0057f20160429_009_Studie_2013_EY_Datenklau-Neue-Herausforderungen-fuer-deutsche-Unternehmen.pdf. [Zugriff am 28.10.2019].

Fleischer, Dirk (2016). Wirtschaftsspionage. Phänomenologie – Erklärungsansätze – Handlungsoptionen. Wiesbaden: Springer.

welche von den verschiedenen beteiligten Organisationen der Bundesverwaltung umgesetzt werden sollten, um Firmen bei Fragen zur digitalen Sicherheit zu unterstützen. Die ersten darin vorgeschlagenen Massnahmen sind bereits umgesetzt, andere werden in den nächsten Jahren angegangen.

Gragido, Will & Pirc, John (2011). Cyber and Espionage. An Analysis of Subversive Multivector Threats. Burlington, MA: Elsevier.

Kasper, Karsten (2014). Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse. Wiesbaden: Bundeskriminalamt.

KMU (2018). Portal für kleinere und mittlere Unternehmen. KMU in Zahlen: Firmen und Beschäftigte. https://www.kmu.admin.ch/kmu/de/home/kmu-politik/kmu-politik-zahlen-und-fakten/kmu-in-zahlen/firmen-und-beschaeftigte.html [Zugriff am 16.8.2019].

Körmer, Claudia & Langer, Martin (2015). Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015. Forschungsbericht im Auftrag des Bundesministeriums für Inneres/ Bundesamt für Verfassungsschutz und Terrorismusbekämpfung durch die FH Campus Wien Forschungs- und Entwicklungs GmbH. https://www.bvt.gv.at/401/files/StudieWirtschafts-undIndustriespionageinoesterreichischenUnternehmen2015.pdf [Zugriff am 25.10.2019].

KPMG (2019). Wirtschaftskriminalität und was man dagegen tun kann. *Audit Committee News – Risk Management & Compliance*. 66 (Q3): 1–6. https://home.kpmg/content/dam/kpmg/ch/pdf/wirtschaftskriminalitaet-was-man-dagegen-tun-kann-de.pdf%20Zugriff%20am%2016.7.2019 [Zugriff am 16.7.2019].

NZZ (2018). Gegen Cyberkriminalität hilft gesunder Menschenverstand. 15.9.2018. https://www.nzz.ch/meinung/gegen-cyberkriminalität-hilft-gesunder-menschenverstand-ld.1420289 [Zugriff am 13.11.2019].

PWC (2016). Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. www.pwc.de/wirtschaftskriminalitaet. [Zugriff am 16.7.2019].

Tages-Anzeiger (2019). Die Hackerin, die zu viel prahlte. 31.7.2019. https://m.tagesanzeiger.ch/articles/15179253 [Zugriff am 13.11.2019].

Tsolkas, Alexander & Wimmer, Friedrich (2013). Wirtschaftsspionage und Intelligence Gathering. Neue Trends der wirtschaftlichen Vorteilsbeschaffung. Wiesbaden: Springer.

Wimmer, Bruce (2015). Business Espionage. Risk, Threats, and Countermeasures. Waltham, MA: Elsevier.

Wirtschaftsspionage Konkurrenzausspähung in Deutschland und Europa (2018): Das Forschungsprojekt WISKOS. https://wiskos.de/files/pdf4/Zusammenfassung_Gesamt_neu.pdf [Zugriff am 16.8.2019].