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.